∫ 5191

A969

DIVISIBILITY CRITERIA AND SEQUENCE GENERATORS ASSOCIATED WITH FERMAT COEFFICIENTS

R.P. Loh

Department of Applied Mathematics,
University of Sydney,
SYDNEY, N.S.W., 2006

A.G. Shannon

School of Mathematical Sciences,
N.S.W. Institute of Technology,
BROADWAY, N.S.W., 2007

A.F. Horadam

Department of Mathematics,
University of New England,
ARMIDALE, N.S.W., 2351

1. INTRODUCTION

The theory of Lucas - type sequences has been useful in the extension of divisibility properties of integers for several decades from Lehmer [7] to Morrison [9]. In this note, we use sequences defined by the recurrence relation

(1.1) $F_{N,n} = F_{N,n-1} + NF_{N,n-2}$ (N > 0, n > 2, integers)

with $F_{N,1} = F_{N,2} = 1$. Gridgeman [3] has tabulated numerical values of these numbers, and from Lucas [8] we have

(1.2) $F_{N,n} = (a^n - b^n)/(a-b)$,

where a,b are zeros of $x^2 - x - N = 0$.

We propose to extend the Fermat coefficients of Piza [10] to develop some divisibility criteria, including a primality test in Section 2, and to generate a number of the sequences of Sloane [12] in Section 3.

2. DIVISIBILITY CRITERIA

Vorob'ev [13] defines v_n as a *proper divisor* of an element $F_{N,n}$ of $\{F_{N,n}\}$ if $v_n | F_{N,n}$ but $v_n \nmid F_{N,m}$ where m < n. Table 1 lists the first few values of these proper divisors. In this, we have extended the definition of proper divisors as follows:

For any sequence $\{u_n\}$, n ≥ 1, where $u_n \in \mathbb{Z}$ or $u_n(x) \in \mathbb{Z}(x)$, the proper divisor v_n is the quantity implicitly defined for n ≥ 1, $v_1 = u_1$, and $v_n = \max \{d : d|u_n, \text{ g.c.d.}(d,v_m) = 1, \text{ for any } m < n\}$.

Thus, the proper divisors themselves form a sequence generated by the original sequence. As particular cases of Equation (2.1) and Theorem 1 respectively of [6], we have that

$$(2.1) \qquad F_{N,n} = \prod_{d|n} v_d$$

and

$$(2.2) \qquad v_n = \prod_{d|n} F_{N,d}^{\mu(n/d)}$$

where μ is the Möbius function.

n	$F_{N,n}$	v_n
3	$N+1$	$N+1$
4	$2N+1$	$2N+1$
5	N^2+3N+1	N^2+3N+1
6	$3N^2+4N+1$	$3N+1$
7	N^3+6N^2+5N+1	N^3+6N^2+5N+1
8	$4N^3+10N^2+6N+1$	$2N^2+4N+1$
9	$N^4+10N^3+15N^2+7N+1$	N^3+9N^2+6N+1

Table 1. Proper Divisors

From equation (2.1) we have that for an odd integer p

$$(2.3) \qquad v_{2p} = F_{N,2p}/F_{N,p}$$

if, and only if, p is prime. By the general formula (1.2) and relations involving a and b, it can be readily established that

$$(2.4) \qquad F_{N,2p} = F_{N,p}^2 + 2NF_{N,p}F_{N,p-1}$$

and

$$(2.5) \qquad v_{2p} = F_{N,p} + 2NF_{N,p-1} \quad \text{(prime } p\text{)}.$$

Applying Equation (2.8) of Barakat [1] we can write

$$(2.6) \qquad F_{N,2n+1} = \sum_{j=0}^{n} \binom{n+j}{n-j} N^{n-j}$$

$$(2.7) \qquad F_{N,2n} = \sum_{j=0}^{n-1} \binom{n+j}{n-j-1} N^{n-j-1} .$$

We then let

$$(2.8) \qquad (i;j) = \frac{1}{2j+1} \binom{i+j}{i-j} ,$$

and use the known binomial coefficient result

$$(2.9) \qquad \frac{2n+1}{2j+1} \binom{n+j}{n-j} = \binom{n+j}{n-j} + 2 \binom{n+j}{n-j-1}$$

to obtain the following test for primality:

$$(2.10) \qquad \frac{v_{2p}-1}{p} = \sum_{j=0}^{i-1} (i;j) N^{i-j}$$

is an integer if, and only if, $p = 2i + 1$ is prime.

<u>Proof of (2.10):</u>

We exclude the case for $p = 2$ from consideration, even though it satisfies the first part.

$$v_{2p} = \left(\frac{a^2-b^2}{a-b}\right)^{\mu(p)} \left(\frac{a^p-b^p}{a-b}\right)^{\mu(2)} \left(\frac{a^{2p}-b^{2p}}{a-b}\right)^{\mu(1)}$$ (if, and only if, p is prime or non-square free)

$$= a^p + b^p$$

$= (a + b)^p \pmod p$ (if p is prime, and not if p is non-square free)

$$= 1 \pmod p .$$

Thus $(v_{2p}-1)/p$ is an integer for p an odd prime. From equations (2.5), (2.6) and 2.9) we get

$$v_{2p} = F_{N,2i+1} + 2\,N\,F_{N,2i}$$

$$= \sum_{j=0}^{i} \left\{ \begin{bmatrix} i+j \\ i-j \end{bmatrix} + 2 \begin{bmatrix} i+j \\ i+j-1 \end{bmatrix} \right\} N^{i-j} \quad ,$$

from which the result follows.

Piza [10] had obtained the right-hand side of equation (2.10) as a test for primality, but the result here goes further by relating the test to the proper divisors. Further properties of the coefficients (i;j) will be illustrated in Section 3.

We define

$$v_{1,n} = \prod_{\substack{2d \nmid n \\ d \mid n}} v_d \qquad \text{and} \qquad v_{2,n} = \prod_{2d \mid n} v_d$$

so that

$$F_{N,n} = v_{1,n}\, v_{2,n}$$

and

$$v_{1,n} = F_{N,n}/F_{N,n/2} \qquad \text{and} \qquad v_{2,n} = F_{N,n/2}.$$

We can now construct Table 2 which yields a set of Simson - type identities (see Equations (11) and (11') of Horadam [5] for 2K = p-1, p prime).

	K odd	K even
$v_p - N^K =$	$v_{1,p-1}\, v_{2,p+1}$	$v_{1,p+1}\, v_{2,p-1}$
$v_p + N^K =$	$v_{1,p+1}\, v_{2,p-1}$	$v_{1,p-1}\, v_{2,p+1}$
$v_{2p} - N^K =$	$v_{1,p-1}\, v_{1,p+1}$	$v_{2,p-1}\, v_{2,p+1}\ (4N+1)$
$v_{2p} + N^K =$	$v_{2,p-1}\, v_{2,p+1}\ (4N+1)$	$v_{1,p-1}\, v_{1,p+1}$

Table 2. Simson-Type Identities

For example, when $p = 19$ and $K = 9$:

$$\begin{aligned} v_{19} - N^9 &= 45N^8 + 330N^7 + 924N^6 + 1287N^5 + 1001N^4 + 455N^3 + 120N^2 + 17N \pm 1 \\ &= (5N^2 + 5N + 1)(N^2 + 3N + 1)(3N^3 + 9N^2 + 6N + 1)(3N + 1) \\ &= (v_{10}\ v_5)\ (v_{18}\ v_6) \\ &= v_{2,20}\ v_{1,18} \end{aligned}$$

In passing, one might note another division property of these numbers, namely

$$(2.11) \qquad \frac{F_{N,k(n+1)}}{F_{N,k}} = \sum_{0 \le r+s \le n} \binom{r}{s} \binom{n-r}{s} F_{k-1}^{r-s}\ F_k^{2s}\ F_{k+1}^{n-r-s}\ N^r$$

When $k = 1$ and $r = s$, the theorem reduces to Barakat's result [1].

<u>Proof of (2.11):</u>

Following Carlitz [2] we let

$$S_n^{(k)}(N) = \sum_{r_1,\ldots,r_k} \binom{n-r_k}{r_1} \binom{n - r_1}{r_2} \cdots \binom{n - r_{k-1}}{r_k} N^{r_1+r_2+\ldots+r_k+kn}$$

$r_1 + r_2 \le n, \ \ldots\ , r_{k-1} + r_k \le n,\ r_k + r_1 \le n.$

Carlitz in effect has shown that

$$S_n^{(k)}(N) = F_{N,k+1}^{r}\ F_{N,k+2}^{n-r}$$

Then

$$\sum_{r=0}^{n} S_n^{(k)}(N)x^n = \sum_{r=0}^{n} F_{N,k+1}^{r} x^r F_{N,k+2}^{n-r} x^{n-r}$$

$$= \sum_{r=0}^{n} (F_k + N F_{k-1})^r (F_{k+1} + N F_k)^{n-r} x^n$$

(in which we write F_k for $F_{N,k}$ for brevity)

$$= \sum_{r,s,t} \binom{r}{s} \binom{n-r}{t} F_{k-1}^{r-s} F_k^{n+s-r-t} F_{k+1}^{t} N^{n-s-t} x^n$$

$$\sum_{n=0}^{\infty} S_n^{(k)}(N) z^n = \sum_{r=0}^{\infty} \sum_{s=0}^{r} \sum_{t=0}^{\infty} \binom{r}{s} \binom{t+s}{s} F_{k-1}^{r-s} F_k^{2s} F_{k+1}^{t} N^r z^{r+s+t}$$

$$(t = n-r-s)$$

$$= \sum_{r=0}^{\infty} \sum_{s=0}^{r} \binom{r}{s} \left(1 - F_{k+1} z\right)^{-s-1} F_{k-1}^{r-s} F_k^{2s} N^r z^{r+s}$$

$$= \sum_{s=0}^{\infty} \sum_{r=0}^{\infty} \binom{r+s}{s} \left(1 - F_{k+1} z\right)^{-s-1} F_{k-1}^{r} F_k^{2s} N^{r+s} z^{r+2s}$$

$$= \sum_{s=0}^{\infty} \left(1 - N F_{k-1} z\right)^{-s-1} \left(1 - F_{k+1} z\right)^{-s-1} F_k^{2s} N^s z^{2s}$$

$$= ((1 - N F_{k-1} z)(1-F_{k+1} z) - N F_k^2 z^2)^{-1}$$

$$= (1 - (N F_{k-1} + F_{k+1})z - N(F_k^2 - F_{k-1} F_{k+1})z^2)^{-1}$$

$$= (1 - (a^k + b^k)z + (-1)^k N^k z^2)^{-1}$$ (from Horadam's equation (4.3) [5])

$$= (1 - a^k z)^{-1}(1 - b^k z)^{-1}$$

$$= ((a^k(1-a^k z)^{-1} - b^k(1-b^k z)^{-1})/(a^k - b^k)$$

$$= \sum_{n=0}^{\infty} \left(\frac{a^{nk+k} - b^{nk+k}}{a^k - b^k}\right) z^n ,$$

from which we get the result on equating coefficients of z^n.

3. SEQUENCE GENERATORS

The coefficients $(i;j)$ introduced in (2.8) satisfy the partial recurrence relation

$$(i+j-1)(i;j-1) = (2j+1)((i;j) - (i-1;j)) \tag{3.1}$$

which can be used to prove some of the results noted below. The $(i;j)$ are related to the Fermat coefficients $(i:j)$ of Piza [10] by

$$(i;j) = (i:i-j), \tag{3.2}$$

and because of this, Table 3 has entries similar to those of Piza. It is included for convenience of referral in the subsequent development. Underlined numbers indicate non-integer values, the number tabulated being $[(i;j)]$, the integer part of $(i;j)$.

i \ j	0	1	2	3	4	5	6	7	8	9	10	11
1	1											
2	1	1										
3	1	2	1									
4	1	$\underline{3}$	3	1								
5	1	5	7	4	1							
6	1	7	14	12	5	1						
7	1	$\underline{9}$	$\underline{25}$	30	$\underline{18}$	6	1					
8	1	12	42	66	55	36	7	1				
9	1	15	66	132	143	91	35	8	1			
10	1	$\underline{18}$	99	$\underline{245}$	$\underline{334}$	273	140	$\underline{45}$	9	1		
11	1	22	143	429	715	728	476	204	57	10	1	
12	1	26	$\underline{200}$	715	1430	1768	1428	$\underline{775}$	285	70	11	1

Table 3. Values for $(i;j)$

Furthermore, in compiling this table it was observed that if p is a prime of the form 6a ± 1, then $(\binom{Np-1}{p-1}-1)/p^3$ is an integer.

Professor Ralph Stanton, of the Department of Computer Science at the University of Manitoba, has observed that this conjecture is stated, without proof, in Dickson's History of the Theory of Numbers (Vol. I ,p. 275). In the same correspondence Professor Stanton has confirmed the conjecture in an elegant proof.

Another phenomenon of interest is the number of different sequences cited by Sloane [12] which are generated by (i;j). Table 4 lists a number which appear along the diagonals of Table 3, and Table 5 illustrates some sequences which are formed in other ways from the values of (i;j) in Table 3.

The Sequence {[(i+j;j)]} $\{ \begin{matrix} i = 1, 2, 3, \ldots \\ j = 0, 1, 2, \ldots \end{matrix}$		
i	Sequence	Sloane No.
1	1, 1, 1, 1, ...	
2	1, 2, 3, 4, ...	
3	1, 3, 7, 12, 18, 26, 35, 45, 57, 70, ...	1042 ✓
4	1, 5, 14, 30, 55, 91, ...	1574 ✓
5	1, 7, 25, 66, 143, 273, 476, 775, ...	1846 ✓
6	1, 9, 42, 132, 334, 728, 1428, ...	1975 ✓
7	1, 12, 66, 245, 715, 1768, ...	2072 ✓
8	1, 15, 99, 429, 1430, ...	2137 ✓

Table 4: Sequences generated along Diagonals of Table 3

General term	Sequence	Sloane No.
$\{[(i;1)]\}$	1, 2, 3, 5, 7, 9, 12, ...	233
$\left\{\sum_{j=0}^{\left[\frac{i+1}{2}\right]} [(i-j;j)]\right\}$	1, 2, 3, 5, 9, 16, 28, ...	262
$\left\{\sum_{j=0}^{i-1} [(i;j)]\right\}$	1, 2, 4, 8, 18, 40, 91, ...	437
$\{[(2j;j)]\}$	1, 3, 12, 55, 273, 1428, ...	1174
$\{[(3i-1;1)]\}$	1, 5, 12, 22, 35, 51, 70, ...	1562
$\{[(3j;2j)]\}$	1, 5, 35, 285, 2530, ...	1646
$\{[(2i+1;2)]\}$	1, 7, 25, 66, 143, ...	1846
$\{[(4j;3j)]\}$	1, 7, 70, 819, 10472, ...	1878

Table 5: Some other sequences generated by $(i;j)$

By way of conclusion, we note that $(i;j)$ is defined when the fractional parts of i and j are both $\frac{1}{2}$. In fact, it can be proved by setting $r=1$ in Equation (3.2) of Shannon [11] that when $i = \frac{1}{2}n-2$, $j=\frac{1}{2}n-m$, after algebraic manipulation,

$$(3.3) \qquad \left(\frac{n-4}{2}\ ;\ \frac{n-2m}{2}\right) = \left(\frac{2n-3m-1}{2}\ ;\ \frac{m-3}{2}\right) .$$

Readers might like to test the conjecture that $\{jk+2j;jk\}$ generates integer sequences for integer k. For $k=1,2,3,4,5,6$, we get sequences 577, 1174, 1454, 1646, 1780 and 1878 respectively. For example, when $k=1$, we get the Catalan numbers (577) $\{1,2,5,14,42,132,429,1430, \ldots\}$ for $j = \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, \ldots$.

REFERENCES

1. R. Barakat, "The matrix operator e^X and the Lucas polynomials", Journal of Mathematics and Physics, 43 (1964), 332-335.

2. L. Carlitz, "Some multiple sums and binomial identities", Journal of the Society for Industrial and Applied Mathematics, 13 (1965), 469-486.

3. N.T. Gridgeman, "A new look at Fibonacci generalization", Fibonacci Quarterly, 11 (1973), 40-55.

4. A.F. Horadam, "A generalized Fibonacci sequence", American Mathematical Monthly, 68 (1961), 455-459.

5. A.F. Horadam, "Basic properties of a certain generalised sequence of numbers", Fibonacci Quarterly, 3 (1965), 161-176.

6. A.F. Horadam, R.P. Loh and A.G. Shannon, "Divisibility properties of some Fibonacci-type sequences", in A.F. Horadam and W.D. Wallis (eds.), Combinatorial Mathematics VI, Lecture Notes in Mathematics, 748, Springer-Verlag, Heidelberg, 1979, 55-64.

7. D.H. Lehmer, "An extended theory of Lucas functions", Annals of Mathematics, 31 (1930), 442-443.

8. E. Lucas, The Theory of Simply Periodic Numerical Functions (edited by D.A. Lind, translated by S.A. Kravitz), Fibonacci Association, San José, 1969.

9. M.A. Morrison, "A note on primality testing using Lucas sequences", Mathematics of Computation, 29 (1975), 181-182.

10. P.A. Piza, "Fermat coefficients", Mathematics Magazine, 27 (1954), 141-146.

11. A.G. Shannon, "Iterative formulas associated with generalized third over recurrence relations", Society for Industrial and Applied Mathematics Journal on Applied Mathematics, 23 (1972), 364-368.

12. N.J.A. Sloane, A Handbook of Integer Sequences, Academic Press, New York, 1961.

13. N.N. Vorob'ev, Fibonacci Numbers, Pergamon, Oxford, 1961.