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

\[(1.1) \quad F_{N,n} = F_{N,n-1} + NF_{N,n-2} \quad (N > 0, n > 2, \text{ integers})\]

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

\[(1.2) \quad F_{N,n} = \frac{a^n - b^n}{a-b},\]

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 \(v_n \mid F_{N,n}\) 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 \(\{u_n\}, n \geq 1\), 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 \(n \geq 1\), \(v_1 = u_1\), and \(v_n = \max \{d : d \mid u_n, \gcd(d, v_m) = 1, \text{ for any } m < n\}\).
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

\[(2.1) \quad F_{N,n} = \prod_{d|n} v_d\]

and

\[(2.2) \quad v_n = \prod_{d|n} F_{N,d}^\mu(n/d)\]

where \(\mu\) is the Möbius function.

<table>
<thead>
<tr>
<th>n</th>
<th>(F_{N,n})</th>
<th>(v_n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>N+1</td>
<td>N+1</td>
</tr>
<tr>
<td>4</td>
<td>2N+1</td>
<td>2N+1</td>
</tr>
<tr>
<td>5</td>
<td>N^2+3N+1</td>
<td>N^2+3N+1</td>
</tr>
<tr>
<td>6</td>
<td>3N^2+4N+1</td>
<td>3N+1</td>
</tr>
<tr>
<td>7</td>
<td>N^3+6N^2+5N+1</td>
<td>N^3+6N^2+5N+1</td>
</tr>
<tr>
<td>8</td>
<td>4N^3+10N^2+6N+1</td>
<td>2N^2+4N+1</td>
</tr>
<tr>
<td>9</td>
<td>N^4+10N^3+15N^2+7N+1</td>
<td>N^3+9N^2+6N+1</td>
</tr>
</tbody>
</table>

**Table 1. Proper Divisors**

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

\[(2.3) \quad v_{2p} = F_{N,2p}/F_{N,p}\]

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

\[(2.4) \quad F_{N,2p} = F_{N,p}^2 + 2N F_{N,p} F_{N,p-1}\]

and

\[(2.5) \quad v_{2p} = F_{N,p} + 2N F_{N,p-1} \quad (\text{prime } p).\]
Applying Equation (2.8) of Barakat [1] we can write

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

\[(2.7) \quad F_{N,2n} = \sum_{j=0}^{n-1} \binom{n+j}{n-j-1} N^{n-j-1}\]

We then let

\[(2.8) \quad (i;j) = \frac{1}{2j+1} \binom{i+j}{i-j}\]

and use the known binomial coefficient result

\[(2.9) \quad \frac{2n + 1}{2j + 1} \binom{n+j}{n-j} = \binom{n+j}{n-j} + 2 \binom{n+j}{n-j-1}\]

to obtain the following test for primality:

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

is an integer if, and only if, \(p = 2i + 1\) is prime.

**Proof of (2.10):**

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

\[v_{2p} = \left( \frac{a^2-b^2}{a-b} \right)^{\mu(p)} \left( \frac{a^p-b^p}{a-b} \right)^{\mu(2)} \left( \frac{a^{2p}-b^{2p}}{a-b} \right)^{\mu(1)}\]

\[= a^p + b^p\]

\[= (a + b)^p \pmod{p} \text{ (if } p \text{ is prime, and not if } p \text{ is non-square free)}\]

\[= 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
\[ v_{2p} = F_{N,2i+1} + 2 N F_{N,2i} \]
\[ = \sum_{j=0}^{i} \left( \binom{i+j}{i-j} + 2 \binom{i+j}{i+j-1} \right) n^{i-j}, \]

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
\[ v_{1,n} = \prod_{d|n} v_d \quad \text{and} \quad v_{2,n} = \prod_{d|n} v_d \]
so that
\[ F_{N,n} = v_{1,n} v_{2,n} \]

and
\[ v_{1,n} = F_{N,n} \sqrt{F_{N,n}/2} \quad \text{and} \quad v_{2,n} = F_{N,n}/2. \]

We can now construct Table 2 which yields a set of Simson-type identities (see Equations (11) and (11') of Horadam [5] for \(2K = p-1, \ p \text{ prime}\).
\[
\begin{array}{c|c|c}
\text{K odd} & \text{K even} \\
\hline
v_p - N^k & v_{1,p-1} v_{2,p+1} & v_{1,p+1} v_{2,p-1} \\
v_p + N^k & v_{1,p+1} v_{2,p-1} & v_{1,p-1} v_{2,p+1} \\
v_{2p} - N^k & v_{1,p-1} v_{1,p+1} & v_{2,p-1} v_{2,p+1} (4N + 1) \\
v_{2p} + N^k & v_{2,p-1} v_{2,p+1} (4N + 1) & v_{1,p-1} v_{1,p+1} \\
\end{array}
\]

Table 2. Simson-Type Identities

For example, when \( p = 19 \) and \( K = 9 \):

\[
v_{19} - N^9 = 45N^8 + 330N^7 + 924N^6 + 1287N^5 + 1001N^4 + 455N^3 + 120N^2 + 17N + 1
\]

\[
= (5N^2 + 5N + 1)(N^2 + 3N + 1)(3N^3 + 9N^2 + 6N + 1)(3N + 1)
\]

\[
= (v_{10} v_5) (v_{18} v_6)
\]

\[
= v_{2,20} v_{1,18}
\]

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

\[
(2.11) \quad \frac{F_{N,k}(n+1)}{F_{N,k}} = \sum_{0 \leq r+s \leq n} \binom{r}{s} \binom{n-r}{s} F_{k-1}^r F_k^{2s} F_{k+1}^{n-r-s} N^r
\]

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

Proof of (2.11):

Following Carlitz [2] we let

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

\[
r_1 + r_2 \leq n, \ldots, r_{k-1} + r_k \leq n, r_k + r_1 \leq n.
\]

Carlitz in effect has shown that

\[
S_n^{(k)}(N) = F_N^r F_{N,k+1}^{n-r} F_{N,k+2}
\]
Then
\[ \sum_{r=0}^{n} S_n^{(k)} (N)x^n = \sum_{r=0}^{n} P_{N,k+1}^r \times P_{N,k+2}^{n-r} \times r^{-r} \]
\( n \)
\( k \)
\( k \)
\( (F_k + N F_{k-1}) \times (F_{k+1} + N F_k)^{n-r} \times x^n \)

(in which we write \( P_k \) for \( P_{N,k} \) for brevity)

\[ = \sum_{r,s,t} \left[ \begin{array}{c} r \\ s \\ t \end{array} \right] \times \left[ \begin{array}{c} n-r \\ n+s-r-t \\ n \end{array} \right] \times F_r^{k-1} F_{k+2}^{s+t} N^n x \]

\[ \sum_{n=0}^{\infty} S_n^{(k)} (N)z^n = \sum_{r=0}^{n} \sum_{s=0}^{r} \sum_{t=0}^{s} \left[ \begin{array}{c} r+s+t \\ s \end{array} \right] \times \left[ \begin{array}{c} r-s \\ 2s \\ t \end{array} \right] \times F_{k-1}^{s} F_{k+1}^{t} N^n z^{r+s+t} \]

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

\[ = \sum_{r=0}^{n} \sum_{s=0}^{r} \sum_{t=0}^{s} \left[ \begin{array}{c} r+s \\ s \end{array} \right] \times \left[ \begin{array}{c} 1-F_{k+1} z \\ 1-F_{k+1} z \end{array} \right] \times F_{k-1}^{r-s} F_{k+1}^{2s} N^n z^{r+s} \]

\[ = \sum_{s=0}^{n} \sum_{r=0}^{s} \sum_{t=0}^{s} \left[ \begin{array}{c} 1-N F_{k-1} z \\ 1-N F_{k-1} z \end{array} \right] \times \left[ \begin{array}{c} 1-F_{k+1} z \\ 1-F_{k+1} z \end{array} \right] \times F_{k-1}^{r-s} F_{k+1}^{2s} N^n z^{r+s} \]

\[ = \left( (1-N F_{k-1} z)(1-F_{k+1} z) - N F_{k+1}^2 z^2 \right)^{-1} \]

\[ = \left( 1 - (N F_{k-1} + F_{k+1}) z - N(F_{k-1}^2 - F_{k+1} F_{k-1}) z^2 \right)^{-1} \]

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

\[ = (1 - a^k z)^{-1} (1 - b^k z)^{-1} \]

\[ = \left( (a^k (1-a^k z)^{-1} - b^k (1-b^k z)^{-1}) / (a^k - b^k) \right) \]

\[ = \sum_{n=0}^{\infty} \left( \frac{a^{n+1} - b^{n+1}}{a^k - b^k} \right) \times z^n , \]

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

\[(i+j-1)(i;j-1) = (2j+1)((i;j) - (i-1;j))\]

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

\[(i;j) = (i,i-j),\]

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 \((i;j)\).

<table>
<thead>
<tr>
<th>i</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>5</td>
<td>7</td>
<td>4</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>7</td>
<td>14</td>
<td>12</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>9</td>
<td>25</td>
<td>30</td>
<td>18</td>
<td>6</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>12</td>
<td>42</td>
<td>66</td>
<td>55</td>
<td>36</td>
<td>7</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>15</td>
<td>66</td>
<td>132</td>
<td>143</td>
<td>91</td>
<td>35</td>
<td>8</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>18</td>
<td>99</td>
<td>245</td>
<td>334</td>
<td>273</td>
<td>140</td>
<td>45</td>
<td>9</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>22</td>
<td>143</td>
<td>429</td>
<td>715</td>
<td>728</td>
<td>476</td>
<td>204</td>
<td>57</td>
<td>10</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>26</td>
<td>200</td>
<td>715</td>
<td>1430</td>
<td>1768</td>
<td>1428</td>
<td>775</td>
<td>285</td>
<td>70</td>
<td>11</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3. Values for \((i;j)\)
Furthermore, in compiling this table it was observed that if \( p \) is a prime of the form \( 6a \pm 1 \), then \( \left( \binom{Np-1}{p-1} \right) / p^3 \) 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.

<table>
<thead>
<tr>
<th>(i)</th>
<th>(j = 0, 1, 2, 3, \ldots)</th>
<th>(j = 0, 1, 2, \ldots)</th>
<th>(i = 1, 2, 3, \ldots)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, 1, 1, 1, ...</td>
<td>1, 1, 1, 1, ...</td>
<td>1, 1, 1, 1, ...</td>
</tr>
<tr>
<td>2</td>
<td>1, 2, 3, 4, ...</td>
<td>1, 2, 3, 4, ...</td>
<td>1, 2, 3, 4, ...</td>
</tr>
<tr>
<td>3</td>
<td>1, 3, 7, 12, 18, 26, 35, 45, 57, 70, ...</td>
<td>1, 3, 7, 12, 18, 26, 35, 45, 57, 70, ...</td>
<td>1, 3, 7, 12, 18, 26, 35, 45, 57, 70, ...</td>
</tr>
<tr>
<td>4</td>
<td>1, 5, 14, 30, 55, 91, ...</td>
<td>1, 5, 14, 30, 55, 91, ...</td>
<td>1, 5, 14, 30, 55, 91, ...</td>
</tr>
<tr>
<td>5</td>
<td>1, 7, 25, 66, 143, 273, 476, 775, ...</td>
<td>1, 7, 25, 66, 143, 273, 476, 775, ...</td>
<td>1, 7, 25, 66, 143, 273, 476, 775, ...</td>
</tr>
<tr>
<td>6</td>
<td>1, 9, 42, 132, 334, 728, 1428, ...</td>
<td>1, 9, 42, 132, 334, 728, 1428, ...</td>
<td>1, 9, 42, 132, 334, 728, 1428, ...</td>
</tr>
<tr>
<td>7</td>
<td>1, 12, 66, 245, 715, 1768, ...</td>
<td>1, 12, 66, 245, 715, 1768, ...</td>
<td>1, 12, 66, 245, 715, 1768, ...</td>
</tr>
<tr>
<td>8</td>
<td>1, 15, 99, 429, 1430, ...</td>
<td>1, 15, 99, 429, 1430, ...</td>
<td>1, 15, 99, 429, 1430, ...</td>
</tr>
</tbody>
</table>

Table 4: Sequences generated along Diagonals of Table 3
Table 5: Some other sequences generated by \((i;j)\)

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

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

\[
\frac{n-4}{2} ; \frac{n-2m}{2} = \frac{2n-3m-1}{2} ; \frac{m-3}{2}
\]

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 \((577)\) \(\{1,2,5,14,42,132,429,1430, ...\}\) for \(j = \frac{1}{2}, 1, \frac{3}{2}, 2, \frac{5}{2}, \ldots\). 

REFERENCES


