A NEW PRIMALITY CRITERION OF MANN AND SHANKS AND ITS RELATION TO A THEOREM OF HERMITE WITH EXTENSION TO FIBONOMIALS

H. W. GOULD
W. Virginia University, Morgantown, West Virginia

1. INTRODUCTION

Henry Mann and Daniel Shanks [4] have found a new necessary and sufficient condition for a number to be a prime. This criterion may be stated in novel terms as a property of a displaced Pascal Arithmetical Triangle as follows. Consider a rectangular array of numbers made by moving each row in the usual Pascal array two places to the right from the previous row. The $n+1$ binomial coefficients $\binom{n}{k}$, $k = 0, 1, \cdots, n$, are then found in the n^{th} row between columns $2n$ and $3n$ inclusive. We shall say that a given column has the Row Divisibility Property if each entry in the column is divisible by the corresponding row number. Then the new criterion is that the column number is a prime if and only if the column has the Row Divisibility Property.

Column Number

Row Number	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1																			
1			1	1																
2					1	2	1													
3							1	3	3	1										
4									1	4	6	4	1							
5											1	5	10	10	5	1				
6													1	6	15	20	15	6	1	
7															1	7	21	35	35	21
8																	1	8	28	56
9																			1	9

The Displaced Array

We wish to show here that by relabelling the array it is easy to relate the new criterion with a theorem of Hermite on factors of binomial coefficients. We shall also generalize to a displaced Fibonomial array. The case for arbitrary rectangular arrays of extended coefficients is treated.

2. THEOREMS OF HERMITE

According to Dickson's History [2, p. 272] Hermite stated that

$$\frac{m}{(m,n)} \Bigg| \binom{m}{n} \tag{2.1}$$

and

$$\frac{m - n + 1}{(m + 1,n)} \Bigg| \binom{m}{n} , \tag{2.2}$$

where (a,b) denotes the greatest common divisor of a and b. Proofs were given by Catalan, Mathews, and Woodall according to Dickson. What is more, there are extensions to multinomial coefficients and Ricci [5] noted that

$$\frac{m!}{a!\,b!\,\cdots\,c!} \equiv 0 \mod \frac{m}{(a, b, \cdots, c)} , \text{ where } a + b + \cdots + c = m . \tag{2.3}$$

These theorems have been used in many ways to derive results in number theory. For example, Eq. (2.1) gives us at once that

$$p \Bigg| \binom{p}{k}$$

for each k with $1 \le k \le p - 1$ provided that p is a prime. This has been used in various proofs of Wilson's criterion and Fermat's congruence. From (2.2) we obtain at once that

$$n + 1 \Bigg| \binom{2n}{n} ,$$

i.e., the numbers generated by

$$\frac{\binom{2n}{n}}{(n + 1)} :$$

1, 1, 2, 5, 14, 42, 132, 429, 1430, $\cdots$ are all integers. This sequence, the so-called Catalan sequence, is of considerable importance in combinatorics and graph theory, and the reader may consult the historical note of Brown [1] for details.

For the sake of completeness we wish to include proofs of (2.1) and (2.2) to show how easily they follow from the Euclidean algorithm.

By the Euclidean algorithm we know that there exist integers A and B such that

$$(m,n) = d = mA + nB .$$

Therefore

$$d\,\frac{(m-1)(m-2)\cdots(m-n+1)}{n!} = \binom{m}{n}A + \binom{m-1}{n-1}B = E, \text{ an integer},$$

so that, upon multiplication by m we have

$$d\binom{m}{n} = mE\,,$$

from which it is obvious that

$$\frac{m}{d} \,\Big|\, \binom{m}{n}$$

as stated in (2.1). This is essentially Hermite's proof [3, 415-416, Letter of 17 April 1889]. Similarly, there exist integers C and D such that

$$(m+1,n) = d = (m+1)C + nD\,.$$

Rearranging,

$$d = (m-n+1)C + (C+D)n\,.$$

Therefore

$$d\,\frac{m(m-1)\cdots(m-n+2)}{n!} = \binom{m}{n}C + \binom{m}{n-1}(C+D) = F, \text{ an integer},$$

whence on multiplying by $m-n+1$ we have

$$d\binom{m}{n} = (m-n+1)F\,,$$

so that

$$\frac{m-n+1}{d} \,\Big|\, \binom{m}{n}$$

as stated in (2.2). Hermite's proof may be applied to other similar theorems.

The usefulness of Hermite's theorems suggested to me that one might get part of the results of Mann and Shanks from them.

3. FIRST RESTATEMENT OF THE CRITERION

Leaving the array arranged as before, it is easy to see that we may restate the condition of Mann and Shanks in the form

(3.1) $$k = \text{prime if and only if } n \,\Big|\, \binom{n}{k-2n}$$

for all integers n such that $k/3 \le n \le k/2$. If we take all entries in the array other than the binomial coefficients to be zero, we can say "for all n."

By Hermite's theorem (2.1) we have in general

$$\frac{n}{(n,k-2n)} \,\Big|\, \binom{n}{k-2n}$$

for all integers $2n \le k \le 3n$. Equivalently,

$$(n,k-2n)\binom{n}{k-2n} = nE\,,$$

for some integer E. Let k = prime. Then, except for $n = k$, $n \nmid k$, whence $n \nmid k - 2n$. But this means that $n \nmid (n, k - 2n)$, so that n must be a factor of

$$\binom{n}{k-2n}\,.$$

The case $n = k$ offers no difficulty since we are only interested in $k/3 \le n \le k/2$. The converse, that k must be prime if n is a factor of

$$\binom{n}{k-2n}$$

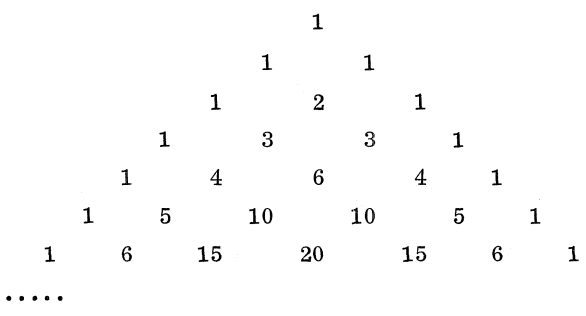
for every n can be handled along the lines of [4];

$$\binom{n}{k-2n} = 1$$

when $2 \mid k$ or $3 \mid k$ so one must consider prime columns that occur for k of form $6j \pm 1$.

4. SECOND RESTATEMENT OF THE CRITERION

Arrange the binomial coefficients in the usual array; $k = 0, 1, \cdots, n$ on the n^{th} row:



It is easy to see that the criterion may be stated as follows:

(4.1) $$2n + 1 = \text{prime} \text{ if and only if } n - k \mid \binom{n - k}{2k + 1}$$

for every

$$k = 0, 1, \cdots, \left(\frac{n - 1}{3}\right).$$

Since $2n \neq \text{prime}$ for $n > 1$ we may ignore the case whether

$$n - k \mid \binom{n - k}{2k}.$$

Again, Hermite's theorem (2.1) is the clue for the proof that $n - k$ is a factor when $2n + 1$ is a prime. For (2.1) gives us in general

$$\frac{n - k}{(n - k, 2k + 1)} \mid \binom{n - k}{2k + 1}$$

for all integers $0 \leq k \leq \frac{n - 1}{3}$. Equivalently,

$$(n - k, 2k + 1)\binom{n - k}{2k + 1} = (n - k)E,$$

for some integer E. Suppose $2n + 1 = \text{prime}$. If $n - k \mid 2k + 1$, then $n - k \mid 2k + 1 + 2(n - k)$, i.e., $n - k \mid 2n + 1$, which is again impossible so that $n - k \nmid (n - k, 2k + 1)$, whence we must have

$$n - k \mid \binom{n - k}{2k + 1} \text{ as desired.}$$

5. QUESTIONS

It would be of interest to see whether (2.2) implies any similar results. We find in general that

(5.1) $$\frac{3n - k + 1}{(n + 1, k - 2n)} \mid \binom{n}{k - 2n} \quad \text{for} \quad 2n \leq k \leq 3n,$$

and

(5.2) $$\frac{n - 3k}{(n - k + 1, 2k + 1)} \mid \binom{n - k}{2k + 1} \quad \text{for} \quad 0 \leq k \leq \frac{n - 1}{3}.$$

In (5.1) let $n - 3k \mid (n - k + 1, 2k + 1)$. Then $n - 3k \mid n - k + 1$ and $n - 3k \mid 2k + 1$. But $n - 3k \mid n - k + 1$ implies also $n - 3k \mid n - k + 1 - (n - 3k)$ or again $n - 3k \mid 2k + 1$.

If then $2k + 1$ = prime we again find that $n - 3k$ must divide the binomial coefficient, and this gives us

$$(5.3) \qquad 2k + 1 = \text{prime} \quad \text{implies} \quad n - 3k \mid \binom{n - k}{2k + 1} \quad \text{for all} \quad n \neq 5k + 1 .$$

It is easy to find examples of composite $2k + 1$ such that $n - 3k$ is not a factor of the binomial coefficient; e.g., take $k = 7$ and $n = 24$:

$$3 \nmid \binom{17}{15} .$$

Other possibilities suggest themselves. Letting $n - 3k \mid (n - k + 1, 2k + 1)$ gives again $n - 3k \mid n - k + 1$ whence also $n - 3k \mid 3(n - k + 1) - (n - 3k)$ or $n - 3k \mid 2n + 3$. If we then take $2n + 3$ = prime we again obtain a useful theorem.

It seems clear from just these samples that the theorems of Hermite can suggest quite a variety of divisibility theorems, some of which may lead to criteria similar to that of Mann and Shanks. Whether any of these have any strikingly simple forms remains to be seen. One possibility suggested by (2.2) is that

$$(n + k, k) \binom{n + k - 1}{k} = nE$$

for some integer E, from which we may argue that under certain hypotheses n divides $\binom{n + k - 1}{k}$.

Result (5.3) is related to a theorem of Catalan [2, p. 265] to the effect that

$$m!\, n! \mid (m + n - 1)!$$

provided $(m, n) = 1$.

Finally we wish to recall that some of the results here are related to a problem posed by Erdos (with published solution by F. Herzog) [6] to the effect that for every k there exist infinitely many n such that $(2n)!/n!(n + k)!$ is an integer (the case $k = 1$ yields the Catalan sequence). In fact Erdos claimed a proof that the set of values of n such that this ratio is not an integer has density zero.

6. FIBONOMIAL TRIANGLE

It is tempting to try and extend the primality criterion to arrays other than the binomial. Consider the array of Fibonomial coefficients of Hoggatt [7] displaced in the same manner as the array of Mann and Shanks:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
0	1																			
1			1	1																
1					1	1	1													
2							1	2	2	1										
3									1	3	6	3	1							
5											1	5	15	15	5	1				
8													1	8	40	60	40	8	1	
13															1	13	104	260	260	104
21																	1	21	273	1092
34																			1	34

Here the Fibonomial coefficients are defined by

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \frac{F_n F_{n-1} \cdots F_{n-k+1}}{F_k F_{k-1} \cdots F_1}, \qquad \left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = 1 ,$$

where $F_{n+1} = F_n + F_{n-1}$, with $F_0 = 0$, $F_1 = 1$, being the Fibonacci numbers. In the displaced array, the row numbers are made to be the corresponding Fibonacci numbers. From the above sampling, as well as from extended tables, one is tempted to conjecture that a column number is prime if and only if each Fibonomial coefficient in the column is divisible by the corresponding row Fibonacci number. In other words, it appears that

(6.1) $$k = \text{prime if and only if } F_n \Bigg| \left\{ \begin{matrix} n \\ k - 2n \end{matrix} \right\} \text{ for all } k/3 \le n \le k/2 .$$

Now as a matter of fact the exact analogue of Hermite's (2.1) is true:

(6.2) $$\frac{F_m}{(F_m, F_n)} \Bigg| \left\{ \begin{matrix} m \\ n \end{matrix} \right\} .$$

The proof is an exact replica of Hermite's proof. What is more, Eq. (2.1) holds true for perfectly arbitrary arrays in the sense defined in [8]. That is, take an arbitrary sequence of integers A_n such that $A_0 = 0$ and $A_n \neq 0$ for $n \ge 1$, and define generalized binomial coefficients by

(6.3) $$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \frac{A_n A_{n-1} \cdots A_{n-k+1}}{A_k A_{k-1} \cdots A_1}, \quad \text{with} \quad \left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} = 1 .$$

If all of these turn out to be integers, then we have

$$\frac{A_m}{(A_m, A_n)} \Bigg| \begin{Bmatrix} m \\ n \end{Bmatrix} . \tag{6.4}$$

However, the corresponding form of (2.2) is in general false. The reason is that the step

$$(A_{m+1}, A_n) = d = CA_{m+1} + DA_n = C(A_{m+1} - A_n) + (D + C)A_n$$

can be applied only if also

$$A_{m+1} - A_n = A_{m-n+1}$$

or something close. Thus it is not at once clear that the Fibonomial Catalan numbers

$$\frac{\begin{Bmatrix} 2n \\ n \end{Bmatrix}}{F_{n+1}}$$

are integers. The first few of these are in fact 1, 1, 3, 20, 364, 17017, etc.

However, having (2.1) extended to (6.4) is a good result because in order to obtain a theorem such as

$$k = \text{prime} \quad \text{implies} \quad A_n \Bigg| \begin{Bmatrix} n \\ k - 2n \end{Bmatrix} \quad \text{for all} \quad k/3 \le n \le k/2 , \tag{6.5}$$

it is only necessary to be able to prove that

$$(A_n, A_{k-2n}) = 1 \quad \text{when} \quad k = \text{prime, and} \quad k/3 \le n \le k/2 . \tag{6.6}$$

For the Fibonacci numbers this is easy because of a known fact that in general

$$(F_a, F_b) = F_{(a,b)} . \tag{6.7}$$

Thus we have $(F_n, F_{k-2n}) = F_{(n,k-2n)}$ so that for k = prime we know as in (3.1) that $(n, k - 2n) = 1$, and since $F_1 = 1$ we have the desired result. The Fibonomial displaced array criterion then parallels the ordinary binomial case studied by Mann and Shanks.

Quite a few standard number-theoretic results have analogues in the Fibonomial case.

7. FIBONOMIAL ANALOGUE OF HERMITE'S SECOND THEOREM

Although we have just indicated that divisibility theorem (2.2) does not hold in general for the generalized binomial coefficients, we now show that it does hold for the Fibonomial coefficients. Thus we now prove that

$$\frac{F_{m-n+1}}{(F_{m+1},\ F_n)} \Bigg| \begin{Bmatrix} m \\ n \end{Bmatrix} \quad . \tag{7.1}$$

We need to observe that $(a - b, b) = (a, b)$. This follows, e.g., from an easily proved stronger assertion that $(a + c, b) = (a, b)$ when $b \mid c$. This lemma is used to modify the proof given by Hermite for (2.2), as follows. Let $(F_{m+1},\ F_n) = d$. Now, by (6.7) and our lemma,

$$d = (F_{m+1},\ F_n) = F_{(m+1,n)} = F_{(m-n+1,n)} = (F_{m-n+1},\ F_n) = xF_{m-n+1} + yF_n$$

for some integers x, y. Therefore

$$d\ \frac{F_m F_{m-1} \cdots F_{m-n+2}}{F_n F_{n-1} \cdots F_1} = x \begin{Bmatrix} m \\ n \end{Bmatrix} + y \begin{Bmatrix} m \\ n-1 \end{Bmatrix} = E, \text{ some integer,}$$

and by multiplication with F_{m-n+1} we obtain

$$d \begin{Bmatrix} m \\ n \end{Bmatrix} = E \cdot F_{m-n+1} \ ,$$

whence F_{m-n+1}/d is indeed a factor of $\begin{Bmatrix} m \\ n \end{Bmatrix}$.

As a valuable corollary we get the fact that the Fibonomial Catalan numbers are integers; this follows at once from (7.1) by setting $m = 2n$, and noting that $(F_{2n+1},\ F_n) = 1$, so that we have

$$F_{n+1} \Bigg| \begin{Bmatrix} 2n \\ n \end{Bmatrix} \quad . \tag{7.2}$$

The Fibonomial Catalan sequence 1, 1, 3, 20, 364, 17017, 4194036, $\cdots$ generated by

$$\frac{\begin{Bmatrix} 2n \\ n \end{Bmatrix}}{F_{n+1}}$$

is the exact analogue of the familiar Catalan sequence 1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, $\cdots$ generated by

$$\frac{\begin{Bmatrix} 2n \\ n \end{Bmatrix}}{(n+1)}$$

A brief history of the Catalan sequence is given in [1]. A nice proof of (6.7) is given in [9].

8. SOME CONGRUENCES FOR PRIME FIBONACCI NUMBERS

It is not known whether there exist infinitely many Fibonacci numbers which are primes, but we may easily obtain congruences which such primes satisfy.

Let F_m be a prime number. Then $(F_m, F_n) = 1$ for $1 \le n \le m - 1$. Thus from (6.2) we obtain:

(8.1) If F_m = prime, then $F_n \Big| \begin{Bmatrix} m \\ n \end{Bmatrix}$ for $1 \le n \le m - 1$.

This is a Fibonacci analogue of the fact that $p \Big| \binom{p}{k}$ for $1 \le k \le p - 1$ if p is a prime.

Now, it is known [10] that

$$(8.2) \qquad \sum_{k=0}^{m} (-1)^{k(k+1)/2} \begin{Bmatrix} m \\ k \end{Bmatrix} F_{a+1-k}^{m-1} = 0, \quad m \ge 2 .$$

This generalizes such relations as $F_{a+1} - F_a - F_{a-1} = 0$, $F_{a+1}^2 - 2F_a^2 - 2F_{a-1}^2 + F_{a-2}^2 = 0$, etc. See also Hoggatt [7]. Brother Alfred gives a useful table [10] of the Fibonomial coefficients up to $m = 12$. Identity (8.2) may be used with (8.1) to obtain an interesting congruence; for every term in (8.2) is divisible by F_m when F_m is a prime, except the first and last terms. Thus we obtain the congruence:

$$(8.3) \qquad \text{If } F_m = \text{prime, then } F_a^{m-1} \equiv -(-1)^{m(m+1)/2} F_{a-m}^{m-1} \pmod{F_m}, \quad m \ge 2 ,$$

for all integers a. A special case is of interest. Let $a = m + 1$ and we get:

$$(8.4) \qquad \text{If } F_m = \text{prime, then } F_{m+1}^{m-1} \equiv -(-1)^{m(m+1)/2} \pmod{F_m}, \quad m \ge 2 .$$

Another result useful for deriving congruences is the identity

$$(8.5) \qquad \sum_{k=0}^{2m+1} \begin{Bmatrix} 2m+1 \\ k \end{Bmatrix} = \prod_{k=0}^{m} L_{2k}, \quad m \ge 0 ,$$

where the L's are Lucas numbers, defined by $L_0 = 2$, $L_1 = 1$, and $L_{n+1} = L_n + L_{n-1}$. The identity was noted in Problem H-63 of Jerbic [11].

If we apply the extended Hermite theorem (8.1) to this, we obtain:

$$(8.6) \qquad \text{If } F_{2m+1} = \text{prime, then } \prod_{k=0}^{m} L_{2k} \equiv 2 \pmod{F_{2m+1}} .$$

[Continued on page 372.]