

GENERALIZATION OF HERMITE'S DIVISIBILITY THEOREMS AND THE MANN - SHANKS PRIMALITY CRITERION FOR s -FIBONOMIAL ARRAYS

H. W. GOULD
West Virginia University, Morgantown, West Virginia 26506

1. INTRODUCTION

In a previous paper [4] I found that two theorems of Hermite concerning factors of binomial coefficients might be extended to generalized binomial coefficients [2], however one of my proofs imposed severe restrictions on the sequence $\{A_n\}$ used to define the generalized coefficients. Also it was found that the Mann-Shanks primality criterion [6] follows from one of the Hermite theorems and it appeared evident that the criterion also held in the Fibonomial array, but the proof was not completed.

In the present paper I remove all these defects by proving the Hermite theorems in a more elegant manner so that very little needs to be assumed for the generalized array, and the Mann-Shanks criterion is not only proved for the Fibonomial array but for the s -Fibonomial and q -binomial arrays. Some typographical errors in [4] are also corrected.

2. THE GENERALIZED HERMITE THEOREMS

Let $\{A_n\}$ be a sequence of integers with $A_0 = 0$, $A_n \neq 0$ for all $n \geq 1$, and otherwise arbitrary. Define generalized binomial coefficients by

$$(2.1) \quad \binom{n}{k} = \frac{A_n A_{n-1} \cdots A_{n-k+1}}{A_k A_{k-1} \cdots A_1}, \quad \text{with} \quad \binom{n}{0} = 1.$$

These generalize the ordinary binomial coefficients which occur for $A_k = k$ identically. Properties of the array and their history may be found in [2]. Our attention here is fixed on the case when these coefficients are all integers. Arithmetic properties are then of primary concern. As usual, (a, b) will mean the greatest common divisor of a and b , and $a|b$ means a divides b . We may now state:

Theorem 1.

$$(2.2) \quad \frac{A_n}{(A_n, A_k)} \mid \binom{n}{k}$$

and

$$(2.3) \quad \frac{A_{n-k+1}}{(A_{n+1}, A_k)} \mid \binom{n}{k},$$

provided only that in (2.3) we suppose $(A_{n+1}, A_k) | A_{n-k+1}$. Of course, in (2.2) we always have $(A_n, A_k) | A_n$, so that (2.3) is only slightly less general than (2.2).

In [4] I stated that (2.3) holds provided $A_{n+1} - A_k = A_{n+1-k}$ or something close to this. We shall see that no such assumption is necessary.

Proof of (2.2). By the Euclidean algorithm we know that there exist integers x and y such that $(A_n, A_k) = xA_n + yA_k$. Therefore

$$(A_n, A_k) \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = xA_n \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + yA_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = xA_n \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + yA_n \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} = A_n \cdot E,$$

for some integer E . Since $(A_n, A_k) | A_n$ we have proved that (2.2) is true.

Proof of (2.3). Again, for some integers x and y , $(A_{n+1}, A_k) = xA_{n+1} + yA_k$, whence

$$\begin{aligned} (A_{n+1}, A_k) \left\{ \begin{matrix} n \\ k \end{matrix} \right\} &= xA_{n+1} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + yA_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \\ &= xA_{n+1-k} \left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} + yA_{n+1-k} \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\} = A_{n+1-k} \cdot F, \end{aligned}$$

for some integer F . Thus we have proved in general that

$$(2.4) \quad A_{n+1-k} \mid (A_{n+1}, A_k) \left\{ \begin{matrix} n \\ k \end{matrix} \right\},$$

and when we suppose that $(A_{n+1}, A_k) | A_{n+1-k}$ we obtain (2.3).

The proof I tried in [4] motivated by Hermite's own argument ran as follows: We have

$$(A_{n+1}, A_k) = xA_{n+1} + yA_k = x(A_{n+1} - A_k) + (x+y)A_k,$$

whence

$$\begin{aligned} (A_{n+1}, A_k) \left\{ \begin{matrix} n \\ k \end{matrix} \right\} &= x(A_{n+1} - A_k) \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + (x+y)A_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \\ &= x \frac{A_{n+1} - A_k}{A_{n+1-k}} A_{n+1-k} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} + (x+y)A_{n+1-k} \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\}, \end{aligned}$$

and from this, if we suppose that $A_{n+1} - A_k = A_{n+1-k}$, as stated in [4], we could obtain (2.3), because this also implies $(A_{n+1}, A_k) | A_{n+1-k}$. We may also merely suppose that $A_{n+1-k} | A_{n+1} - A_k$ and we shall have proved (2.4), but as seen in our general proof none of these assumptions is necessary. Hermite's device of shifting terms around does not generalize, but then also the shifting is not needed.

In the proof of (2.2) we have used the obvious fact that

$$A_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = A_n \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\},$$

and in our proof of (2.3) we used the obvious relations

$$A_{n+1} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = A_{n+1-k} \left\{ \begin{matrix} n+1 \\ k \end{matrix} \right\} \quad \text{and} \quad A_k \left\{ \begin{matrix} n \\ k \end{matrix} \right\} = A_{n+1-k} \left\{ \begin{matrix} n \\ k-1 \end{matrix} \right\},$$

simple analogues of corresponding formulas for ordinary binomial coefficients.

As our results apply to the Fibonacci numbers, and Fibonomial coefficients, it still seems necessary to know that $(F_a, F_b) = F_{(a,b)}$ if only to get an easy proof that $(F_{n+1}, F_n) | F_{n+1-k}$ so that we can have (2.3) as well as (2.2). Thus we have

$$(F_{n+1}, F_k) = F_{(n+1,k)} = F_{(n+1-k,k)} = (F_{n+1-k}, F_k)$$

which means that $(F_{n+1}, F_k) | F_{n+1-k}$. In any event, our results are obtained more elegantly by our present proofs.

According to Dickson's History [1, p. 265] Th. Schönemann in 1839 proved that

$$(2.5) \quad \frac{(a, b, \dots, m)(a + b + \dots + m - 1)!}{a! b! \dots m!}$$

is an integer. The situation for two integers a, b is just that

$$(2.6) \quad \frac{(a, b)(a + b - 1)!}{a! b!}$$

is an integer. This follows at once from Hermite's original form of (2.2), because by putting

$$H(n, k) = \frac{\binom{n, k}}{n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\},$$

which is an integer, then clearly

$$H(a + b, b) = \frac{(a + b, b)}{a + b} \left\{ \begin{matrix} a + b \\ b \end{matrix} \right\} = \frac{(a, b)(a + b - 1)!}{a! b!}$$

must be an integer. The multinomial extension of Schönemann follows readily from Hermite's theorem. I was reminded of these things by a letter from Gupta [5] who remarked that a nice Fibonomial extension of (2.6) would be that

$$(2.7) \quad \frac{F_{(m, n)} [m + n - 1]!}{[m]! [n]!}$$

is an integer. This, of course, follows at once from (2.2) when $A_n = F_n$ and we define generalized factorials by

$$(2.8) \quad [n]! = A_n A_{n-1} \dots A_2 A_1, \quad \text{with} \quad [0]! = 1.$$

Indeed, the more general assertion from (2.2) is that since

$$H(n, k) = \frac{\binom{A_n, A_k}}{A_n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$$

is an integer, so also is

$$(2.9) \quad H(m + n, n) = \frac{\binom{A_{m+n}, A_n}}{A_{m+n}} \left\{ \begin{matrix} m + n \\ n \end{matrix} \right\} = \frac{\binom{A_{m+n}, A_n} [m + n - 1]!}{[m]! [n]!}$$

an integer.

According to Dickson [1, p. 265] Cauchy also proved Schönemann's theorem for (2.5), and Catalan (1874) proved that (2.6) is an integer in case $(a, b) = 1$.

Catalan, Segner, Euler, etc., found that $(n + 1) \left\{ \begin{matrix} 2n \\ n \end{matrix} \right\}$ by combinatorial or geometrical arguments. See my bibliography [3] for a list of 243 items dealing with the Catalan numbers, ballot numbers, and related matters. A supplement of over 75 items is being prepared.

The fact that $(n + 1) \left\{ \begin{matrix} 2n \\ n \end{matrix} \right\}$ follows at once from (2.3) so that the number

$$(2.10) \quad C(n, k) = \frac{\binom{A_{n+1}, A_k}{A_{n+1-k}}}{\binom{n}{k}}$$

is a natural generalization. Unfortunately, even in the case $A_n = F_n$ we do not yet have a suitable combinatorial interpretation of this number.

3. THE MANN-SHANKS CRITERION FOR FIBONOMIALS

In [4] we gave some alternative formulations of the elegant Mann-Shanks primality criterion [6]. In particular we noted that their beautiful theorem maybe written in the form:

$$(3.1) \quad \left\{ \begin{array}{l} C = \text{prime if and only if } R \mid \binom{R}{C - 2R} \\ \text{for every integer } R \text{ such that } C/3 \leq R \leq C/2, R \geq 1. \end{array} \right.$$

Here R and C are the row and column numbers, respectively, in the original Mann-Shanks shifted binomial array. We showed that when C is a prime the indicated divisibility follows at once from Hermite's form of (2.2).

The corresponding theorem for Fibonomial coefficients (i. e., with $A_n = F_n$ in (2.1)) is also true. That is, we have

Theorem 2. In the Fibonomial coefficient array,

$$(3.2) \quad \left\{ \begin{array}{l} C = \text{prime if and only if } F_R \mid \left\{ \binom{R}{C - 2R} \right\} \\ \text{for every integer } R \text{ such that } C/3 \leq R \leq C/2, R \geq 1. \end{array} \right.$$

Note that the single difference between this and (3.1) is that the row number R must be replaced by the corresponding Fibonacci number F_R . When $C = \text{prime}$, the divisibility follows from (2.2) since this implies that $F_R / (F_R, F_{C-2R})$ is a factor of the Fibonomial coefficient; however we also have

$$(F_R, F_{C-2R}) = F_{(R, C-2R)} = F_{(R, C)} = F_1 = 1$$

when $C/3 \leq R \leq C/2$. Thus, we have only to consider the case when C is composite. Our proof is just a slight modification of the proof given by Mann-Shanks. Suppose $C = 2k$, with $k = 0, 2, 3, 4, \dots$; then the unit $\binom{k}{0} = 1$ always occurs in the column, so divisibility cannot occur, and it is sufficient to consider odd composite C . Let p be an odd prime factor of C , and write $C = p(2k + 1)$, with $k \geq 1$. Choose $R = pk$. Then the coefficient in the R -row and C -column is $\binom{kp}{p}$, and

$$\frac{1}{F_{pk}} \binom{kp}{p} = \frac{F_{pk} \cdot F_{pk-1} \cdot F_{pk-2} \cdot \dots \cdot F_{pk-p+1}}{F_{pk} \cdot F_p \cdot F_{p-1} \cdot \dots \cdot F_1}$$

Cancel F_{pk} with F_{pk} . The factors $F_{p-1}, F_{p-2}, \dots, F_1$ in the denominator cannot affect the possible divisibility of F_p into the numerator since

$$(F_p, F_{p-r}) = F_{(p,p-r)} = F_{(p,r)} = F_1 = 1 \quad \text{for all } 1 \leq r \leq p-1,$$

while on the other hand F_p is relatively prime to every factor in the numerator since

$$(F_p, F_{pk-j}) = F_{(p,pk-j)} = F_{(p,j)} = F_1 = 1 \quad \text{for all } 1 \leq j \leq p-1.$$

and so F_p , which is greater than 1 for odd primes p , cannot divide into the numerator. This means, equivalently, that the row number F_{pk} cannot divide the coefficient $\binom{kp}{p}$. The proof is complete.

Our proof is a modification of the Mann-Shanks argument using the fact again that

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

4. THE MANN-SHANKS CRITERION FOR s-FIBONOMIAL ARRAYS

The s-Fibonomial coefficients follow from (2.1) when we set $A_n = F_{sn}$, s being any positive integer. Our theorem 2 above handles the case $s = 1$. We now have

Theorem 3. In the s-Fibonomial array, the Mann-Shanks criterion is true. That is,

$$(4.1) \quad \left\{ \begin{array}{l} C = \text{prime} \text{ if and only if } \frac{F_{sR}}{F_s} \mid \binom{R}{C-2R}_s \\ \text{for every integer } R \text{ such that } C/3 \leq R \leq C/2, R \geq 1. \end{array} \right.$$

To see the motivation, consider Hermite's extended theorem (2.2) with $A_n = F_{sn}$. We see that $F_{sR} / (F_{sR}, F_{sC-2sR})$ is a factor of the coefficient in the R-C position of the Mann-Shanks type array. But when $C = \text{prime}$ we have

$$(F_{sR}, F_{sC-2sR}) = F_{(sR, sC-2sR)} = F_{(sR, sC)} = F_{s(R, C)} = F_s,$$

since $C = \text{prime}$ implies $(R, C) = 1$ for each $C/3 \leq R \leq C/2, R \geq 1$. Thus (2.2) yields F_{sR} / F_s as a factor. By the way, it is a known fact that $F_s \mid F_{sR}$. To prove the converse case, when C is composite, first assume $C = 2k, k = 0, 2, 3, 4, \dots$. Then again the unit $\binom{k}{0} = 1$ occurs in the column; so that it is sufficient to study the situation for odd composite C . Let p be an odd prime factor of C , and put $C = p(2k+1), k \geq 1$. Choose as before $R = pk$. Then the coefficient in the R-C spot is the s-Fibonomial coefficient $\binom{kp}{p}$. We find now that

$$\frac{F_s}{F_{spk}} \binom{kp}{p}_s = \frac{F_s}{F_{spk}} \frac{F_{spk} \cdot F_{spk-s} \cdot F_{spk-2s} \cdot \dots \cdot F_{spk-sp+s}}{F_{sp} \cdot F_{sp-s} \cdot \dots \cdot F_{3s} F_{2s} F_s}.$$

Cancel F_s and F_{spk} . Now it is easy to see that

$$(F_{sp}, F_{sp-sr}) = F_{(sp, sp-sr)} = F_{(sp, sr)} = F_{s(p, r)} = F_s$$

for all $1 \leq r \leq p - 1$. Also,

$$(F_{sp}, F_{spk-sj}) = F_{(sp, spk-sj)} = F_{(sp, sj)} = F_{s(p, j)} = F_s$$

for all $1 \leq j \leq p - 1$. Remove the common factor F_s throughout. We see now that

$$\left(\frac{F_{sp}}{F_s}, \frac{F_{sp-sr}}{F_s} \right) = 1, \text{ for all } 1 \leq r \leq p - 1,$$

and

$$\left(\frac{F_{sp}}{F_s}, \frac{F_{spk-sj}}{F_s} \right) = 1, \text{ for all } 1 \leq j \leq p - 1.$$

Also, $F_{sp}/F_s > 1$, and we find that F_{sp}/F_s cannot divide the numerator; equivalently we have shown that F_{spk}/F_s cannot divide the s -Fibonomial coefficient so that our proof is complete.

It would appear that a Fibonacci-type property (a homomorphism)

$$(4.2) \quad (A_a, A_b) = A_{(a,b)}$$

would be very useful for proving Mann-Shanks type criteria in general arrays.

5. THE MANN-SHANKS CRITERION FOR q -BINOMIAL ARRAYS

The q -binomial or Gaussian coefficients are defined by

$$(5.1) \quad \begin{bmatrix} n \\ k \end{bmatrix} = \prod_{j=1}^k \frac{q^{n-j+1} - 1}{q^j - 1}, \quad \text{with } \begin{bmatrix} n \\ 0 \end{bmatrix} = 1.$$

They are polynomials in q . Since in fact $(q^a - 1, q^b - 1) = q^{(a,b)} - 1$, it is not surprising now that we can assert the Mann-Shanks criterion for the q -binomial array. The q -analogue of (3.1) is motivated by Hermite's generalized theorem (2.2) for we now have that the coefficient in the R - C position is divisible by

$$\frac{q^R - 1}{(q^R - 1, q^{C-2R} - 1)},$$

which reduces to

$$\frac{q^R - 1}{q - 1}$$

when C is a prime and $C/3 \leq R \leq C/2$, $R \geq 1$. Consequently we are led to the following:

Theorem 4. The Mann-Shanks criterion for primality holds in the q -binomial array. That is:

$$(5.2) \quad \left\{ \begin{array}{l} C = \text{prime if and only if } \frac{q^R - 1}{q - 1} \mid \left[\begin{array}{c} R \\ C - 2R \end{array} \right] \\ \text{for every integer } R \text{ such that } C/3 \leq R \leq C/2, \quad R \geq 1, \\ \text{and where the } q\text{-binomial coefficients are defined by (5.1).} \end{array} \right.$$

The proof is left to the reader.

In each of the cases we have presented in this paper, the first non-trivial instance of the non-divisibility by a row number occurs when $C = 25$. The next case is then $C = 35$. Up to this point a row number fails to divide an array number because of the presence of a unit in the column. $C = 25$ and 35 are the first composite numbers where no unit appears. The next such numbers are 49, 55, 65, 77, 85, 95, corresponding to those numbers of form $6j \pm 1$ which are composite.

The column entries for $C = 25$ in the ordinary Pascal case are 36, 252, 165, 12, with corresponding row numbers 9, 10, 11, 12. 10 fails to divide 252, while the other row numbers divide their column entries. Similarly, for the Fibonomial array, the column entries are 714, 136136, 83215, 144, with row numbers 34, 55, 89, 144. Here 55 fails to divide 136136. In the q -binomial array, the column entries are

$$\frac{(q^9 - 1)(q^8 - 1)}{(q^2 - 1)(q - 1)}, \quad \frac{(q^{10} - 1)(q^9 - 1)(q^8 - 1)(q^7 - 1)(q^6 - 1)}{(q^5 - 1)(q^4 - 1)(q^3 - 1)(q^2 - 1)(q - 1)},$$

$$\frac{(q^{11} - 1)(q^{10} - 1)(q^9 - 1)}{(q^3 - 1)(q^2 - 1)(q - 1)}, \quad \frac{(q^{12} - 1)}{q - 1}.$$

The corresponding row numbers are

$$(q^9 - 1)/(q - 1), \quad (q^{10} - 1)/(q - 1), \quad (q^{11} - 1)/(q - 1), \quad \text{and} \quad (q^{12} - 1)/(q - 1).$$

It is again, of course, the second row number that fails to divide the coefficient in the column. For arrays of the type we are studying this behavior is typical.

The column entries for $C = 35$ in the Pascal array are 12, 715, 3432, 3003, 560, 17, with row numbers 12, 13, 14, 15, 16, 17. Here $14 \nmid 3432$, and $15 \nmid 3003$. For the Fibonomial array the entries are 144, 27372840, 14169550626, 22890661872, 113490195, 1597, with row numbers 144, 233, 377, 610, 987, 1597, and the row numbers 377 and 610 are the ones which fail to divide their corresponding column entries.

6. GENERALIZED MANN-SHANKS CRITERIA

By placing units in the (R, 2R) and (R, 3R) positions in their rectangular array and carefully choosing the other entries (which turned out to be binomial coefficients) Mann and Shanks developed a kind of sieve which tests numbers of the form $6j \pm 1$ for primality. This suggests that there may be ways to devise similar sieves based on other arithmetic progressions. After all, it is a very old theorem of Dirichlet that if $(a, b) = 1$ then there are infinitely many primes of the form $a + bt$, where t ranges over the integers. We might expect then to find a criterion similar to that of Mann-Shanks by using the progressions $4j \pm 1$ for example. Although I have not found any simple formula for generating the entries in an array, I can suggest some obvious necessary properties of such an array, by analogy with the original Mann-Shanks array. Below is presented an outline for such an array:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
0	1																					
1		1	-	1																		
2				1	2	-	2	1														
3						1	3	-	*		-	3	1									
4								1	*		-	4	-	4	-	*	1					
5										1	5	-	5	-	*	-	5	-	5	1		
6												1	6	-	*	-	6	-	6	-	*	
7														1	*	-	7	-	7	-	*	
8																	1	8	-	8	-	*
9																			1	9	-	*
10																					1	*

Numbers listed above are the smallest factors which an entry must have in order to be allowed, so that the row number will divide each entry in a prime column. This guarantees that a prime will correspond to the row-column divisibility property desired. However, of the remaining entries, those spots marked by a dash (-) can be filled arbitrarily, while those marked by a star (*) must be chosen so that at least one of the starred numbers in each column will not be divisible by the row number. Such special column numbers are 9, 15, 21, 25, 27, etc. One may imagine that it would be desirable to have a symmetrical row, in analogy to the binomial coefficients, though this may not be desired. However, it seems worth exploring. The first few rows suggest such symmetry. For this reason, I place a factor of 7 in the R = 7, C = 25 position to preserve symmetry in that row, etc. It would be very remarkable if we could determine simple formulas for generating such generalized Mann-Shanks arrays based on Dirichlet progressions.

In the outline array based on $4j \pm 1$, it is easy to see that the bottom star in the special columns will always occur for row number $(K - 1)/2$, where $K = 4j \pm 1 \neq \text{prime}$. If we choose an entry for that position which is not divisible by the row number and otherwise fill open spots in the array by the row number in any given row, we shall obtain the following array having the Mann-Shanks property:

binomial coefficients, Fibonomial coefficients, or q-binomial coefficients is that they automatically take care of the situation. Nevertheless, it is felt that Theorems 5 and 6 shed further light on the nature of the Mann-Shanks property.

Another intriguing problem would be to find out whether any similar extensions to higher dimensions might be possible, using multinomial coefficients and variations.

7. TYPOGRAPHICAL ERRORS IN PREVIOUS PAPER

In [4] the following errors have been noted: p. 356, in (2.3), for "mod ..." read "(mod ...)" ; p. 359, line 4, for

$$\left(\frac{n-1}{3}\right) \text{ read } \left[\frac{n-1}{3}\right] ;$$

p. 360, lines 6 and 8 from bottom, for "Erdos" read "Erdős"; p. 372, in Ref. 2, for "Institute" read "Institution."

REFERENCES

1. L. E. Dickson, History of the Theory of Numbers, Carnegie Institution, Washington, D.C., Vol. I, 1919. Reprinted by Chelsea Publ. Co., New York, 1952.
2. H. W. Gould, "The Bracket Function and Fontené-Ward Generalized Binomial Coefficients with Application to Fibonomial Coefficients," Fibonacci Quarterly, Vol. 7 (1969), No. 1, pp. 23-40, 55.
3. H. W. Gould, "Research Bibliography of Two Special Number Sequences," Mathematica Monongaliae, No. 12, May, 1971, Morgantown, W. Va. iv + 25 pp.
4. H. W. Gould, "A New Primality Criterion of Mann and Shanks and its Relation to a Theorem of Hermite with Extension to Fibonomials," Fibonacci Quarterly, Vol. 10 (1972), No. 4, pp. 355-364, 372.
5. H. Gupta, Personal Correspondence, 19 March, 1972.
6. Henry B. Mann and Daniel Shanks, "A Necessary and Sufficient Condition for Primality, and its Source," J. Combinatorial Theory, Ser. A, 13 (1972), 131-134.

