DIVISIBILITY OF BINOMIAL AND MULTINOMIAL COEFFICIENTS BY PRIMES AND PRIME POWERS

DAVID SINGMASTER
Polytechnic of the South Bank, London
and
*Istituto Matematico, Pisa, Italy**

1. ABSTRACT AND INTRODUCTION

Questions on the title subject have been raised and answered many times. However, there does not seem to be a place where all this knowledge is gathered together, other than Dickson (*History of the Theory of Numbers*, Vol. I, Chapter 9). It is my intention to give here a systematic presentation of the subject. Much of the material is known, but there is a moderate amount of new formulations and new results.

The main theorem in the subject is that $p^e || \binom{n}{k}$ if and only if e is the number of carries in the addition $k + (n - k) = n$ when done in p-ary arithmetic. The multinomial analog is that $p^e || n!/\Pi k_j!$ if and only if e is the total amount carried in the p-ary addition $\Sigma k_j = n$. The historical background of these results and its relation to Lucas' result will be discussed.

Then the main theorem is used to investigate the following topics:

a) When does $d | \binom{n}{k}$ for $k = 1, 2, \ldots, n - 1$?

b) When does $d \nmid \binom{n}{k}$ for $k = 0, 1, \ldots, n$?

c) Equalities, lower bounds and upper bounds for e in $p^e || \binom{n}{k}$.

For example, we shall see that $p^s | \binom{p^s}{k}$ iff $(k,p) = 1$ and $p^e | \binom{n}{k}$ implies $p^e \leqq n$.

d) The multinomial analogs of a, b, and c.

e) How often does $p || \binom{n}{k}$ or does $p^2 | \binom{n}{k}$ for $k = 0, 1, \ldots, n$?

f) How often does $d | \binom{n}{k}$ for $n = k, k + 1, \ldots$?

Numerous related questions arise in connection with these topics and some unsolved problems occur. Some other related results are discussed afterward. The contents are described in more detail in Section 3, after introducing notations in Section 2.

2. NOTATIONS AND CONVENTIONS

All letters n, k, e, etc., denote nonnegative integers, with p and q being distinct primes, $r \geqq 2$, and (usually) $d > 1$. In general, k is always the bottom term of some binomial coefficient $\binom{n}{k}$ and is always assumed to satisfy $0 \leqq k \leqq n$. Similarly, if we have $\binom{p^s}{k}$, we assume $0 \leqq k \leqq p^s$. The phrases "all k," "some k," etc., will always imply this, unless otherwise specified.

For $r \geqq 2$, we let $\overline{k}$ denote any r-tuple $(k_1, k_2, \ldots, k_r)$ such that $\Sigma k_j = n$ (or whatever the top term of the r-nomial coefficient concerned is). The phrases "all $\overline{k}$," "some $\overline{k}$," etc., will always imply this, unless otherwise specified. We denote the multionomial (or r-nomial) coefficient $n!/\Pi k_j!$ by $M_r(n,\overline{k})$.

Any n has a unique p-ary representation (or expansion)

$$n = \sum_{i=0}^{m} a_i p^i \quad \text{with} \quad 0 \leqq a_i < p.$$

Occasionally, it is convenient to have $a_m \neq 0$. In that case, we must exclude $n = 0$ or let $0 = 0 \cdot p^0$ with $m = 0$. In most cases, we write the sum indefinitely: $n = \Sigma a_i p^i$. We also denote the p-ary expansion by $(a_m, \ldots, a_1, a_0)$ or by $(\ldots, a_i, \ldots, a_1, a_0)$. We let $k = \Sigma b_i p^i$, $n - k = \Sigma c_i p^i$, and $k_j = \Sigma_i b_{ji} p^i$ be the respective p-ary representations. We refer to the positions as the 0th, 1st, ..., ith, etc., so that the ith position (or place) means the place corresponding to p^i and it has i places to its right.

We use $p^e || n$ for $p^e | n$ and $p^{e+1} \nmid n$. Note that $p^0 || n$ means $p \nmid n$. Square brackets [ ] will denote the greatest integer function. We use the ALGOL symbol ↑ to denote exponentiation when the exponent becomes complicated. E.g., we write $n = \Pi p_i \uparrow e_i$.

*This paper was prepared while the author held a research fellowship of the Italian National Research Council (Consiglio Nazionale delle Ricerche).

Definition 1: $E(p,n) = e$ if $p^e || n$.

Definition 2: (A) $f(p,n) = E(p,n!)$.

(B) $e(p,n,k) = E\left(p,\binom{n}{k}\right)$.

(C) $e_r(p,n,\overline{k}) = E\left(p,M_r(n,\overline{k})\right)$.

Clearly, E and e stand for exponent and f is used to avoid too many e's and because it is next to e.

Definition 3: (A) $N(n,d)$ is the number of k such that $d \nmid \binom{n}{k}$.

(B) $N_r(n,d)$ is the number of $\overline{k}$ such that $d \nmid M_r(n,\overline{k})$.

When there is no danger of confusion, we may drop references to p and/or r in $M_r(n,\overline{k})$, $f(p,n)$, $e(p,n,k)$, $e_r(p,n,k)$ and $N_r(n,d)$.

All main items (theorems, definitions, lemmas, and propositions) are numbered consecutively. Corollary 16.1 denotes the first corolllary to item 16. (I hope that those readers who have found a Definition 4 located between Theorem 8 and Lemma 2 or who have tried to locate a Definition 3.1.2.4 will find this system a bit easier to follow.)

3. SUMMARY

With the above notations in hand, we can now give a more precise description of the contents of the paper.

Section 4 will present the main theorem that $e(p,n,k)$ is the number of carries in the p-ary addition $k + (n - k)$, and its multidimensional analog that $e_r(p,n,\overline{k})$ is the total amount carried in the p-ary addition $\Sigma k_j = n$. These will be derived from Legendre's classic results. Then we deduce a necessary and sufficient condition for $p \nmid \binom{n}{k}$ and for $p \nmid M_r(n,\overline{k})$.

Section 5 will discuss the history of the results given in Section 4, in their several forms. The connection with Lucas' congruence will be noted.

In Section 6, we shall determine $N(n,p)$, when $N(n,p) = 2$ and when $N(n,d) = 2$. The final result is that $N(n,d) = 2$ if any only if $d = p$ and $n = p^m$ for some p.

In Section 7, we shall consider $N(n,p^e) = n + 1$ and $N(n,d) = n + 1$. The main result is that $N(n,p^e) = n + 1$ if and only if $n = ap^s - 1$ with $1 \leqq a < p^e$. The related question of determining n such that $\left(d,\binom{n}{k}\right) = 1$ for all k is considered.

Section 8 will give a number of results on the exact value of, or lower or upper bounds for, $e(p,n,k)$, depending on n and k. This will lead us to the determination of

$$\text{GCD}\left\{\binom{n\alpha}{k} \middle| (k,n) = 1\right\} \quad \text{and of} \quad \text{LCM}\left\{\binom{n}{k}\right\}$$

and to results such as:

$$p^s \left| \binom{p^s}{k} \right. \text{ iff } (k,p) = 1;\ p^e \left| \binom{n}{k} \right. \text{ implies } p^e \leqq n;\ \text{and } \frac{n}{(n,k)} \left| \binom{n}{k} \right. .$$

(This section is large and contains many diverse things. I can only give an idea in this short summary.)

In Section 9, we shall find multinomial analogs for most of the results of Sections 6, 7, and 8. The main result of Section 7 is radically different when $r \geqq 3$:

$$N_r(n,d) = \binom{n + r - 1}{r - 1}$$

has only finitely many solutions and all have $n < d$.

Section 10 will cover a number of results on the number of k such that $p || \binom{n}{k}$ and $p^2 || \binom{n}{k}$.

Section 11 will deal with problems on the density of n such that $d \left| \binom{n}{k} \right.$, for $n = k$, $k + 1$, ... The basic result is the theorem of Zabek which gives the period of $\binom{n}{k}$ (mod d) and hence shows that the density being considered does exist. We shall see that the density is $\geqq d^{-1}$, with equality iff $d = p^e$ and $k = p^m$ for some prime p.

In Section 12, a few related topics that occur in the literature are discussed.

The references are intended to be reasonably exhaustive (but not too exhausting).

4. THE MAIN THEOREMS

We first state and sketch two well-known results of Legendre.

Lemma 4: $f(p,n) = f(n) = \sum_{j \geqq 1} [n/p^j]$.

Lemma 5: $f(n) = (n - \Sigma a_i)/(p - 1)$.

Sketch of Proofs: For the first, observe that $[n/p^j]$ counts the number of terms in $n!$ that are divisible by p^j. A term which is exactly divisible by p^e will be counted exactly e times in the sum, once by each $[n/p^j]$ with $1 \leq j \leq e$. For the second, observe that

$$[n/p^j] = a_j + a_{j+1}p + \cdots + a_m p^{m-j};$$

collect terms and simplify. ■

Lemma 4 may be found, usually in more detail, in [41, p. 10; 2, p. 50; 4, p. 25; 22, p. 41; 23, p. 86; 28, p. 342; 38, p. 46; 39, p. 7; 42, p. 90; 44, p. 47; 46, p. 79; 49, p. 117; 50, p. 113; 58, p. 131; 66, p. 99; 67, p. 17]. Lemma 5 may be found in [41, p. 12; 2, p. 55; 4, p. 26; 22, p. 42; 38, p. 49; 39, p. 8; 60; 66, p. 103].

Note that when $p = 2$, Lemma 5 becomes $f(n) = n - \Sigma a_i$ and that Σa_i is simply the number of ones in the binary expansion of n [4, p. 26; 25, p. 158; 38, p. 49].

Theorem 6: $e(p,n,k) = e(n,k)$ is the number of carries in the p-ary addition $k + (n - k)$.

Proof: Applying Lemma 5 to k, $n - k$, and n, we have:

(1) $$e(n,k) = f(n) - f(k) - f(n - k);$$

(2) $$= \Sigma(b_i + c_i - a_i)/(p - 1).$$

Now consider the p-ary addition. Set $\varepsilon_i = 1$ if there is a carry from the ith place and set $\varepsilon_i = 0$ if not. (Let $\varepsilon_{-1} = 0$.) Then

(3) $$a_i + p\varepsilon_i = b_i + c_i + \varepsilon_{i-1}.$$

Hence $\Sigma(b_i + c_i - a_i) = p\Sigma\varepsilon_i - \Sigma\varepsilon_{i-1} = (p - 1)\Sigma\varepsilon_i$ and so $e(n,k) = \Sigma\varepsilon_i$ is the number of carries. ■

Corollary 6.1: $e(n,k)$ is the number of borrows in the p-ary subtraction $n - k$.

Corollary 6.2: For $p = 2$, $e(n,k) = \Sigma b_i + \Sigma c_i - \Sigma a_i$ and Σa_i is the number of ones in the binary representation of n, etc.

Theorem 7: $e_r(p,n,\overline{k}) = e(n,\overline{k})$ is the total amount carried in the p-ary addition $\Sigma k_j = n$.

Proof: Proceeding as before, we get

(4) $$e(n,\overline{k}) = \Sigma_i(\Sigma_j b_{ji} - a_i)/(p - 1)$$

and we have

(5) $$a_i + p\varepsilon_i = \Sigma_j b_{ji} + \varepsilon_{i-1},$$

where ε_i is the amount carried and may be greater than one. Hence, $e(n,\overline{k}) = \Sigma\varepsilon_i$ is the total amount carried. ■

Corollary 7.1: For $p = 2$, $e(n,\overline{k}) = \Sigma_j\Sigma_i b_{ji} - \Sigma_i a_i$.

Proposition 8: $p\nmid\binom{n}{k}$ if and only if $0 \leq b_i \leq a_i$ for all i.

Proof: We have that $p\nmid\binom{n}{k}$ iff $e(n,k) = 0$ iff $a_i = b_i + c_i$ for all i iff $0 \leq b_i \leq a_i$ for all i. (Note that $0 \leq b_i \leq a_i$ for all i implies that $0 \leq k \leq n$.) ■

Proposition 9: $p\nmid M(n,\overline{k})$ if and only if $\Sigma_j b_{ji} = a_i$ for all i.

5. HISTORICAL NOTES

Lemma 4 is due to Legendre [7, p. 263, item 2; 41, p. 10] but is only rarely attributed to him [14; 22, p. 41; 50, p. 113]. Lemma 5 is also due to Legendre [7, p. 263, item 2; 41, p. 12] and is sometimes attributed to him [1; 2, p. 55; 14; 36; 38, p. 49; 60]. Carlitz [3, p. 305] cites Bachmann [2] for Lemma 5, but this is presumably not intended as a primary reference. In general, number theorists all know these results are due to Legendre, especially Lemma 4, but they don't seem to write it down in textbooks. (None of the other sources I have mentioned give any reference for these results. Personally, I think this is a shame.)

Kummer [7, p. 270, item 71; 40, p. 115] gives most of Theorem 6, but he does not identify $\Sigma\varepsilon_i$ as the number of carries. To me, this identification is an important step; it clarifies the equations (3) and it reduces the whole question to simple p-ary arithmetic. I have found only two references to Theorem 6 in its present form, namely Knuth [38, p. 68], who gives it as a problem and cites Kummer, and Simmons [59], who mentions only the case appropriate to Proposition 8. Bachmann [2, p. 60] shows that $\Sigma b_i + \Sigma c_i = \Sigma a_i + (p - 1)\Sigma\varepsilon_i$, but not in a context of binomial coefficients.

On the other hand, Glaisher [17, pp. 353, 357] specifically states Corollary 6.1, although Dickson's reference [7, p. 273, item 92] does not mention it. Dickson gives no references to either Theorem 6 or Corollary 6.1 in their present forms.

Dickson [7, p. 273, item 93; 6, p. 378] has essentially obtained Theorem 7, but without identifying the ε_i or forming their sum or even stating the result. Fray [14, p. 473] notes this and states the result, but does not identify the ε_i as carries.

Modern authors have used Kummer's original form [3, p. 302; 14, p. 470] or other forms, sometimes simply equivalent and sometimes not. If one puts Lemma 4 directly into equation (1), we have one such form:

$$e(n,k) = \sum_{j \geq 1} [n/p^j] - [k/p^j] - [(n-k)/p^j]. \tag{6}$$

See [1; 9; 63]. Another form is simply equation (2) as it stands. See [7, p. 272, item 79; 53; 57]. Corollary 6.2 occurs in [33]. Some complicated forms occur in [24; 26; 36; 43], the first two being related to Glaisher's form, Corollary 6.1.

Theorem 6 is complementary to Lucas' result:

$$\binom{n}{k} \equiv \Pi\binom{a_i}{b_i} \pmod{p},$$

where we set $\binom{a}{b} = 0$ for $b > a$. See [7, p. 271, items 76 and 77; 3; 11; 14; 15; 16; 38, p. 68]. Clearly, Proposition 8 also follows easily from this result. Dickson [7, p. 273, item 90; 5, p. 76[has generalized Lucas' result to multinomial coefficients and derived Proposition 9 from it. Numerous authors have given Proposition 8, usually as a consequence of Lucas' result; see [11; 15; 17, p. 357; 53; 59]. Proposition 9 has been given less often [7, p. 273, item 90; 5; 14, p. 473].

6. WHEN DOES $N(n,d) = 2$?

The topic of this section is to determine when $d \mid \binom{n}{k}$ for $k = 1, 2, \ldots, n-1$. We are only interested in $d > 1$ and $n \geq 1$. Then $d \nmid \binom{n}{0}$ and $d \nmid \binom{n}{n}$ so we always have $N(n,d) \geq 2$ and $d \mid \binom{n}{k}$ for $1 \leq k \leq n-1$ is equivalent to $N(n,d) = 2$.

Proposition 10: $N(n,p) = \Pi(a_i + 1)$.

Proof: This follows easily from Proposition 8. See also [3; 11; 53]. ∎

Corollary 10.1: Setting $p = 2$, the number of odd binomial coefficients in the nth row = $N(n,2) = 2\uparrow(\Sigma a_i)$. (See also [7, p. 274, item 98; 16, p. 156].)

Corollary 10.2: $N(n,p) = 2$ if and only if $n = p^m$. (See also [11; 12; 53].)

Corollary 10.3: Again setting $p = 2$, $\binom{n}{k}$ is even for $1 \leq k \leq n-1$ if and only if $n = 2^m$.

Proposition 11: For $n > 1$, $N(n,pq) > 2$.

Proof: If $N(n,pq) = 2$, then $N(n,p) = N(n,q) = 2$. This would imply that $n = p^m = q^\mu$, which is impossible. Since $N(n,pq) \geq 2$, we must have $N(n,pq) > 2$. ∎

Theorem 12: For $n > 1$, $N(n,p^2) > 2$.

Proof: If $N(n,p^2) = 2$, then $N(n,p) = 2$ and so $n = p^m$. The p-ary expansion of n is $(1, 0, 0, \ldots, 0)$. Let $k = (0, 1, 0, \ldots, 0)$, so $n - k = (0, p-1, 0, \ldots, 0)$. Clearly there is only one carry in the addition of k and $n - k$, so $p^2 \nmid \binom{n}{k}$ and $N(n,p^2) > 2$. See also [12]. ∎

Theorem 13: For $d > 1$ and $n \geq 1$, we have $N(n,d) = 2$ if and only if $n = 1$ or d is a prime p with $n = p^m$ and $m > 0$.

Proof: For $n = 1$, everything is trivial. Let $n > 1$, and suppose $N(n,d) = 2$. By Proposition 11, d cannot have two distinct prime factors. By Theorem 12, d cannot have a square prime factor. Hence $d = p$ and Corollary 10.2 gives us $n = p^m$ and $m > 0$ follows since $n > 1$. The converse is given by Corollary 10.2. ∎

Theorem 13 can be rephrased as saying that the GCD of $\binom{n}{k}$ for $1 \leq k \leq n-1$ can only be a prime p, and then iff $n = p^m$ [7, p. 274, item 98], or as saying that $(a+b)^n \equiv a^n + b^n \pmod{d}$ can hold iff $n = 1$ or $d = p$ with $n = p^m$.

7. WHEN DOES $N(n,d) = n + 1$?

The theme of this section is to partially determine when $d \nmid \binom{n}{k}$ for all k, i.e., when is $N(n,d) = n + 1$, and to solve the related question of when $\left(d, \binom{n}{k}\right) = 1$ for all k. In this section, $n = 0$ is permissible.

Theorem 14: For $e \geqq 1$, $N(n,p^e) = n + 1$ if and only if $n = ap^s - 1$ with $1 \leqq a < p^e$.

Proof: For $n = 0$, everything is trivial, so consider $n > 0$ and suppose $N(n,p^e) = n + 1$. Assume that $n = (a_m, a_{m-1}, \ldots, a_0)$ with $a_m \neq 0$. We claim that $a_i = p - 1$ for $i \leqq m - e$. Consider $k = (a_m - 1, p - 1, p - 1, \ldots, p - 1)$. Then $0 \leqq k \leqq n$. Consider the addition of k and $n - k$. If $a_i < p - 1$, then there must be a carry from the ith position, which creates carries up to one from the $(m - 1)$st position, making a total of $m - i$ carries, so $p^{m-i} | \binom{n}{k}$. So if $N(n,p^e) = n + 1$, then $p^e \nmid \binom{n}{k}$, hence $a_i < p - 1$ implies $m - i < e$, or $i > m - e$, as claimed.

Let $s = \min\{i | a_i \neq p - 1\}$, so that $s > m - e$ and $m - s < e$. Then $n = (a_m, \ldots, a_s, p - 1, \ldots, p - 1)$ with $a_s < p - 1$. Hence, we have $n = (a_m p^{m-s} + \cdots + a_s)p^s + (p^s - 1) = (\alpha + 1)p^s - 1$, where $0 \leqq \alpha < p^e - 1$. So $n = ap^s - 1$ with $1 \leqq a < p^e$, by setting $a = \alpha + 1$.

Conversely, if $n = ap^s - 1$ with $1 \leqq a < p^e$, we let $a - 1 = (\alpha_{e-1}, \ldots, \alpha_0)$. Then $n = (a - 1)p^s + (p^s - 1) = (\alpha_{e-1}, \ldots, \alpha_0, p - 1, \ldots, p - 1)$. For any k, the subtraction $n - k$ can have at most $e - 1$ borrows; hence,

$$p^e \nmid \binom{n}{k} \text{ for all } k. \blacksquare$$

Corollary 14.1: $N(n,p) = n + 1$ if and only if $n = ap^s - 1$, with $1 \leqq a < p$. See [7, p. 274, item 98; 11; 38, p. 483; 53].

Corollary 14.2: Setting $p = 2$, all the binomial coefficients in the nth row are odd if and only if $n = 2^s - 1$. See [16, p. 156; 38, p. 69].

The exact determination of when $N(n,d) = n + 1$ appears intractable for d not a prime power. For example: $N(4, 12) = 5$, but $N(4, 3) = 4$ and $N(4, 4) = 3$. However, we can say the following.

Proposition 15: For any $d > 1$, there are infinitely many n such that $N(n,d) = n + 1$.

Proof: Let $p|d$. Then $N(n,p) = n + 1$ implies $N(n,d) = n + 1$, so we can let $n = ap^s - 1$ with $1 \leqq a < p$. $\blacksquare$

This result is of particular interest, since it fails for multinomial coefficients with $r \geqq 3$.

For the related problem of finding n such that d is relatively prime to each $\binom{n}{k}$, we have an easy solution. If d is a prime power, say $d = p^e$, then the problem is equivalent to finding $N(n,p) = n + 1$ and Corollary 14.1 applies. Otherwise, we have the following.

Theorem 16: Let d have at least two prime divisors. Then there are only a finite number of n such that $\left(d, \binom{n}{k}\right) = 1$ for all k.

Proof: Without loss of generality, we may assume d is square-free and we set $d = \prod p_i$ with $p_1 < p_2 < \ldots$. Then $\left(d, \binom{n}{k}\right) = 1$ for all k if and only if $p_i \nmid \binom{n}{k}$ for all i and k, i.e., $N(n,p_i) = n + 1$ for all i. From Corollary 14.1, we must have $n + 1 = a_i \cdot p_i \uparrow s_i$ with $1 \leqq a_i < p_i$. Now $a_1 < p_1 < p_2$, hence $p_2 \nmid (n + 1)$ and so $n + 1 = a_2 < p_2$ and so $n \leqq p_2 - 2$. $\blacksquare$

In fact, the proof gives a determination of all such n as all numbers of the form $n = a \cdot p_1^s - 1$ with $1 \leqq a < p_1$ and $a \cdot p_1^s < p_2$, since all such numbers have $N(n,p_i) = n + 1$ by Corollary 14.1.

Most of the results of these last two sections are known, but are usually derived via Lucas' result. Theorems 12 and 14 do not follow from Lucas' result, but Theorem 12 can be and has been derived by ad hoc arguments. Theorem 14 does appear to be new, although its corollaries are not. I have not seen Proposition 14 or Theorem 16 before, but their proofs do not require anything new.

8. SOME INEQUALITIES ON $e(p,n,k)$

First we shall consider a few exact determinations of $e(p,n,k) = e(n,k)$. These lead into a number of lower bounds. Combining the lower bounds for various primes will give assertions of divisibility such as $(k,n) = 1$ implies $n | \binom{n}{k}$. Then we consider a few upper bounds. Recall that $e(n,k) = e$ is equivalent to $p^e \| \binom{n}{k}$, hence $e(n,k) \geqq e$ is equivalent to $p^e | \binom{n}{k}$ and $e(n,k) \leqq e$ is equivalent to $p^{e+1} \nmid \binom{n}{k}$.

Proposition 17: If $n = kp^s$, then $e(n,k) = \Sigma c_i/(p - 1)$.

Proof: We have that $\Sigma b_i = \Sigma a_i$, so the result follows from equation (2). ■

Corollary 17.1: Setting $p = 2$ and $s = 1$, we have $e(2k,k) = \Sigma b_i$ is the number of ones in the binary representation of k (or $2k$).

Corollary 17.2: For $k \geqq 1$, $\binom{2k}{k}$ is even; $2 \| \binom{2k}{k}$ if and only if $k = 2^m$; $4 | \binom{2k}{k}$ unless $k = 2^m$.

Theorem 18: Let $n = p^m$ and let $p^t \| k$. (If $k = 0$, set $t = m$.) Then $p^{m-t} \| \binom{n}{k}$.

Proof: We have $n = (1, 0, 0, \ldots, 0)$ and $k = (b_m, \ldots, b_t, 0, 0, \ldots, 0)$, hence there are exactly $m - t$ carries in adding k and $n - k$. ■

Corollary 18.1: $p^m | \binom{p^m}{k}$ if and only if $(k,p) = 1$.

Corollary 18.2: For $0 < k < p^{u+1}$, we have $p^s | \binom{p^{s+u}}{k}$.

Proof: Let $p^t \| k$, so $t \leqq u$. By the theorem, $p^s | p^{s+u-t} \| \binom{p^{s+u}}{k}$. (This corollary will be needed in Section 11.) ■

Corollary 18.3: For $0 < k < p^m$, we have $p | \binom{p^m}{k}$, i.e., $N(p^m,p) = 2$. (See Corollary 10.2.)

We have already moved into considering lower bounds with the above corollaries. We now examine lower bounds more directly.

Theorem 19: Let $p^s | n$ and $p^t \| k$. If $t \leqq s$, then $p^{s-t} | \binom{n}{k}$.

Proof: The argument is a slight modification of that of Theorem 18. ■

Corollary 19.1: If $p^s | n$ and $(k,p) = 1$, then $p^s | \binom{n}{k}$.

Corollary 19.2: For $\nu \geqq 1$, we have $\frac{n}{(n,k)} | \binom{n\nu}{k}$.

Proof: Consider any prime p and let $p^s \| n$ and $p^t \| k$. If $t \geqq s$, then $p \nmid \frac{n}{(n,k)}$ and is irrelevant. If $t < s$, then $p^{s-t} \| \frac{n}{(n,k)}$ and $p^{s-t} | \binom{n\nu}{k}$ by the theorem. ■

Corollary 19.3: If $(k,n) = 1$ and $\nu \geqq 1$, then $n | \binom{n\nu}{k}$.

Corollaries 18.1 and 19.3 (with $\nu = 1$) partially resolve the question of when does $n | \binom{n}{k}$. This problem was posed by Hausmann in 1954 [29] and no answer has been published. The first case not covered by the corollaries is $10 | \binom{10}{4}$. See also [47, p. 86; 7, p. 265, items 18 and 21; 2, p. 62; 4, p. 28; 22, p. 45; 46, p. 82). Gould [20] attributes Corollary 19.2 (with $\nu = 1$) to Hermite, apparently on the basis of [7, p. 272, item 85], while Bachmann [2, p. 62] assigns it to Catalan. However, Dickson [7, p. 265, item 18] makes it clear that the result is due to Schonemann. Gupta [25] has studied the parity of the ratio $\frac{(n,k)}{n}\binom{n}{k}$ and asserts that his method applies to the study of its divisibility by any prime.

Corollary 19.4: For $(b,k) = 1$, we have $(ak + b) | \binom{ak + b}{k}$; in particular, $(ak + 1) | \binom{ak + 1}{k}$, and $((a - 1)k + 1) | \binom{ak}{k}$. Setting $a = 2$ gives $k + 1 | \binom{2k}{k}$.

The ratios $\binom{2k}{k}/(k + 1) = \binom{2k + 1}{k}/(2k + 1)$ are known as Catalan or Segner numbers (although due to Euler). They occur often in combinatorial problems, particularly as the number of ways of associating $k + 1$ terms. See [27, p. 25; 38, pp. 239, 531-533; 45, pp. 140-152; 52, p. 101, and elsewhere (see his index); 69, p. 154; 21; 48], the last two giving numerous other references.

Theorem 20: For $n > 1$, let $n = \Pi p_i\uparrow e_i$ and let $p_i\uparrow f_i \| \nu$. Then $\text{GCD}\left\{\binom{n\nu}{k} \mid (k,n) = 1\right\} = \Pi p_i\uparrow(e_i + f_i)$. (Recall that $0 \leq k \leq n\nu$, by convention.)

Proof: We have $(p_i\uparrow(e_i + f_i)) \mid n\nu$ and $(k,n) = 1$ implies $(k,p_i) = 1$, so that $(p_i\uparrow(e_i + f_i)) \mid \binom{n\nu}{k}$ for all such k by Corollary 19.1. Hence $\Pi p_i\uparrow(e_i + f_i) \mid \text{GCD}$. On the other hand, $\text{GCD} \mid \binom{n\nu}{1} = n\nu$ and $(p_i\uparrow(e_i + f_i)) \| n\nu$, so no higher power of p_i can divide the GCD. Further, the only other primes which can enter into the GCD are primes p such that $p \mid \nu$ and $p \neq p_i$ for each i. Consider such a prime p and let $p^e \| \nu$, so $p^e \| n\nu$ and $p^e \neq n\nu$ (since $n > 1$). Hence $n\nu = (a_m, \ldots, a_e, 0, 0, \ldots, 0)$ with $a_e \neq 0$. Setting $k = p^e = (0, \ldots, 1, 0, 0, \ldots, 0)$, we have $0 \leq k \leq n$, $(k,n) = 1$, and $p \nmid \binom{n}{k}$ by Proposition 8. Hence, $p \nmid \text{GCD}$. ■

The case $n = 2$ is solved in [64] using a special argument only suitable for $n = 2$ instead of the second half of the above proof.

The next theorem is complementary to Theorem 19.

Theorem 21: Let $p^s \| n + 1$ and let $p^t \mid k + 1$. If $t \geq s$, then $p^{t-s} \mid \binom{n}{k}$.

Proof: We have $n = (a_m, \ldots, a_s, p - 1, p - 1, \ldots, p - 1)$ with $a_s \neq p - 1$ and $k = (b_m, \ldots, b_t, p - 1, p - 1, \ldots, p - 1)$. Hence $n - k$ has at least $t - s$ borrows. ■

Corollary 21.1: If $(k + 1, n + 1) = 1$, then $k + 1 \mid \binom{n}{k}$.

Corollary 21.2: $k + 1 \mid \binom{2k}{k}$. (See also Corollary 19.4.)

The proofs of Theorems 19 and 21 can be somewhat generalized to give the following two results.

Proposition 22: Let $p^s \mid n - \alpha$ and $p^t \| k - \alpha$ where $0 \leq \alpha < p^t$ and $t \leq s$. Then $p^{s-t} \mid \binom{n}{k}$.

Proposition 23: Let $p^s \| n + \alpha$ and $p^t \mid k + \alpha$ where $0 < \alpha \leq p^s$ and $t \geq s$. Then $p^{t-s} \mid \binom{n}{k}$.

Note that Proposition 22, with $\alpha = 0$, is Theorem 19 and that Proposition 23, with $\alpha = 0$, is Theorem 21. However, these are the only two simple applications of the propositions.

Now we consider some upper bounds on $e(p,n,k) = e(n,k)$. We now assume that $n = (a_m, \ldots, a_0)$ has $a_m \neq 0$, i.e., $p^m \leq n < p^{m+1}$. For $n = 0$, we take $m = 0$.

Theorem 24: Let $p^t \mid k$. (For $k = 0$, set $t = m$.) Then $e(n,k) \leq m - t$.

Proof: We have $n = (a_m, \ldots, a_t, \ldots, a_0)$ and we have $k = (b_m, \ldots, b_t, 0, 0, \ldots, 0)$. Hence, there can be at most $m - t$ borrows in $n - k$. ■

Note that Theorems 19 and 24 imply Theorem 18.

Corollary 24.1: For $n > 0$ and any k, $e(n,k) \leq m$. Hence, $p^e \mid \binom{n}{k}$ implies $p^e \leq p^m \leq n$.

See [1; 9; 63] for proofs using equation (6) and [57] for a proof using equation (2). The special case, that $p^e \mid \binom{2k}{k}$ implies $p^e \leq 2k$, occurs often in prime number theory [23, p. 103; 28, p. 342; 42, p. 105; 44, p. 60; 46, p. 165; 58, p. 133].

Corollary 24.1 can also be derived as a consequence of Theorem 14, as $p^e \mid \binom{n}{k}$ implies $N(n,p^e) < n + 1$ and the least such n is the least n not of the form $ap^e - 1$ with $1 \leq a < p^e$, which is p^e.

Corollary 24.2: For $1 < k < n - 1$, $\binom{n}{k}$ is never a prime power. (See [30; 57; 63].)

Proof: If $\binom{n}{k} = p^e$, then $p^e \mid \binom{n}{k}$, hence $p^e \leq n = \binom{n}{1} < \binom{n}{k}$. ■

Erdös and others [10 and its references and its review] have considered the question of whether $\binom{n}{k}$ can be a power for $1 < k < n - 1$. For $3 < k < n - 3$, Erdös has shown that $\binom{n}{k}$ is never a power, but the situation for $k = 2$ and $k = 3$ does not yet appear to be fully resolved.

The next theorem is the complement of Theorem 24.

Theorem 25: Assume $p^m \leq n + 1 < p^{m+1}$ and $p^s \| n + 1$. Then, for any k, $e(n,k) \leq m - s$ and equality can hold.

Proof: Write $n + 1 = \alpha p^s$, where $p^{m-s} \leqq \alpha < p^{m+1-s}$. Then $n = (\alpha - 1)p^s + (p^s - 1) = (a_m, \ldots, a_s, p - 1, p - 1, \ldots, p - 1)$. Hence, there can be at most $m - s$ carries for any k. Note that $a_m = 0$ may occur, but only if $m = s$ and $\alpha = 1$. Also note that $a_s \neq p - 1$. If $m = s$, then equality holds for any k. If $m > s$, then equality holds for $k = (b_m, \ldots, b_s, \ldots, b_0)$ if and only if $a_s < b_s < p$, $a_i \leqq b_i < p$ for $s < i < m$, and $0 \leqq b_m < a_m$. Such k are readily found. ■

Corollary 25.1: $\text{LCM}\left\{\binom{n}{k}\right\} = \frac{1}{n+1} \Pi_p p\uparrow[\log_p(n + 1)] = \frac{1}{n+1} \Pi_p p\uparrow\left[\frac{\log(n + 1)}{\log p}\right]$.

Meynieux [43] has considered this LCM.

Corollary 25.2: $\text{Max}_k\{e(n,k)\} = e$ if and only if $n = ap^s - 1$ with $p \nmid a$ and $p^e \leqq a < p^{e+1}$.

The form of Corollary 25.2 is clearly reminiscent of Theorem 14. In fact, Theorems 14 and 25 each imply the other. Theorems 24 and 25 do not seem to have generalizations similar to Propositions 22 and 23. The reader may convince himself that Theorems 19, 21, 24, and 25 give all the bounds on $e(n,k)$ which arise in the four cases when n ends in more (or less) zeros (or p - 1's) than k.

9. MULTINOMIAL ANALOGS

In this section, we shall obtain multinomial analogs for most of the results of Sections 6, 7, and 8. In many cases, the analog is straightforward or only requires some greater care in the statement, e.g., the condition $(k,n) = 1$ must be replaced by $\text{GCD}\{k_j\} = 1$. If the reader has forgotten the conventions for the multinomial case, he should review Section 2, Theorem 7 and Proposition 9. We shall place the number(s) of the binomial analog(s) in parentheses after the results in this section.

First, we need the following basic combinatorial fact.

Lemma 26: A nonnegative integer n can be partitioned into an ordered sum of r nonnegative integers in $\binom{n + r - 1}{r - 1}$ ways.

For proofs, see [27, p. 5; 58, p. 402]. This is the same as the number of ways of distributing n objects into r distinct cells [51, p. 92], which is the same as the number of n-combinations of r things, with repetition [45, p. 59; 51, p. 6].

Corollary 26.1: There are $\binom{n + r - 1}{r - 1}$ r-nomial coefficients of rank n.

Proposition 27 (10): $N_r(n,p) = \Pi\binom{a_i + r - 1}{r - 1}$.

Corollary 27.1 (10.1): Setting $p = 2$, the number of odd r-nomial coefficients of rank n is $N_r(n,2) = r\uparrow(\Sigma a_i)$.

Corollary 27.2 (10.2): $N_r(n,p) = r$ if and only if $r = p^m$.

The r-nomial coefficients contain $\binom{r}{2}$ copies of the binomial coefficients, corresponding to setting all but two k_j's equal to zero, and they contain r bounding axes of ones, corresponding to setting all but one k_j equal to zero. We shall refer to these bounding axes as the edges. Consequently, for $n \geqq 1$, we have $N_r(n,d) \geqq r$ and $N_r(n,d) = r$ implies that $N(n,d) = N_2(n,d) = 2$.

Corollary 27.3 (10.3): Again setting $p = 2$, $M(n,\overline{k})$ is even except at the edges if and only if $n = 2^m$.

Theorem 28 (11, 12, 13): For $n \geqq 1$ and $d > 1$, the following are equivalent:

(a) $N_r(n,d) = r$.
(b) $N_2(n,d) = 2$.
(c) Either $n = 1$ or d is a prime p with $n = p^m$ and $m > 0$.

Proof: (a) implies (b) by the discussion above. (b) implies (c) by Theorem 13. (c) implies (a) by Corollary 27.2. ■

Now we ask when can $N_r(n,d) = \binom{n + r - 1}{r - 1}$. This implies that $N_2(n,d) = n + 1$, but not conversely. For example, consider $r = 3$ and $p = 2$. Let $n = 3 = 2^2 - 1$, so that $N_2(n,p) = n + 1$. But $2 \mid \frac{3!}{1!1!1!}$, and so $N_3(n,p) \neq \binom{n + r - 1}{r - 1}$. In fact, for $r \geqq 3$, this question has a radically different solution than for $r = 2$.

Theorem 29 (14, 15): For $d > 1$ and $r \geqq 3$, $N_r(n,d) = \binom{n+r-1}{r-1}$ implies that $n < d$.

Proof: Let $n_1 = n - k_1$ and $n_2 = n_1 - k_2$. Then we have

$$(7) \qquad M(n,\overline{k}) = \frac{n!}{k_1!k_2! \ldots k_r!} = \binom{n}{k_1}\binom{n_1}{k_2}\frac{n_2!}{k_3! \ldots k_r!}.$$

By varying the k_j's, we can let n_1 and k_2 be any integers such that $0 \leqq k_2 \leqq n_1 \leqq n$. In particular, we can take $k_2 = 1$. Hence, $N_r(n,d) = \binom{n+r-1}{r-1}$ implies that $d \nmid n_1$ for $n_1 = 2, 3, \ldots, n$. Hence, $n < d$. ■

Corollary 29.1 (14.1): For $r \geqq 3$, $N_r(n,p) = \binom{n+r-1}{r-1}$ if and only if $0 \leqq n < p$.

Corollary 29.2 (14.2): For $p = 2$ and $r \geqq 3$, all r-nomial coefficients of rank n are odd if and only if $n = 0$ or $n = 1$.

The exact determination of when $N_r(n,d) = \binom{n+r-1}{r-1}$ seems awkward, but may perhaps be easier for $r \geqq 3$ than for $r = 2$.

Corollary 29.3 (16): If $r \geqq 3$ and $d = \Pi p_i \uparrow e_i$ with $p_1 < p_2 < \ldots$, then $(d,M(n,\overline{k})) = 1$ for all $\overline{k}$ if and only if $0 \leqq n < p_1$.

The converse of Theorem 29 need not hold, even for $r = 3$. Let $r = 3$, $d = p^e = 9$, and $n = 6$. Then $9|\frac{6!}{2!2!2!}$, so $N_r(n,d) \neq \binom{n+r-1}{r-1}$. I shall discuss this more fully at the end of the section.

Now we consider inequalities for $e_r(p,n,\overline{k}) = e(n,\overline{k})$. Proposition 17 can be generalized in several ways, but I shall give only two.

Proposition 30 (17.1): Let $r = p$ and let all $k_j = k = \Sigma b_i p^i$, so that $n = pk$. Then $e(pk,\overline{k}) = \Sigma b_i$ is the sum of the digits in the p-ary expansion of k (or n).

Corollary 30.1 (17.2): For $k \geqq 1$, we have $p|(pk)!/(k!)^p$ and $p||(pk)!/(k!)^p$ if and only if $n = p^m$.

Theorem 31 (17.1): Let $k_j = k = \Sigma b_i p^i$ for all j, so that $n = rk$. Then $e(rk,\overline{k}) \geqq f(r) \cdot \Sigma b_i$.

Proof: Consider the addition in p-ary arithmetic. In the ith place, we have $\Sigma_j b_{ji} + \varepsilon_{i-1} = rb_i + \varepsilon_{i-1}$. This produces a carry to the $(i + 1)$st place of at least $[rb_i/p] + [\varepsilon_{i-1}/p]$ and this produces a carry to the $(i + 2)$nd place of at least $[rb_{i+1}/p] + [rb_i/p^2] + [\varepsilon_{i-1}/p^2]$, etc. Hence,

$$\Sigma\varepsilon_i \geqq \Sigma_i\left(\sum_{j \geqq 1} [rb_i/p^j]\right) = \Sigma_i f(rb_i) \geqq \Sigma_i b_i f(r). \blacksquare$$

Corollary 31.1 (17.2): If $\Sigma b_i \geqq \alpha$ for all primes $p \leqq r$, then $(r!)^\alpha|(rk)!/(k!)^r$. (Note that $\alpha \geqq 1$.) See [7, p. 266, item 28; 2, p. 57; 42, p. 92; 46, p. 81; 66, p. 103].

The argument used in Theorem 18 fails to generalize to the multinomial case because a carry can now have a value greater than one. In general, this fact prevents us from obtaining any useful upper bounds. However, we do have some nice lower bounds.

Theorem 32 (19): Let $p^s|n$ and $(p\uparrow t_j)||k_j$. Set $t = \min\{t_j\}$. If $t \leqq s$, then $p^{s-t}|M(n,\overline{k})$.

Proof: Suppose, without loss of generality, that $t = t_1$. Then $p^{s-t}|\binom{n}{k_1}|M(n,\overline{k})$, using equation (7). ■

Corollary 32.1 (19.1): If $p^s|n$ and $(k_j,p) = 1$ for some j, then $p^s|M(n,\overline{k})$.

Corollary 32.2 (19.2): For $\nu \geqq 1$, we have $\frac{n}{\mathrm{GCD}\{t_j\}}|M(n\nu,\overline{k})$. See [7, p. 265, item 18].

Corollary 32.3 (19.3): If $\mathrm{GCD}\{t_j\} = 1$ and $\nu \geqq 1$, then $n|M(n\ ,\overline{k})$. See [16, p. 103; 22, p. 46; 46, p. 82]. Obviously the question of when does $n|M(n,\overline{k})$ is even more unsolved than $n|\binom{n}{k}$.

Corollary 32.4 (19.4): $rk + 1|(rk + 1)!/(k + 1)!(k!)^{r-1}$, hence $k + 1|(rk)!/(k!)^r$.

One can write down numerous similar consequences of 32.3.

Proposition 33 (20): For $n > 1$, let $n = \Pi p_i{\uparrow}e_i$ and let $p_i{\uparrow}f_i \,||\, \nu$. Then $\mathrm{GCD}\{M(n,\overline{k}) \mid \mathrm{GCD}\{k_j\} = 1\} = \Pi p_i{\uparrow}(e_i + f_i)$.

Theorem 34 (21): Let $p^s || n + 1$ and let $(p{\uparrow}t_j) \mid (k_j + 1)$. Set $t = \max\{t_j\}$. If $t \geqq s$, then $p^{t-s} \mid M(n,\overline{k})$.

Proof: As for Theorem 32. ■

Corollary 34.1 (21.1): If $(k_j + 1, n + 1) = 1$ for some j, then $k_j + 1 \mid M(n,\overline{k})$.

Corollary 34.2 (21.2): $k + 1 \mid (rk)!/(k!)^r$. (See 32.4.)

Versions of Propositions 22 and 23 can be stated, but do not seem useful. I have not been able to obtain any useful upper bounds, but one can still obtain the analog of 24.2.

Proposition 35 (24.2): If $1 < k_j < n - 1$ for some j, then $M(n,\overline{k})$ is not a prime power.

Proof: From equation (7) and symmetry, we have that $\binom{n}{k_j} \mid M(n,\overline{k})$ for all j. From Corollary 24.2, if $M(n,\overline{k})$ is a prime power, we must have $k_j = 0,\ 1,\ n - 1$ or n for each j. ■

I have not seen any work on the general problem of whether $M(n,\overline{k})$ can be a power.

We have obtained Proposition 35, which is the analog of Corollary 24.2, but we have not obtained a multinomial analog of Theorem 24 or of Corollary 24.1. In fact, since $9 \mid \frac{6!}{2!2!2!}$, the obvious analog of 24.1 does not hold. In [61], I have given a method for finding the least n such that $p^e \mid M(n,\overline{k})$ for some $\overline{k}$, i.e., the least n such that $N_r(n,p^e) \neq \binom{n+r-1}{r-1}$. For $p \geqq r$, the method gives the following simple result. For $e \geqq 1$, let $e = s(r - 1) + \beta$ with $0 < \beta \leqq r - 1$. Then the least n such that $N_r(n,p^e) \neq \binom{n+r-1}{r-1}$ is $n = \beta p^{s+1}$.

The exact determination of when $N_r(n,p^e) = \binom{n+r-1}{r-1}$ appears to be very messy.

10. DETERMINATION OF $N(n,p^2)$, ETC.

We now return to the ordinary binomial case and use the main Theorem 6 to determine the number of k such that $p \,||\, \binom{n}{k}$. This number is simply $N(n,p^2) - N(n,p)$, so that we can then determine $N(n,p^2)$, since $N(n,p)$ is known from Proposition 10.

Theorem 36: $N(n,p^2) - N(n,p) = N(n,p)\sum\left(\frac{p}{a_i + 1} - 1\right)\left(1 - \frac{1}{a_{i+1} + 1}\right)$.

Proof: As remarked above, the left-hand side is the number of k such that $p \,||\, \binom{n}{k}$, that is, such that $k + (n - k)$ has exactly one carry. If this carry occurs at the ith place, we have that there is exactly one carry if and only if $a_i < b_i < p$, $0 \leqq b_{i+1} < a_{i+1}$ and $0 \leqq b_j \leqq a_j$ for $j \neq i,\ i + 1$. There are

$$(p - a_i - 1)a_{i+1}\prod_{j\neq 1,i+1}(a_j + 1) = N(n,p)\left(\frac{p}{a_i + 1} - 1\right)\left(1 - \frac{1}{a_{i+1} + 1}\right)$$

ways of doing this. Adding this for all i gives the theorem. ■ See [3, p. 303; 53].

Corollary 36.1: Let $p = 2$ and let w be the number of pairs $(a_{i+1},a_i) = (1,0)$ in the binary representation of n. Then $N(n,4) - N(n,2) = N(n,2)w/2$ and $N(n,4) = N(n,2)(1 + w/2)$.

The argument of the theorem can be extended to obtain the following results, which we only state.

Proposition 37:

$$N(n,p^3) - N(n,p^2) = N(n,p)\sum\left(\frac{p}{a_i + 1} - 1\right)\left(\frac{p + 1}{a_{i+1} + 1} - 1\right)\left(1 - \frac{1}{a_{i+2} + 1}\right)$$
$$+ N(n,p)\sum_{i+1<j}\left(\frac{p}{a_i + 1} - 1\right)\left(1 - \frac{1}{a_{i+1} + 1}\right)\left(\frac{p}{a_j + 1} - 1\right)\left(1 - \frac{1}{a_{j+1} + 1}\right).$$

See [53].

Corollary 37.1: Let $p = 2$. In the binary expansion of n, let w_1 be the number of triples $(a_{i+2}, a_{i+1}, a_i) = (1,0,0)$; let w_2 be the number of triples $(a_{i+2}, a_{i+1}, a_i) = (1,1,0)$; and let w_3 be the number of quadruples $(a_{j+1}, a_j, a_{i+1}, a_i) = (1,0,1,0)$ with $j > i + 1$. Then $N(n,8) - N(n,4) = N(n,2)(w_1 + (w_2 + w_3)/4)$.

A multinomial analog for Theorem 36 seems very difficult to express. One must determine the number of ways $p + a_i = \Sigma_j b_{ji}$ subject to $0 \leqq b_{ji} < p$.

11. RESULTS FOR k FIXED, n VARYING

Thus far, we have been concerned with k (or n and k) varying. Now we hold k fixed and let n vary; that is, we look at the diagonals of Pascal's triangle, rather than at the rows. We no longer have a finite set of values for n and so we cannot reasonably ask for the number of n with some property, say $p \nmid \binom{n}{k}$. However, one can ask for the density of such n. The basic theorem for this study is due to Zabek [70, p. 42] and determines the period of the sequence $\binom{n}{k}$ (mod p^e) as $n = k, k + 1, \ldots$. We give the proof of Trench [65], somewhat simplified by use of our previous results. In this section, we shall always take $k > 0$, except in one discussion.

Theorem 38: Let $k = \sum_{i=0}^{m} b_i p^i = (b_m, \ldots, b_0)$ with $b_m \neq 0$. (That is, $p^m \leqq k < p^{m+1}$.) Then the sequence of residues $\binom{n}{k}$ (mod p^e) for $n = k, k + 1, \ldots$, is periodic with minimal period p^{m+e}.

Proof: Let $x = p^{m+e}$. Then $\binom{n + x}{k}$ is a polynomial $f(x)$ of degree k. Let $\Delta f(x) = f(x + 1) - f(x)$ be the usual forward difference operator and let $\Delta^j f(x)$ be the iterates. For $f(x) = \binom{n + x}{k}$, we have $\Delta f(x) = \binom{n + x + 1}{k} - \binom{n + x}{k} = \binom{n + x}{k - 1}$ and $\Delta^j f(x) = \binom{n + x}{k - j}$. By Newton's formula,

$$f(x) = \sum_{j=0}^{k} \Delta^j f(0) \binom{x}{j} = \sum_{j=0}^{k} \binom{n}{k - j}\binom{x}{j}.$$

Now $j \leqq k < p^{m+1}$, so Corollary 18.2 gives us $p^e \mid \binom{p^{e+m}}{j}$, i.e., $p^e \mid \binom{x}{j}$, for $0 < j \leqq k$. Hence $f(x) = \binom{n + x}{k} \equiv \binom{n}{k}$ (mod p^e) and so $x = p^{m+e}$ is a period.

Now let $n = p^{m+e} + k - p^m = (1, 0, \ldots, 0, b_m - 1, b_{m-1}, \ldots, b_0)$ and let $n_1 = n + p^{m+e+1} = (1, 1, 0, \ldots, 0, b_m - 1, b_{m-1}, \ldots, b_0)$. Examining the subtractions $n - k$ and $n_1 - k$ shows that $p^e \| \binom{n}{k}$ while $p^{e-1} \| \binom{n_1}{k}$, hence p^{m+e-1} is not a period and so p^{m+e} is the minimal period. ■ See also [14, p. 479].

Corollary 38.1: For $d > 1$, let $d = \Pi p_i \uparrow e_i$. For each i, let $p_i \uparrow (m_i + 1) > k \geqq p_i \uparrow m_i$. Then $\binom{n}{k}$ (mod d) is periodic with minimal period $\Pi p_i \uparrow (m_i + e_i)$.

Definition 39: Given $d > 1$, let $d^* = d^*(k,d)$ be the minimal period of $\binom{n}{k}$ (mod d) as given in Corollary 38.1.

Note that $d^*(k,d)$ is (weakly) multiplicative in d by virtue of Corollary 38.1. Further, $d = d^*$ if and only if $p_i > k$ for each i. If d has r distinct prime factors, then $d^* > k^r$.

Definition 40: Let

$A(k,d)$ be the number of residue classes n (mod d^*) such that $d \nmid \binom{n}{k}$;

$B(k,d)$ be the number of residue classes n (mod d^*) such that $d \mid \binom{n}{k}$;

$C(k,d)$ be the number of residue classes n (mod d^*) such that $\left(d, \binom{n}{k}\right) = 1$; and let

$A^*(k,d) = A(k,d)/d^*$; $B^*(k,d) = B(k,d)/d^*$; $C^*(k,d) = C(k,d)/d^*$ be the corresponding densities.

Proposition 41:

(a) $B(k,d) = d^* - A(k,d)$; $B^*(k,d) = 1 - A^*(k,d)$.
(b) $B(k,d)$, $C(k,d)$, $B^*(k,d)$ and $C^*(k,d)$ are (weakly) multiplicative in d.

(c) $C(k,p) = A(k,p)$; $C^*(k,p^e) = C^*(k,p) = A^*(k,p)$; $C(k,p^e) = p^{e-1}C(k,p)$.

Theorem 42: For $k = \sum_{i=0}^{m} b_i p^i$ with $b_m \neq 0$, we have $A(k,p) = \prod_{i=0}^{m} (p - b_i)$ and so $A^*(k,p) = \prod(1 - b_i/p)$.

Proof: From Proposition 8, we know that $p \nmid \binom{n}{k}$ if and only if $b_i \leqq a_i < p$ for each i. Since $\binom{n}{k}$ is periodic (mod p) with period p^{m+1}, we need only consider $0 \leqq i \leqq m$, so there are $\prod_{i=0}^{m} (p - b_i)$ choices for n (mod p^{m+1}). Hence, $A^*(k,p) = \prod_{i=0}^{m} (p - b_i)/p = \prod(1 - b_i/p)$, where the last product is indefinite, since $i > m$ gives $1 - b_i/p = 1$. ■

We note that we can now determine $C(k,d)$ and $C^*(k,d)$.

Corollary 42.1: For $p = 2$, $A^*(k,2) = 1/(2\uparrow\Sigma b_i) = 1/N(k,2)$.

One may interpret $A^*(0,d) = 1$, for $d > 1$, which agrees with the formula for A^* in Theorem 42. Conversely, $A^*(k,p) = 1$ can only occur for $k = 0$. So, for $k > 0$, the maximal value of $A^*(k,p)$ is $1 - 1/p$.

Corollary 42.2: For $k > 0$, we have $A^*(k,p) \leqq 1 - 1/p$, i.e., $B^*(k,p) \geqq 1/p$, with equality if and only if $k = p^m$.

Corollary 42.3: For $k > 0$ and m as above, we have $A^*(k,p) \geqq 1/p^{m+1}$, i.e., $B^*(k,p) \leqq 1 - 1/p^{m+1}$, with equality if and only if $k = p^{m+1} - 1$.

In fact, since $\binom{k}{k} = 1$, we always know at least one residue class $n \equiv k$ (mod p^{m+1}) such that $p \nmid \binom{n}{k}$. From the Corollary, this is the only one when $k = p^{m+1} - 1$. For example:

$$2 \nmid \binom{n}{3} \text{ if and only if } n \equiv 3 \pmod 4.$$

We can extend the above inequalities by some simple analysis.

Proposition 43: $B(k,d) \geqq k$.

Proof: Consider the k values: $n = d \cdot k! + i$, for $i = 0, 1, \ldots, k - 1$. Then $d \mid \binom{n}{k}$ for all these n. Further, $k < d^*$, so these values are all distinct (mod d^*). ■

Corollary 43.1:

(a) $B^*(k,p^e) \geqq k/p^{m+e}$.
(b) $B^*(k,p^e) \geqq 1/p^e$ with equality only if $k = p^m$.
(c) $B^*(k,d) \geqq 1/d$ with equality only if $d = p^e$, $k = p^m$.

Proposition 44: $B(p^m,p^e) = p^m$.

Proof: We have $k = p^m = (0, \ldots, 0, 1, 0, \ldots, 0)$. Consider $n \equiv (a_{m+e-1}, \ldots, a_m, \ldots, a_0)$. Then $p^e \mid \binom{n}{k}$ if and only if $a_m = a_{m+1} = a_{m+2} = \cdots = a_{m+e-1} = 0$. There are exactly p^m such values. ■

Corollary 44.1:

(a) $B^*(k,p^e) = 1/p^e$ if and only if $k = p^m$.
(b) $B^*(k,d) = 1/d$ if and only if $d = p^e$ and $k = p^m$.

Proposition 45: $B^*(k,p^e) \leqq 1 - 1/p^{m+1}$ with equality if and only if $e = 1$ and $k = p^{m+1} - 1$.

Proof: First we have $B^*(k,p^e) \leqq B^*(k,p) \leqq 1 - 1/p^{m+1}$ by Corollary 42.3. If equality holds, it must also hold on the right and so $k = p^{m+1} - 1 = (0, p - 1, \ldots, p - 1)$. Consider $n = (p - 1, 0, p - 1, \ldots, p - 1)$. Then $p \| \binom{n}{k}$. Hence, for $e \geqq 2$, $B^*(k,p^e) < B^*(k,p^2) < B^*(k,p) \leqq 1 - 1/p^{m+1}$. ■

I have not been able to find the appropriate form of this result for $B^*(k,d)$. However, for $C^*(k,d)$, we do have a result.

Proposition 46: Let $d = \prod p_i \uparrow e_i$, let $p_i \uparrow (m_i + 1) > k \geqq p_i \uparrow m_i$ and let $d' = \prod p_i$. Then we have $C^*(k,d) = C^*(k,d') = \prod C^*(k,p_i) = \prod A^*(k,p_i) \geqq \prod 1/(p_i(m_i + 1)) = 1/d^*(k,d')$ with equality if and only if $d = p^e$ and $k = p^{m+1} - 1$. See [59; $\bar{\bar{8}}$].

Proposition 47: $A^*(k,p^2) - A^*(k,p) = A^*(k,p)\sum\left(\frac{p}{p - b_i} - 1\right)\left(1 - \frac{1}{p - b_{i+1}}\right)$.

Corollary 47.1: Let $p = 2$ and let w be the number of pairs $(b_{i+1},b_i) = (0,1)$ in the binary expansion of k. Then

$$A^*(k,4) - A^*(k,2) = A^*(k,2)w/2$$

and

$$A^*(k,4) = A^*(k,2)(1 + w/2).$$

Most of the material in this section, after Zabek's Theorem (Theorem 38), seems to be new, and I feel that there is room for improvement and extension of it. I am not sure what the proper multinomial analogs are.

12. OTHER RESULTS IN THE LITERATURE

In this section, I shall discuss a number of topics related to the subject of this paper, but either too complex or too distant to consider in full detail.

The pattern of the binomial coefficients divisible by an integer d is rather pretty. S. Rösch has published three articles on these patterns [54; 55; 56], the latter two using colors. I sometimes find these, or similar, patterns useful in visualizing theorems.

Fine [11] has shown that the density of binomial coefficients divisible by a prime p is one. One can prove this fairly easily using Proposition 10. On the basis of numerical evidence, Rösch conjectured [54; 56] that the density of coefficients divisible by any integer d is one. Using Theorem 6, I have shown this [62] by showing that p^e divides "almost all" binomial coefficients, using four different senses of "almost all." These include showing that $N(n,p^e)/(n + 1)$ and $A^*(k,p^e)$ both converge in mean to zero.

Sylvester, Schur, and then Erdös [9] have shown that for $n > 2k$, there is a prime p dividing $\binom{n}{k}$ with $p > k$. I do not see that the material of this paper is useful in attacking this type of problem, despite the apparent connection.

Lucas' congruence, mentioned in Section 5, has been generalized by Kazandzidis [36, p. 3] and I have given a simple proof in [60]. The result is that

$$\binom{n}{k} \equiv (-p)^e \prod \frac{a_i!}{b_i!c_i!} \pmod{p^{e+1}}$$

where $e = e(p,n,k)$. This extends readily to multinomial coefficients and to arbitrary ratios of factorials. The analogous result for $n!$ was given by Stickelberger [7, p. 263, items 4, 7, 8; 38, p. 50]:

$$n! \equiv (-p)^f \Pi a_i! \pmod{p^{f+1}}$$

where $f = f(p,n)$.

A problem which has been extensively studied is when a ratio of factorials is an integer. If $\Sigma n_j = \Sigma k_j = n$, then the ratio $\Pi n_j!/\Pi k_j!$ can be expressed as a ratio of multinomial coefficients and we can apply Theorem 7. Another approach is to extend the concept of $p^e||a$ to $p^e||a/b$, allowing $e < 0$. If we set each $n_j = \Sigma_i a_{ji}p^i$, we can obtain

$$e = e(\overline{n},\overline{k}) = \left(\sum_{j,i} b_{ji} - \sum_{j,i} a_{ji}\right)/(p - 1)$$

by arguing as in Theorem 7. Hence, in this case where $\Sigma n_j = \Sigma k_j$, then the ratio $\Pi n_j!/\Pi k_j!$ is an integer iff $\Sigma a_{ji} \leqq \Sigma b_{ji}$ for every prime p.

The problem of when does $n\left|\binom{n}{k}\right.$ can be rephrased in this form as: When is $\frac{(n-1)!1!}{k!(n-k)!}$ an integer? Hence, the above discussion gives an answer to this problem, but not a very satisfactory one. Dickson [7, pp. 295-269] gives a number of other forms, e.g., the following are always integers:

$$\frac{(2a)!(2b)!}{a!b!(a+b)!} \quad \text{and} \quad \frac{(4a)!(4b)!}{a!b!(2a+b)!(a+2b)!}.$$

See also [2, p. 63; 4, p. 27; 22, p. 45; 42, p. 92; 46, p. 81; 66, p. 103].

A number of authors have considered generalized binomial coefficients [13; 14; 18; 19; 20; 31; 32; 35; 68] defined by

$$\binom{n}{k}_A = \frac{A_nA_{n-1}\cdots A_1}{A_k \cdots A_1A_{n-k}\cdots A_1}, \text{ with } \binom{n}{0}_A = \binom{n}{n}_A = 1.$$

In general, even if the A_i are integers, $\binom{n}{k}_A$ may not be integers. Remarkably, if $A_n = F_n$

is the nth Fibonacci number (with $F_1 = F_2 = 1$), then the generalized binomial ("Fibonomial") coefficients are integers (see [31]). One also has generalized multinomial coefficients.

I have only seen one paper which treats the divisibility of such coefficients by primes and prime powers, namely Fray [14]. In it, he considers the case when

$$A_n = q^n - 1 \text{ (or } A_n = (q^n - 1)/(q - 1))$$

which gives the q-binomial coefficients of Jackson [34; see the references of 68]. He obtains analogs of Lemma 5, Kummer's form of Theorem 6, Dickson's unstated form of Theorem 7, Proposition 9, Lucas' result, Proposition 10, and Theorem 38. He also observes and states the results for the ordinary case. He establishes that for any n, the least d^* such that

$$\binom{n + d^*}{k} \equiv \binom{n}{k} \pmod{p^e} \text{ for } 0 \leqq k \leqq n \text{ is } d^* = d^*(n,p^e),$$

a result which is in a somewhat different direction than Theorem 38.

Gould [20] mentions the generalized and the Fibonomial forms of Corollary 19.2 (with $\nu = 1$).

13. ADDENDUM

While this draft was being prepared and typed, several items became available to me. These include some articles which I had previously only known via references, reviews, or memory, and some articles which have only just appeared. This addendum will briefly discuss these articles and the changes to be made in a later version of this paper. The references [A1], etc., refer to the addendum to the references.

Gould [19] gives more detailed information and references on generalized binomial coefficients than I have indicated in Section 12. He remarks that the q-binomial coefficients date back to Causs and Cauchy, prior to Jackson.

Gould has now published [A1], the paper announced in [20]. He again attributes Corollary 19.2 (with $\nu = 1$) to Hermite, referring to [7, p. 272]. He attributes the multinomial analog to Ricci [A4], although it is due to Schönemann [7, p. 264, item 18]. He also considers the following equivalent form of Corollary 19.2 (with $\nu = 1$):

$$\frac{n - k + 1}{(n + 1,k)} \Big| \binom{n}{k}.$$

He gives simple proofs based on $(n,k) = na + kb$. He gives a number of variations and special cases of this type of divisibility relation and extends many of them to Fibonomial coefficients.

Gupta [24] also shows the form of Theorem 6 given in [6] of Section 2, part of Corollary 14.1, and part of Theorem 13. His paper [A2] is an earlier and alternate version of [25].

Sato [A4] has obtained the results of Stickelberger and Kazanzidis discussed in Section 12.

14. REFERENCES

1. H. L. Abbot, P. Erdos, & D. Hanson. "On the Number of Times an Integer Occurs as a Binomial Coefficient." *American Math. Monthly* (to appear).
2. P. Bachmann. *Niedere Zahlentheorie*. Vol. I. Leipzig: B. G. Teubner, 1902.
3. L. Carlitz. "The Number of Binomial Coefficients Divisible by a Fixed Power of a Prime." *Rend. Circ. Mat. Palermo* (II) 16 (1967):229-320. MR 40, #2554.
4. R. D. Carmichael. *The Theory of Numbers and Diophantine Analysis*. New York: Dover, 1959.
5. L. E. Dickson. "The Analytic Representation of Substitutions of a Prime Number of Letters with a discussion of the Linear Group." *Ann. of Math.* 11 (1896-97):65-120.
6. L. E. Dickson. "Theorems on the Residues of Multinomial Coefficients with Respect to a Prime Modulus." *Quarterly J. Pure Appl. Math.* 33 (1901-2):378-384.
7. L. E. Dickson. *History of the Theory of Numbers*. Vol. I. New York: Chelsea, 1952.
8. D. Drazin. "Complements and Comments." *American Math. Monthly* 77 (1970):1078-1079.
9. P. Erdös. "A Theorem of Sylvester and Schur." *J. London Math. Soc.* 9 (1934):282-288.
10. P. Erdös. "On a Diophantine Equation." *J. London Math. Soc.* 26 (1951):176-178. MR 12, p. 804.
11. N. J. Fine. "Binomial Coefficients Modulo a Prime." *American Math. Monthly* 54 (1947): 589-592. MR 9, p. 331.
12. O. M. Fomenko. "Sur quelques propriétés des coefficients binomiaux." *Mathesis* 69 (1960):291-293. MR 25, #5030.
13. G. Fontené. "Généralisation d'une formule connue." *Nouvelles Annales de Mathématiques* (4) 15 (1915):112.

14. R. D. Fray. "Congruence Properties of Ordinary and q-Binomial Coefficients." *Duke Math. J.* 34 (1967):467-480. MR 35, #4151.

15. R. D. Fray. "Solution of Problem E2205: Consequences of a Lucas Congruence." (Proposed by S. M. Farber, D. W. Walkup, and R. J. B. Wets.) *American Math. Monthly* 77 (1970):889-890.

16. J. W. L. Glaisher. "On the Residue of a Binomial-Theorem Coefficient with Respect to a Prime Modulus." *Quarterly J. Pure Appl. Math.* 30 (1899):150-156.

17. J. W. L. Glaisher. "On the Residue with Respect to p^{n+1} of a Binomial-Theorem Coefficient Divisible by p^n." *Quarterly J. Pure Appl. Math.* 30 (1899):349-360.

18. H. W. Gould. "The Bracket Function, q-Binomial Coefficients and Some New Stirling Number Formulas." *The Fibonacci Quarterly* 5 (1967):401-423. MR 37, #1262.

19. H. W. Gould. "The Bracket Function and Fontené-Ward Generalized Binomial Coefficients with Applications to Fibonomial Coefficients." *The Fibonacci Quarterly* 7 (1969):23-40, 55. MR 39, #4021.

20. H. W. Gould. "A New Primality Criterion of Mann and Shanks and Its Relation to a Theorem of Hermite." *Notices Amer. Math. Soc.* 16 (1971):551-552. Abstract 71T-A75.

21. H. W. Gould. *Research Bibliography of Two Special Number Sequences.* Mathematica Monongaliae, No. 12. Department of Mathematics, West Virginia University, Morgantown, W. Va., 1971. MR 43, #4755.

22. H. Griffin. *Elementary Theory of Numbers.* New York: McGraw-Hill, 1954.

23. E. Grosswald. *Topics From the Theory of Numbers.* New York: Macmillan, 1966.

24. H. Gupta. "On the p-Potency of $G(n,r)$." *Proc. Indian Acad. Sci.* Sect. A 1 (1935):620-622.

25. H. Gupta. "On a Problem in Parity." *Indian J. Math.* 11 (1969):157-163. MR 41, #5283.

26. H. Gupta. "Reviewer's Remarks." *Math. Reviews* 40 (1970):467, #2554.

27. M. Hall, Jr. *Combinatorial Theory.* Waltham, Mass.: Blaisdell, 1967.

28. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers.* 4th ed. Oxford: Oxford University Press, 1960.

29. B. A. Hausmann. "Problem E1145." *American Math. Monthly* 61 (1954):712.

30. F. Hering. "Eine Beziehung zwischen Binomialkoeffizienten und Primzahlpotenzen." *Arch. Math.* (Basel) 19 (1968):411-412. MR 38, #1010.

31. V. E. Hoggatt, Jr. "Fibonacci Numbers and Generalized Binomial Coefficients." *The Fibonacci Quarterly* 5 (1967):383-400. MR 37, #6193.

32. V. E. Hoggatt, Jr., & D. A. Lind. "A Power Identity for Second-Order Recurrent Sequences." *The Fibonacci Quarterly* 4 (1966):274-282. MR 34, #128.

33. F. T. Howard. "A Combinatorial Problem and Congruences for the Rayleigh Function." *Proc. Amer. Math. Soc.* 26 (1970):574-580. MR 42, #1756.

34. F. H. Jackson. "q-Difference Equations." *American J. Math.* 32 (1910):305-314.

35. D. Jarden & T. Motzkin. "The Product of Sequences with a Common Linear Recursion Formula of Order 2." *Riveon Lematematika* 3 (1949):25-27. (Hebrew; English summary.) MR 10, p. 698. Reprinted in English in: D. Jarden, "Recurring Sequences," *Riveon Lematematika* (Jerusalem) (1958):42-45.

36. G. S. Kazandzidis (Γ. Σ. Καζαντζιδου). "On a Congruence and on a Practical Method for Finding the Highest Power of a Prime Which Divides the Binomial Coefficient $\binom{A}{B}$" [Περι μιασ ισοτιμιασ και περι ενοσ πρακτικου κανονοσ δια χην ευρεσιν τησ ανωτατησ δυναμεωσ του πρωτου p τησ διαιρουσησ τον διωνυμικον συντελεστην $\binom{A}{B}$]. *Bull. Soc. Math. Grèce* (NS) 6 (1965):358-360. MR 34, #7440.

37. G. S. Kazandzidis. "Congruences on the Binomial Coefficients." *Bull. Soc. Math. Grèce* (NS) 9 (1968):1-12. MR 42, #182.

38. D. E. Knuth. *The Art of Computer Programming.* Vol. I: *Fundamental Algorithms.* World Student Series Edition. Reading, Mass.: Addison-Wesley, 1972.

39. M. Kraitchik. *Introduction a la théorie des nombres.* Paris: Gauthier-Villars, 1952.

40. E. E. Kummer. "Uber die Ergänzungssätze zu den allgemeinen Reciptocitätsgesetzen." *J. Reine Angew. Math.* 44 (1852):93-146.

41. A. M. Legendre. *Théorie des nombres.* Vol. I. 3rd ed. Paris: Didot Freres, 1830.

42. W. J. LeVeque. *Topics in Number Theory.* Vol. I. Reading, Mass.: Addison-Wesley, 1956.

43. R. Meynieux. "Sur le plus petit commun multiple des coefficients du polynôme $(1 + z)^n$ et celui de certains de ces coefficients." *C. R. Acad. Sci. Paris* Sér A 271 (1970):861-864. MR 42, #5892.

44. T. Nagell. *Introduction to Number Theory.* 2nd ed. New York: Chelsea, 1964.

45. I. Niven. *Mathematics of Choice*. New York: Random House, 1965. (New Mathematical Library, No. 15.)

46. I. Niven & H. S. Zuckerman. *An Introduction to the Theory of Numbers*. New York: John Wiley & Sons, 1960.

47. C. S. Ogilvy. *Tomorrow's Math*. 2nd ed. New York: Oxford University Press, 1972.

48. E. T. Ordman. "Algebraic Characterization of Some Classical Combinatorial Problems." *American Math. Monthly* 78 (1971):961-970.

49. O. Ore. *Invitation to Number Theory*. New York: Random House, 1967. (New Mathematical Library, No. 20.)

50. H. Rademacher. *Lectures on Elementary Number Theory*. New York: Blaisdell, 1972.

51. J. Riordan. *An Introduction to Combinatorial Analysis*. New York: John Wiley & Sons, 1958.

52. J. Riordan. *Combinatorial Identities*. New York: John Wiley & Sons, 1968.

53. E. G.-Rodeja F. "Una Propiedad de los Coefficientes Binomicos." *Rev. Mat. Hisp.-Amer.* (4) 24 (1964):250-253. MR 31, #78.

54. S. Rösch. "Expedition in unerforschtes Zahlenland." *Neues Universum* 79 (1962):93-98.

55. S. Rösch. "Farbenlehre, auf die Mathematik angewandt." 1964. (This is either a pamphlet or a reprint from an unidentifiable journal.) Available from the author, 633 Wetzlar, Philosophenweg 2, West Germany.

56. S. Rösch. "Neues vom Pascal-Dreieck." *Bild der Wissenschaft* 9 (1965):758-762.

57. H. Scheid. "Die Anzahl der primfaktoren in $\binom{n}{k}$. *Arch. Math.* (Basel) 20 (1969):581-582. MR 41, #146.

58. W. Sierpinski. *Elementary Theory of Numbers*. Translated by A. Hulanicki. Warszawa: Państwowe Wydawnictwo Naukowe, 1964.

59. G. J. Simmons. "Some Results Concerning the Occurrence of Specified Prime Factors in $\binom{n}{r}$. *American Math. Monthly* 77 (1970):510-511. MR 42, #4476.

60. D. Singmaster. "Notes on Binomial Coefficients—I: A Generalization of Lucas' Congruence" (to appear).

61. D. Singmaster. "Notes on Binomial Coefficients—II: The Least n Such That p^e Divides an r-Nomial Coefficient in the nth Plane" (to appear).

62. D. Singmaster. "Notes on Binomial Coefficients—III: Any Integer Divides Almost All Binomial Coefficients" (to appear).

63. W. Stahl. "Bemerkung zu einer Arbeit von Hering." *Arch. Math.* (Basel) 20 (1969):500. MR 41, #145.

64. St. Olaf College Students. "Solution of Problem E2227." (Proposed by N. S. Mendelsohn.) *American Math. Monthly* 78 (1971):201.

65. W. F. Trench. "On Periodicities of Certain Sequences of Residues." *American Math. Monthly* 67 (1960):652-656. MR 23A, #2365.

66. J. V. Uspensky & M. A. Heaslet. *Elementary Number Theory*. New York: McGraw-Hill, 1939.

67. I. M. Vinogradov. *An Introduction to the Theory of Numbers*. Translated by H. Popova. London: Pergamon Press, 1955.

68. M. Ward. "A Calculus of Sequences." *American J. Math.* 58 (1936):255-266.

69. M. B. Wells. *Elements of Combinatorial Computing*. Oxford: Pergamon Press, 1971.

70. S. Zabek. "Sur la périodicité modulo m des suites de nombres $\binom{n}{k}$. *Ann. Univ. Mariae Curie-Sklodowska* Sect. A 10 (1956):37-47. MR 20, #1653.

15. ADDENDUM TO REFERENCES

A1. H. W. Gould. "A New Primality Criterion of Mann and Shanks and Its Relation to a Theorem of Hermite with Extension to Fibonomials." *The Fibonacci Quarterly* 10 (1972):355-365, 372.

A2. H. Gupta. "On the Parity of $(n + m - 1)!(n,m)/n!m!$." *Res. Bull. Panjab Univ.* (N.S.) 20 (1969):571-575. MR 43, #3201.

A3. G. Ricci. "Sui coefficienti binomiali e polinomiali. Una dimostrazione del teorema di Staudt-Clausen sui numeri di Bernoulli." *Giorn. Mat. Battaglini* 69 (1931):9-12.

A4. S. Sato. "Some Properties on p-Adic Expansions of Natural Numbers." *Res. Bull. Fac. Ed. Oita Univ.* 3 (1970):1-4. MR 44, #145.

*****

A MATRIX GENERATION OF FIBONACCI IDENTITIES FOR F_{2nk}

VERNER E. HOGGATT, JR.
San Jose State University, San Jose, CA 95192
and
MARJORIE BICKNELL-JOHNSON
Wilcox High School, Santa Clara, CA 95051

A series of identities involving even-subscripted Fibonacci numbers and binomial coefficients are derived in this paper by means of a sequence of special 2 x 2 matrices. We begin with the simplest case.

Let $R = \begin{pmatrix} 3 & 1 \\ -1 & 0 \end{pmatrix}$ and the characteristic equation, of course, is $x^2 - 3x + 1 = 0$, which is related to the recursion formula for the alternate Fibonacci numbers. By induction, one can easily establish that, for all integers n,

$$R^n = \begin{pmatrix} F_{2n+2} & F_{2n} \\ -F_{2n} & -F_{2n-2} \end{pmatrix},$$

and, if the auxiliary matrix $S = \begin{pmatrix} 2 & 1 \\ -1 & -1 \end{pmatrix}$, then

$$R^nS = \begin{pmatrix} F_{2n+3} & F_{2n+1} \\ -F_{2n+1} & -F_{2n-1} \end{pmatrix},$$

where F_n is the nth Fibonacci number defined by $F_{n+1} = F_n + F_{n-1}$, $F_1 = F_2 = 1$. Since R satisfies its own characteristic equation, $R^2 - 3R + I = 0$ or $(R + I)^2 = 5R$, which leads to

$$(1) \qquad R^m(R + I)^{2n} = 5^nR^{n+m},$$

$$(2) \qquad R^m(R + I)^{2n}S = 5^nR^{n+m}S,$$

$$(3) \qquad R^m(R + I)^{2n+1} = 5^nR^{n+m}(R + I),$$

$$(4) \qquad R^m(R + I)^{2n+1}S = 5^nR^{n+m}(R + I)S.$$

We use the binomial theorem to rewrite equation (1) and equate elements in the upper right from equations (1) and (2), which gives us

$$\sum_{k=0}^{2n} \binom{2n}{k} R^{k+m} = 5^nR^{n+m},$$

$$(1') \qquad \sum_{k=0}^{2n} \binom{2n}{k} F_{2k+2m} = 5^nF_{2n+2m},$$

$$(2') \qquad \sum_{k=0}^{2n} \binom{2n}{k} F_{2k+2m+1} = 5^nF_{2n+2m+1}.$$

Similarly, from equations (3) and (4), we can obtain

$$(3') \qquad \sum_{k=0}^{2n+1} \binom{2n+1}{k} F_{2k+2m} = 5^n(F_{2n+2m+2} + F_{2n+2m}) = 5^nL_{2n+2m+1},$$

$$(4') \qquad \sum_{k=0}^{2n+1} \binom{2n+1}{k} F_{2k+2m+1} = 5^n(F_{2n+2m+3} + F_{2n+2m+1}) = 5^nL_{2n+2m+2},$$

where L_n is the nth Lucas number defined by $L_{n+1} = L_n + L_{n-1}$, $L_1 = 1$, $L_2 = 3$.

The equations above can be simplified still further. Equations (1′) and (2′) can be combined by letting $p = 2m$ in (1′) and $p = 2m + 1$ in (2′), and noting that p takes on any integral value, we write, finally,