COLLOQUIUM MATHEMATICUM

VOL. LX/LXI DÉDIÉ À M. ANTONI ZYGMUND 1990

THE NUMBER OF BINOMIAL COEFFICIENTS IN RESIDUE CLASSES MODULO p AND p^2

BY

WILLIAM A. WEBB (PULLMAN, WASHINGTON)

Introduction. What can be said about the distribution of binomial coefficients modulo m? By the Chinese Remainder Theorem it usually suffices to consider $m = p^s$ where p is a prime. Most work so far has been for $s = 1$ and small values of p, in particular the case $m = 2$ has been extensively studied [1], [5]–[10]. When the binomial coefficients are arranged into Pascal's triangle we find that the number of odd entries in row r is 2^{n_1} where n_1 is the number of ones in the base 2 expansion of r. Thus, the number of elements which are congruent to 1 modulo 2 depends only on the number of ones in the base 2 expansion of r, not on where they occur nor on the number of zeros.

Let $N(r, m, a)$ denote the number of elements of the rth row of Pascal's triangle which are congruent to a modulo m, where $0 \leq a < m$. The problem of determining the total number of such elements in rows zero through r is essentially equivalent, although not as convenient for our purposes. Also, the latter problem is sometimes considered only for special values of r such as $r = m^h$ [11].

Explicit formulas for $N(r, m, a)$ become increasingly complicated as m grows larger. Formulas for the primes $m = 3$ and 5 are given in [7] and for the prime power $m = 4$ in [3]. An expression for $N(r, p, a)$ is also obtained in [7]. Also, the following interesting result is mentioned. It is an extension of the fact that $N(r, 2, 1)$ depends on only the number of ones in the base 2 expansion of r.

THEOREM 1. *If p is a prime and $1 \leq a < p$, then $N(r, p, a)$ depends only on the number of occurrences of each nonzero digit d in the base p expansion of r and not on where they occur nor on the number of zeros in the expansion.*

For example, $N(r, 3, 1) = 2^{n_1 - 1}(3^{n_2} + 1)$ and $N(r, 3, 2) = 2^{n_1 - 1}(3^{n_2} - 1)$ where n_i is the number of digits i in the base 3 expansion of r.

The number $N(r, p, 0)$ does not satisfy such a nice relation. Of course if $N(r, p, a)$ is known for each $a \neq 0$, then $N(r, p, 0)$ is easily obtained. The general question of what power of p divides $\binom{r}{t}$ is quite old. It is well known for example that $p^a || \binom{r}{t}$ where a is the number of borrows needed when the subtraction $r - t$ is done in base p [10]. Recently, the total number of such binomial coefficients has been studied in [11].

In the next section, we give a simple proof of Theorem 1 using Lucas' Theorem and generalize it to $N(r, p^2, a)$. In the final section, we derive another formula for $N(r, p, a)$ for an arbitrary prime p.

Lucas' Theorem and $N(r, p^s, a)$. One of the most beautiful results concerning binomial coefficients is Lucas' Theorem [4], [5]. For any positive integer r let $r = r_k p^k + r_{k-1} p^{k-1} + \ldots + r_0 = r_k r_{k-1} \ldots r_0$, $r_k > 0$, be the base p representation of r. Similarly for $t \le r$, $t = t_k t_{k-1} \ldots t_0$, where we now allow $t_k = 0$ if necessary. With the usual interpretation that $\binom{r_i}{t_i} = 0$ if $t_i > r_i$, we have

LUCAS' THEOREM. *If p is a prime then*

$$\binom{r}{t} \equiv \binom{r_k}{t_k}\binom{r_{k-1}}{t_{k-1}} \cdots \binom{r_0}{t_0} \pmod{p}.$$

Thus, $p \nmid \binom{r}{t}$ if and only if $0 \le t_i \le r_i$, for $i = 0, 1, \ldots, k$. Furthermore, the number of binomial coefficients $\binom{r}{t}$ which are congruent to a given value a modulo p is the number of ways the t_i can be chosen so that

$$\binom{r_k}{t_k}\binom{r_{k-1}}{t_{k-1}} \cdots \binom{r_0}{t_0} \equiv a \pmod{p},$$

which in turn depends only on the number of r_i in each nonzero residue class modulo p and not on where they occur. This establishes Theorem 1.

The primary goal in this section is to extend Theorem 1 to residues modulo p^2. A generalized form of Lucas' Theorem appearing in [2] will be used. Although the generalized version applies to any power of a prime p, we need only the following form.

THEOREM 2. *If p is a prime then*

$$\binom{r}{t} \equiv \binom{r_k r_{k-1}}{t_k t_{k-1}}\binom{r_{k-1} r_{k-2}}{t_{k-1} t_{k-2}} \cdots \binom{r_1 r_0}{t_1 t_0}\binom{r_{k-1}}{t_{k-1}}^{-1}\binom{r_{k-2}}{t_{k-2}}^{-1} \cdots \binom{r_1}{t_1}^{-1} \pmod{p^2}$$

where

$$\binom{r_i}{t_i} = p \quad \text{if } t_i > r_i, \quad \binom{r_i r_{i-1}}{t_i t_{i-1}} = p \quad \text{if } r_i = t_i \text{ and } t_{i-1} > r_{i-1},$$

$$\binom{r_i r_{i-1}}{t_i t_{i-1}} = p\binom{r_{i-1}}{t_{i-1}} \quad \text{if } t_i > r_i.$$

Thus, for example, if we write numbers in base $p = 5$:

$$\begin{aligned}\binom{13342}{1421} &\equiv \binom{13}{1}\binom{33}{14}\binom{34}{42}\binom{42}{21}\binom{3}{1}^{-1}\binom{3}{4}^{-1}\binom{4}{2}^{-1} \\ &\equiv \binom{13}{1}\binom{33}{14}5\binom{4}{2}\binom{42}{21}\binom{3}{1}^{-1}5^{-1}\binom{4}{2}^{-1} \\ &\equiv \binom{13}{1}\binom{33}{14}\binom{42}{21}\binom{3}{1}^{-1} \equiv 13\cdot 40\cdot 12\cdot 32 \equiv 30 \pmod{100}.\end{aligned}$$

(In base 10 this means $\binom{1097}{236} \equiv 15 \pmod{25}$.)

The case $p = 2$ was solved in [3], where explicit formulas for $N(r,4,a)$ are obtained.

$$N(r,4,1) = \begin{cases} 2^{n_1} & \text{if } n_{11} = 0, \\ 2^{n_1-1} & \text{if } n_{11} > 0, \end{cases}$$
$$N(r,4,2) = n_{10}2^{n_1-1},$$
$$N(r,4,3) = \begin{cases} 0 & \text{if } n_{11} = 0, \\ 2^{n_1-1} & \text{if } n_{11} > 0, \end{cases}$$

where n_B = number of blocks B in the base 2 representation of r.

These results suggest that in general $N(r,p^2,a)$ should depend on only the number of occurrences of each nonzero digit or pair of digits in the base p expansion of r. However, this is not the case. We will prove the following extension of Theorem 1.

THEOREM 3. *If p is a prime and $p \nmid a$ then $N(r,p^2,a)$ depends only on the number of occurrences of each block of nonzero digits in the base p expansion of r and not on where they occur nor on the number of zeros in the expansion.*

EXAMPLE. Let $p = 3, r_1 = 1210222, r_2 = 2220121$ and $r_3 = 12100222$. We have $N(r_i,9,1) = 40$, $N(r_i,9,2) = 92$, $N(r_i,9,4) = 36$, $N(r_i,9,5) = 36$, $N(r_i,9,7) = 88$ and $N(r_i,9,8) = 32$, for $i = 1,2,3$.

Note that in the example above the two digit blocks 10 and 02 appear in r_1 but the reversed blocks 01 and 20 appear in r_2. Nonetheless, each residue a not divisible by 3 occurs equally often.

Proof of Theorem 3. Note first that $\binom{a0}{b0} \equiv \binom{a}{b} \pmod{p^2}$ for any nonnegative integers a and b written in base p. If we expand

$$\binom{a0}{b0} = \binom{pa}{pb} = \frac{(pa)(pa-1)\dots(pa-pb+1)}{(pb)(pb-1)\dots 1}$$

and collect all the terms divisible by p and simplify, we obtain $\binom{pa}{pb} = \binom{a}{b}Q$ where Q is a product of factors each of the form

$$(r_1 + sp)(r_2 + sp)\dots(r_{p-1} + sp)/r_1 r_2 \dots r_{p-1}$$

where the r_i form a reduced residue system modulo p and s is some positive integer. It suffices to show that each such factor is congruent to 1 modulo p^2. The numerator of each factor is

$$r_1 r_2 \dots r_{p-1} + sp\Sigma_1 + p^2\Sigma_2 \equiv r_1 r_2 \dots r_{p-1} + sp\Sigma_1 \pmod{p^2}$$

where Σ_1 is the elementary symmetric function of $r_1, \dots, r_{p-1}$ taken $p-2$ at a time, and Σ_2 is a sum of integers whose form is immaterial.

The polynomial $f(x) = (x - r_1)\dots(x - r_{p-1}) - (x^{p-1} - 1)$ has degree at most $p - 2$ and $r_1, \dots, r_{p-1}$ are all roots, so $f(x)$ must be identically zero modulo p. This implies that all elementary symmetric functions of $r_1, \dots, r_{p-1}$ except $r_1 \dots r_{p-1}$ must be divisible by p. This shows that each factor in Q is indeed congruent to 1 modulo p.

Now suppose r_1 when written in the base p has the form $B_1 0 B_2 0 \dots 0 B_k$ where each B_i is a block of nonzero digits and each 0 is a block of zeros of unspecified length. If $\binom{r_1}{t_1} \not\equiv 0 \pmod p$ then $t_1 = T_1 0 T_2 0 \dots 0 T_k$ where the blocks have the same length as the corresponding blocks in r_1 but the T_i may contain some zeros.

If r_2 has the same blocks B_i as r_1 then r_2 can be written $r_2 = B_{s_1} 0 B_{s_2} 0 \dots$ $\dots 0 B_{s_k}$ where the B_{s_i} are a permutation of the blocks B_i. (The blocks 0 may have different lengths.) If $t_2 = T_{s_1} 0 T_{s_2} 0 \dots 0 T_{s_k}$, we have a one-to-one correspondence between the elements of rows r_1 and r_2 in Pascal's triangle which are not divisible by p. It remains to show that $\binom{r_1}{t_1} \equiv \binom{r_2}{t_2} \pmod{p^2}$.

If we apply Theorem 2 to $\binom{r_1}{t_1}$ and $\binom{r_2}{t_2}$ then the factors are identical except *possibly* for

$$\binom{0b_{s_1}}{0t_{s_1}}\binom{b_{s_1}}{t_{s_1}}^{-1}, \quad \binom{b^*_{s_k}0}{t^*_{s_k}0}\binom{b^*_{s_k}}{t^*_{s_k}}^{-1}, \quad \binom{0b_1}{0t_1}\binom{b_1}{t_1}^{-1}, \quad \binom{b^*_k 0}{t^*_k 0}\binom{b^*_k}{t^*_k}^{-1}$$

where b_i and b^*_i denote the first and last digit of block B_i respectively, and similarly for T_i. However, each such product is congruent to 1 modulo p^2 by our earlier remarks, which completes the proof.

As expected, the residues divisible by p do not satisfy this theorem.

EXAMPLE. Let $p = 3$, $r_1 = 1210222$, $r_2 = 2220121$ as before. We have $N(r_1, 9, 3) = 220$, $N(r_2, 9, 3) = 264$; $N(r_1, 9, 6) = 212$, $N(r_2, 9, 6) = 276$.

In the following example the two numbers r_1 and r_2 have exactly the same pairs of digits (and single digits), but longer blocks are different.

EXAMPLE. $p = 3$, $r_1 = 12102202$, and $r_2 = 12021022$. We have $N(r_1, 9, 1) = 44$ but $N(r_2, 9, 1) = 68$.

A formula for $N(r,p,a)$. We can also use Lucas' Theorem to find a formula for $N(r,p,a)$ where $a \neq 0$. If $r = r_k \dots r_0$ in base p, let n_j be the number of the r_i which equal j for $j = 0, 1, \dots, p-1$. By Lucas' Theorem

$$\binom{r}{t} \equiv \prod_{j=1}^{p-1} \prod_{i=0}^{j} \binom{j}{i}^{s_{ji}} \pmod{p}$$

where s_{ji} = number of $t_h = i$ corresponding to values where $r_h = j$. Let $s = \{s_{ji}\}$ denote a fixed set of these values. Thus, the number of ways to arrange such values of t_h is

$$\prod_{j=1}^{p-1} \prod_{i=0}^{j} \frac{n_j!}{s_{ji}!} = A_s.$$

Also, for a given set of values s let

$$B_s = \prod_{j=1}^{p-1} \prod_{i=0}^{j} \binom{j}{i}^{s_{ji}}.$$

If $\varepsilon = \exp(2\pi i/p)$ then $(1/p) \sum_{h=0}^{p-1} \varepsilon^{h(B_s - a)}$ is the characteristic function for the values of B_s which are congruent to a given residue a. If we now sum over the possible sets of values s we obtain

$$N(r,p,a) = \frac{1}{p} \sum_{s_{10}+s_{11}=n_1} \cdots \sum_{s_{p-1,0}+\dots+s_{p-1,p-1}=n_{p-1}} \sum_{h=0}^{p-1} \varepsilon^{h(B_s - a)} A_s.$$

Such formulas also imply Theorem 1, but are not the easiest way to approach this result. In such general form they are not very effective in actually calculating $N(r,p,a)$. However, for small values of p we may obtain more effective formulas.

If we use Lucas' Theorem when $p = 3$, all factors except those of the form $\binom{2}{1}$ are congruent to 1. The value of $\binom{r}{t}$ thus depends on whether there are an even or an odd number of such factors. Thus,

$$N(r,3,1) = 2^{n_1} \sum_{j=0}^{[n_2/2]} \binom{n_2}{2j} 2^{n_2 - 2j} = 2^{n_1 - 1}(3^{n_2} + 1),$$

$$N(r,3,2) = 2^{n_1} \sum_{j=0}^{[(n_2-1)/2]} \binom{n_2}{2j+1} 2^{n_2 - 2j - 1} = 2^{n_1 - 1}(3^{n_2} - 1).$$

REFERENCES

[1] L. Carlitz, *The number of binomial coefficients divisible by a fixed power of a prime*, Rend. Circ. Mat. Palermo (2) 16 (1967), 299–320.

[2] K. Davis and W. Webb, *Lucas' theorem for prime powers*, European J. Combin. 11(1990), 229–233.
[3] —, —, *Pascal's triangle modulo* 4, Fibonacci Quart., to appear.
[4] L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, New York 1952.
[5] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589–592.
[6] H. Harborth, *Number of odd binomial coefficients*, Proc. Amer. Math. Soc. 62 (1977), 19–24.
[7] E. Hexel and H. Sachs, *Counting residues modulo a prime in Pascal's triangle*, Indian J. Math. 20 (1978), 91–105.
[8] C. Long, *Some divisibility properties of Pascal's triangle*, Fibonacci Quart. 19 (1981), 257–263.
[9] —, *Pascal's triangle modulo p*, ibid. 19 (1981), 458–463.
[10] D. Singmaster, *Divisibility of binomial and multinomial coefficients by primes and prime powers*, in: A Collection of Manuscripts Related to Fibonacci Sequences, 1980, 98–113.
[11] M. Sved and J. Pitman, *Divisibility of binomials by prime powers*, Ars Combin. 26A (1988), 197–222.

DEPARTMENT OF PURE AND APPLIED MATHEMATICS
WASHINGTON STATE UNIVERSITY
PULLMAN, WASHINGTON 99164, U.S.A.

Reçu par la Rédaction le 6.3.1990