NUMBER OF BINOMIAL COEFFICIENTS DIVISIBLE BY A FIXED POWER OF A PRIME

William B. Everett
Chernogolovka, Moscow Oblast, Russia
bill@chgnet.ru

Received: 11/21/07, Accepted: 2/4/08, Published: 3/5/08

Abstract

We present a general formula for the number of binomial coefficients in a given row of Pascal's triangle that are divisible by p^j and not divisible by p^{j+1}, where p is a prime.

1. Introduction

Let n be a nonnegative integer and p be a prime. Let $\theta_j(n,p)$ denote the number of binomial coefficients $\binom{n}{k}$, $0 \le k \le n$, such that p^j divides $\binom{n}{k}$ and p^{j+1} does not divide $\binom{n}{k}$. To write the general formula for $\theta_j(n,p)$, we first represent n in the base p: $n = c_0 + c_1 p + c_2 p^2 + \cdots + c_r p^r$, $0 \le c_i < p$, $i = 0, 1, \ldots, r$, $c_r > 0$ for $n \ne 0$. We use this representation of n in the base p throughout this paper.

We let W be the set of r-bit binary words, i.e.,

$$W = \left\{ \mathbf{w} = w_1 w_2 \ldots w_r \colon w_i \in \{0,1\},\ 1 \le i \le r \right\},$$

and partition W into $r{+}1$ subsets W_j, $0 \le j \le r$:

$$W_j = \left\{ \mathbf{w} \in W \colon \sum_{i=1}^{r} w_i = j \right\}.$$

The general formula for $\theta_j(n,p)$ is

$$\theta_j(n,p) = \sum_{\mathbf{w} \in W_j} F(\mathbf{w}) L(\mathbf{w}) \prod_{i=1}^{r-1} M(\mathbf{w}, i), \tag{1}$$

where the functions $F(\mathbf{w})$, $L(\mathbf{w})$, and $M(\mathbf{w}, i)$ are defined as

$$F(\mathbf{w}) = \begin{cases} c_0 + 1 & \text{if } w_1 = 0, \\ p - c_0 - 1 & \text{if } w_1 = 1, \end{cases}$$

$$L(\mathbf{w}) = \begin{cases} c_r + 1 & \text{if } w_r = 0, \\ c_r & \text{if } w_r = 1, \end{cases}$$

$$M(\mathbf{w}, i) = \begin{cases} c_i + 1 & \text{if } w_i = 0 \text{ and } w_{i+1} = 0, \\ p - c_i - 1 & \text{if } w_i = 0 \text{ and } w_{i+1} = 1, \\ c_i & \text{if } w_i = 1 \text{ and } w_{i+1} = 0, \\ p - c_i & \text{if } w_i = 1 \text{ and } w_{i+1} = 1. \end{cases}$$

Formula (1) reproduces known formulas for some particular values. For example, for $j = 0$, we obtain the known formula [1]

$$\begin{aligned} \theta_0(n, p) &= (c_0 + 1)(c_r + 1)(c_1 + 1) \cdots (c_{r-1} + 1) \\ &= (c_0 + 1)(c_1 + 1) \cdots (c_r + 1). \end{aligned}$$

For $j = 1$, we obtain the known formula [2]

$$\begin{aligned} \theta_1(n, p) = {} & (c_0 + 1)c_r(c_1 + 1)(c_2 + 1) \cdots (c_{r-2} + 1)(p - c_{r-1} - 1) \\ & + (c_0 + 1)(c_r + 1)(c_1 + 1)(c_2 + 1) \cdots (p - c_{r-2} - 1)c_{r-1} \\ & + \cdots \\ & + (c_0 + 1)(c_r + 1)(p - c_1 - 1)c_2(c_3 + 1) \cdots (c_{r-1} + 1) \\ & + (p - c_0 - 1)(c_r + 1)c_1(c_2 + 1) \cdots (c_{r-1} + 1) \\ = {} & \sum_{k=0}^{r-1} (c_0 + 1) \cdots (c_{k-1} + 1)(p - c_k - 1)c_{k+1}(c_{k+2} + 1) \cdots (c_r + 1). \end{aligned}$$

Other particular formulas for $\theta_j(n, p)$ can be found in [3] and [4].

We find a matrix representation convenient for considering questions of the prime divisibility of Pascal's triangle. We describe this matrix representation in Sec. 2. Based on this representation, we construct what we call a "crossword" for a row in Pascal's triangle in Sec. 3. Each vertical "word" in the crossword corresponds to a binomial coefficient in the row of Pascal's triangle. The "letters"(zero or one) in the vertical word correspond to the carries in Kummer's theorem on the highest power of a prime that divides a binomial coefficient [5]. In Sec. 4, we use the relations between the structures of the horizontal "words" to construct formula (1).

2. Matrices

For considering the prime divisibility of the binomial coefficients in Pascal's triangle, we use a sequence of square matrices of sizes $p, p^2, p^3, \dots$ containing zeros on the main diagonal and in the lower triangle and ones in the upper triangle above the main diagonal. Letting M be the $p \times p$ matrix containing all ones and I be the $p \times p$ identity matrix, we can define the sequence of prime divisibility matrices T_i for Pascal's triangle recursively:

$$\begin{aligned} &T_1 = (t_{ij}), \qquad t_{ij} = \begin{cases} 0, & i \geq j, \\ 1, & i < j, \end{cases} \qquad i, j = 1, 2, \dots, p, \\ &T_{n+1} = T_n \otimes M + I \otimes T_n, \quad n > 0, \end{aligned} \tag{2}$$

where $A \otimes B$ is the Kronecker product of the matrices A and B (also called the tensor product or outer product). As a simple illustrative example, we write the first three T matrices for $p = 2$ (in a condensed format to save space):

$$\begin{matrix} 01 \\ 00 \end{matrix}\, , \qquad \begin{matrix} 0111 \\ 0011 \\ 0001 \\ 0000 \end{matrix}\, , \qquad \begin{matrix} 01111111 \\ 00111111 \\ 00011111 \\ 00001111 \\ 00000111 \\ 00000011 \\ 00000001 \\ 00000000 \end{matrix}\, .$$

Using these matrices, we can recursively define a sequence of matrices H_i containing the degrees of the highest power of the prime p that divides each binomial coefficient in Pascal's triangle:

$$\begin{aligned} &H_1 = T_1, \\ &H_{n+1} = T_{n+1} + M \otimes H_n, \quad n > 0. \end{aligned} \tag{3}$$

We illustrate this with the specific example of H_1 and H_2 for $p = 3$:

$$H_1 = \begin{matrix} 011 \\ 001 \\ 000 \end{matrix}\, ,$$

$$H_2 = \begin{matrix} 011111111 \\ 001111111 \\ 000111111 \\ 000011111 \\ 000001111 \\ 000000111 \\ 000000011 \\ 000000001 \\ 000000000 \end{matrix} + \begin{matrix} 111 \\ 111 \\ 111 \end{matrix} \otimes \begin{matrix} 011 \\ 001 \\ 000 \end{matrix}$$

$$= \begin{array}{c} 011111111 \\ 001111111 \\ 000111111 \\ 000011111 \\ 000001111 \\ 000000111 \\ 000000011 \\ 000000001 \\ 000000000 \end{array} + \begin{array}{c} 011011011 \\ 001001001 \\ 000000000 \\ 011011011 \\ 001001001 \\ 000000000 \\ 011011011 \\ 001001001 \\ 000000000 \end{array}$$

$$= \begin{array}{c} 022122122 \\ 002112112 \\ 000111111 \\ 011022122 \\ 001002112 \\ 000000111 \\ 011011022 \\ 001001002 \\ 000000000 \end{array} .$$

The main diagonal and lower triangle of H_i correspond to the rows 0 through $p^i - 1$ of Pascal's triangle, and the upper triangle is ready to appear in rows p^i through $p^{i+1} - 1$ at the next iteration of the recursion.

In passing, we note that the sequence of matrices R_i, $i = 1, 2, \ldots$, corresponding to Pascal's triangle modulo p can also be defined recursively:

$$R_1 = (r_{ij}), \qquad r_{ij} = \begin{cases} 0, & j > i, \\ 1, & j = 1, \qquad i, j = 1, 2, \ldots, p, \\ r_{i-1,j-1} + r_{i-1,j} \bmod p, & 1 < j \leq i, \end{cases} \tag{4}$$
$$R_{n+1} = R_1 \otimes R_n, \quad n > 0,$$

where the matrix elements are multiplied modulo p. Then $\binom{n}{k}$ modulo p is the element $r_{n+1,k+1}$ of the matrix R_m, $p^m > n$.

3. Crossword

In constructing formula (1), we use a crossword $\mathrm{C}_{n,p}$ consisting of an $r \times (n+1)$ array of zeros and ones, where r is the degree of the highest power of p not exceeding n. The sum of the zeros and ones in a vertical word is equal to the degree of the highest power of p dividing the binomial coefficient in the corresponding position in the nth row of Pascal's triangle. We build the crossword using "powers" of the basic T matrices recursively defined as

$$T_i^1 = T_i,$$
$$T_i^m = M \otimes T_i^{m-1}, \quad m > 1.$$

The ith horizontal word in $\mathrm{C}_{n,p}$ is defined as the first n+1 elements of the (n+1)th row of T_i^m, where m is sufficiently large (so that T_i^m in fact contains an (n+1)th row).

As a simple illustrative example, we give the crosswords $\mathrm{C}_{n,3}$ for $n = 27, 28, 29, 30$:

$$n = 27: \quad \begin{matrix} 0110110110110110110110110110 \\ 0111111110111111110111111110 \\ 0111111111111111111111111110 \end{matrix} \; ,$$

$$n = 28: \quad \begin{matrix} 00100100100100100100100100100 \\ 00111111100111111100111111100 \\ 00111111111111111111111111100 \end{matrix} \; ,$$

$$n = 29: \quad \begin{matrix} 000000000000000000000000000000 \\ 000111111000111111000111111000 \\ 000111111111111111111111111000 \end{matrix} \; ,$$

$$n = 30: \quad \begin{matrix} 0110110110110110110110110110110 \\ 0000111110000111110000111110000 \\ 0000111111111111111111111110000 \end{matrix} \; .$$

Kummer's theorem [5] states that the degree of the highest power of a prime p that divides the binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

is equal to the number of carries when adding k and $n - k$ in the base p. We illustrate this with the example of $n = 27$ and $p = 3$:

carry	000	111	111	110	111	111	110	111	111	
k	0	1	2	10	11	12	20	21	22	
$n-k$	1000	222	221	220	212	211	210	202	201	
$n = k + (n{-}k)$	1000	1000	1000	1000	1000	1000	1000	1000	1000	
	100	111	111	110	111	111	110	111	111	
	100	101	102	110	111	112	120	121	122	
	200	122	121	120	112	111	110	102	101	
	1000	1000	1000	1000	1000	1000	1000	1000	1000	
	100	111	111	110	111	111	110	111	111	000
	200	201	202	210	211	212	220	221	222	1000
	100	22	21	20	12	11	10	2	1	0
	1000	1000	1000	1000	1000	1000	1000	1000	1000	1000

Comparing the carries here with the crossword $\mathrm{C}_{27,3}$ above makes the correspondence clear: the top row in the crossword corresponds to the least significant carry position (3^1 in this example), and the bottom row corresponds to the most significant carry position (3^3 in this example).

4. Constructing the Formula

The column sums of the $r\times(n+1)$ crossword $\mathrm{C}_{n,p}$ are the degrees of the highest powers of p dividing the corresponding binomial coefficients. In other words, the sum of the $(k+1)$th column in the crossword is the number of carries when adding k and $n-k$ in the base p. To construct formula (1), we must determine how many columns in the crossword produce the given value j as their column sum. The subset W_j defined in Sec. 1 contains all the possible vertical words containing exactly j ones. If we can determine the number of occurrences of a given vertical word in the crossword, then we can sum these numbers over the words in W_j to obtain the total number of binomial coefficients $\binom{n}{k}$, $0 \le k \le n$, that are divisible by p^j and not divisible by p^{j+1}.

To determine the number of occurrences of a given vertical word in the crossword $\mathrm{C}_{n,p}$, we study the structure of the horizontal words and, in particular, the relation between the ith and the $(i+1)$th horizontal words. To facilitate the discussion, we introduce auxiliary variables m_i and s_i (depending on n and p) and a notation for substrings in the horizontal words. Recalling the representation of n in the base p, $n = c_0 + c_1p + c_2p^2 + \cdots + c_rp^r$, $0 \le c_i < p$, $i = 0, 1, \ldots, r$, $c_r > 0$ for $n \ne 0$, we define the auxiliary variables as

$$m_i = c_i + c_{i+1}p + c_{i+2}p^2 + \cdots + c_rp^{r-i}, \tag{5}$$

$$s_i = c_0 + c_1p + c_2p^2 + \cdots + c_{i-1}p^{i-1} \tag{6}$$

for $1 \le i \le r$. Clearly, $n = m_ip^i + s_i$, $0 \le s_i < p^i$.

Before defining the substring notation, we mention some obvious properties of the matrices T_i^m underlying the structure of the horizontal words. Clearly, each horizontal word ends on the main diagonal of the matrix T_i^m from which it was taken ($n + 1 = n + 1$). It follows from the structure of the matrices T_i^m (a transition from zero to one in T_i only occurs in passing from the main diagonal into the upper triangle) that a transition from zero to one in the ith horizontal word ($i > 1$) always coincides with a transition from zero to one in the $(i-1)$th horizontal word except when the $(i-1)$th horizontal word contains only zeros.

We let I_i denote a substring in the ith horizontal word consisting of ones and preceded by a zero and followed by a zero. Letting $\ell(\,\cdot\,)$ denote the length of a substring, we have $\ell(\mathrm{I}_i) = p^i - s_i - 1$. We consider that a substring I_i of length 0 actually exists at a given position in the word; this "convention" obviates the exception at the end of the preceding paragraph and allows the subsequent argument to apply to all cases without exception. We let O_i denote a substring in the ith horizontal word consisting of zeros and preceded and followed by I_i (possibly with $\ell(\mathrm{I}_i) = 0$) or a word boundary. We have $\ell(\mathrm{O}_i) = s_i + 1$. We can now represent the ith horizontal word in the crossword $\mathrm{C}_{n,p}$ as

$$[\mathrm{O}_i\mathrm{I}_i]^{m_i}\mathrm{O}_i, \tag{7}$$

where $[\,\cdot\,]^m$ denotes concatenation of m copies of the argument string. Clearly, $\ell(\mathrm{O}_i\mathrm{I}_i) = p^i$ and $\ell([\mathrm{O}_i\mathrm{I}_i]^{m_i}\mathrm{O}_i) = m_i p^i + s_i + 1 = n + 1$.

Defining a projection π of a substring of the $(i{+}1)$th horizontal word $(i > 1)$ to be the substring of the ith horizontal word beginning and ending at the same locations, we have

$$\pi(\mathrm{O}_{i+1}) = [\mathrm{O}_i\mathrm{I}_i]^{c_i}\mathrm{O}_i \tag{8}$$

and

$$\pi(\mathrm{I}_{i+1}) = [\mathrm{I}_i\mathrm{O}_i]^{p-c_i-1}\mathrm{I}_i. \tag{9}$$

We are now ready to determine the number of occurrences of a given vertical word in the crossword $\mathrm{C}_{n,p}$. We proceed from the top of the crossword (row 1) to the bottom of the crossword (row r). If the first letter in the given vertical word is zero, then we want the length of O_1, but if the first letter is one, then we want the length of I_1. We define our first function $F(\mathbf{w})$ as

$$F(\mathbf{w}) = \begin{cases} \ell(\mathrm{O}_1) & \text{if } w_1 = 0, \\ \ell(\mathrm{I}_1) & \text{if } w_1 = 1. \end{cases}$$

By definition, $\ell(\mathrm{O}_1) = s_1 + 1$ and $\ell(\mathrm{I}_1) = p - s_1 - 1$. By (6), $s_1 = c_0$. Consequently, we have

$$F(\mathbf{w}) = \begin{cases} c_0 + 1 & \text{if } w_1 = 0, \\ p - c_0 - 1 & \text{if } w_1 = 1. \end{cases}$$

We now consider four cases for a two-bit substring in the word: 00, 01, 10, and 11. Further, we need to do this for each of $r{-}1$ two-bit substrings beginning with the first letter, the second letter, and so on to the next-to-last letter of the word. For the substring 00 starting from the ith letter, $i = 1, 2, \ldots, r-1$, we want to know how many times O_i occurs within O_{i+1}. From inspection of Eq. (8), we see that this is $c_i{+}1$ times, and we also see that I_i is included in O_{i+1} c_i times (corresponding to the two-bit substring 10). Similarly, from Eq. (9), we see that O_i is included in I_{i+1} $p{-}c_i{-}1$ times (corresponding to the substring 01) and I_i is included in I_{i+1} a total of $p - c_i - 1 + 1 = p - c_i$ times. We thus construct the middle function

$$M(\mathbf{w}, i) = \begin{cases} c_i + 1 & \text{if } w_i = 0 \text{ and } w_{i+1} = 0, \\ p - c_i - 1 & \text{if } w_i = 0 \text{ and } w_{i+1} = 1, \\ c_i & \text{if } w_i = 1 \text{ and } w_{i+1} = 0, \\ p - c_i & \text{if } w_i = 1 \text{ and } w_{i+1} = 1, \end{cases}$$

and to account for the $r{-}1$ two-bit substrings, we take the product

$$\prod_{i=1}^{r-1} M(\mathbf{w}, i). \tag{10}$$

Multiplying $F(\mathbf{w})$ times product (10), we obtain the number of multiple occurrences of the given word either in O_r if the last letter in the word is zero or in I_r if the last letter in the word is one. Our last step before summing over the words in W_j is to determine the number of repetitions of either O_r or I_r depending on the value of w_r in the given vertical word. From (7), we see that O_r occurs m_r+1 times and I_r occurs m_r times. By definition (5), $m_r = c_r$. We therefore write the last function

$$L(\mathbf{w}) = \begin{cases} c_r + 1 & \text{if } w_r = 0, \\ c_r & \text{if } w_r = 1. \end{cases}$$

Summing the product for each word over the set of words satisfying the criterion that the number of ones in the word is exactly j, we obtain the general formula

$$\theta_j(n,p) = \sum_{\mathbf{w}\in W_j} F(\mathbf{w}) \left(\prod_{i=1}^{r-1} M(\mathbf{w},i) \right) L(\mathbf{w}).$$

By the commutativity of ordinary multiplication, this is the same as formula (1) in Section 1.

References

[1] Fine, N. J.: Binomial coefficients modulo a prime. *Amer. Math. Monthly* **54**, 589–592 (1947)

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

[3] Howard, F. T.: The number of binomial coefficients divisible by a fixed power of 2. *Proc. Amer. Math. Soc.* **29**, 236–242 (1971)

[4] Howard, F. T.: Formulas for the number of binomial coefficients divisible by a fixed power of a prime. *Proc. Amer. Math. Soc.* **37**, 358–362 (1973)

[5] Kummer, E. E.: Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. *J. Reine Angew. Math.*, **44**, 93–146, (1852)