# $p$-ADIC CONGRUENCES BETWEEN BINOMIAL COEFFICIENTS

**V. Giambalvo**
University of Connecticut, Storrs, CT 06268

**Ray Mines**
New Mexico State University, Las Cruces, NM 88003

**David J. Pengelley**
New Mexico State University, Las Cruces, NM 88003

(Submitted April 1989)

The study of identities and congruences involving binomial coefficients has a long history, not only because of the intrinsic beauty and apparent simplicity of many of the results, but also because applications for these abound in many fields, both inside and outside mathematics. The impetus for the present study came from work on classifying spaces in algebraic topology [3], where one needed to know how the 2-divisibility of $\binom{a+2^n}{b} - \binom{a}{b}$ depends on $n$, $a$, and $b$.

The basic question we would like to address is this: For a given prime $p$, and natural numbers $a$, $b$, $a \geq b \geq 1$, what is the $p$-divisibility of the difference

$$\binom{a+x}{b} - \binom{a}{b}$$

and how does it depend on the $p$-divisibility of $x$? For any integer $k$, let $v_p(k)$ denote the exponent of the highest power of $p$ dividing $k$, and $v_p(k/n) = v_p(k) - v_p(n)$. We wish to consider

$$f(x) = v_p\left(\binom{a+x}{b} - \binom{a}{b}\right),$$

where $x$ is any natural number. Now

$$F(x) = \binom{a+x}{b}$$

is a polynomial in $x$ with $F'(0) \neq 0$, so it is elementary that, for $v_p(x)$ large (i.e., $x$ near 0 in the $p$-adic metric),

$$f(x) = v_p(F(x) - F(0)) = v_p(x) + v_p(F'(0)).$$

In other words, $f$ "stabilizes" for $v_p(x)$ sufficiently large. The aims of this note are threefold. First to determine exactly how large is sufficiently large, second to examine the behavior of $f$ both in and near this range, and third to understand how the behavior of $f$ is related to the divisibilities of $\binom{a+x}{b}$ and $\binom{a}{b}$. These three divisibilities are intimately connected by the fact that

$$v_p(y \pm z) \geq \min\{v_p(y), v_p(z)\},$$

with equality holding for $p = 2$ precisely when $v_2(y) \neq v_2(z)$. This creates some surprising phenomena when $p = 2$. The most striking is that while constancy of $v_2\binom{a+x}{b}$ for $v_2(x)$ large is necessary in order for $f$ to exhibit stability, the latter always occurs before, not after, the former. One of our main aims is to understand the phenomena underlying this curious fact. Our Conclusion summarizes why this occurs.

Complete results will be given for $p = 2$, and some partial results will be obtained for odd primes, where the situation is much more complicated.

## 1. Preliminaries

First we look at $\binom{a+x}{b}$ and its $p$-divisibility. The basic result on divisibility is due to Kummer [4, pp. 115-16; 1, p. 270]: If $a = \sum a_i p^i$ and $b = \sum b_i p^i$ are the base $p$ expansions of $a$ and $b$ (here, of course, $a_i, b_i \in [0, p)$), then $v_p\binom{a}{b}$, the $p$-divisibility of $\binom{a}{b}$, is the number of borrows in the base $p$ subtraction $a - b$. A good general reference is [5]. Some related results can be found in [2]. Therefore,

$$v_p\binom{a+x}{b} = v_p\binom{a}{b} \text{ for } v_p(x) \text{ large,}$$

and we wish to quantify "large."

*Definition 1:* $M(a, b, p)$ is the smallest integer $M$ such that

$$v_p\binom{a+x}{b} = v_p\binom{a}{b} \text{ whenever } v_p(x) \geq M.$$

For any integer $n$, let $\overline{n}_\ell$ be the residue of $n$ modulo $p^\ell$. From Kummer's theorem, it is clear that $M$ is nothing other than $\min\{\ell | \overline{a}_\ell \geq b\}$. Let

$$S = \{a, a - 1, \ldots, a - b + 1\}$$

be the set of integers in the "numerator" of $\binom{a}{b}$. Let $s_1, s_2, \ldots, s_b$ be the elements of $S$ arranged in order of decreasing $p$-divisibility, and let $d_i = v_p(s_i)$. So $d_1$ is the highest divisibility occurring in $S$, etc. Note that the $d_i$ are not necessarily distinct. Our first lemma relates $M$ to $d_1$.

*Lemma 2:* $v_p\binom{a+x}{b} = v_p\binom{a}{b}$ whenever $v_p(x) \geq M$, where $M = \min\{\ell | \overline{a}_\ell \geq b\} = d_1 + 1$.

*Proof:* Everything was done above, except the equality $M = d_1 + 1$. We show this by manipulating the base $p$ expansion of $a$. Since $\overline{a}_M \geq b$, $\overline{a}_M$ can never be reduced to zero by subtracting something in the interval $[0, b)$, so no element of $S$ is congruent to 0 mod $p^M$. Hence, $d_1 \leq M - 1$. To see that $d_1 \geq M - 1$, note that $\overline{a}_{M-1} < b$, and so there is an element of $S$ which is zero mod $p^{M-1}$. Thus, $d_1 \geq M - 1$. □

We now turn our attention to $f(x)$.

*Definition 3:* $N(a, b, p)$ is the smallest integer $N$ such that

$$f(x) = v_p(x) + v_p(F'(0)) \text{ whenever } v_p(x) \geq N.$$

Since the equality

$$v_p\binom{a+x}{b} = v_p\binom{a}{b}$$

of Lemma 1 is clearly necessary for this stabilizing of $f$, one might expect that $N \geq M$. It is therefore surprising that, on the contrary, we will show that exactly the opposite occurs for $p = 2$, and that, for odd primes, $M$ and $N$ are more or less independent. The first step in computing $N$ is to bound it from above. That is one purpose of the next section.

## 2. A Formula for $f$ and a bound on $N(a, b, p)$

We start with the degree $b$ polynomial

$$F(x) - F(0) = \binom{a+x}{b} - \binom{a}{b}.$$

Note that $f(x) = v_p(F(x) - F(0))$. Let $S$ be as before and $S^{-1} = \{1/s | s \in S\}$. For any set of integers $A$ let $\sigma_i(A)$ denote the $i^{\text{th}}$-elementary symmetric function on the elements of $A$ and abbreviate $\sigma_k(S^{-1})$ by $\sigma_k$. Then expanding $F(x) - F(0)$, we obtain

$$F(x) - F(0) = \frac{1}{b!}\sum_{k=1}^{b}\sigma_{b-k}(S)x^k = \binom{a}{b}\sum_{k=1}^{b}\sigma_k(S^{-1})x^k = x\binom{a}{b}\sum_{k=1}^{b}\sigma_k x^{k-1}.$$

Clearly, for $v_p(x)$ large, $v_p$ applied to the final sum leaves only $v_p(\sigma_1)$. This shows that $f$ stabilizes as claimed, and gives our first formula for it.

*Theorem 4:* $f(x) = v_p(x) + v_p\binom{a}{b} + v_p(\sigma_1)$ for $v_p(x) \geq N$.

Our main interest is in what determines $N$, and in the curious way that this is related to $v_p\binom{a+x}{b}$ in and near the stable range when $p = 2$. Now to obtain a bound for $N$ from the above, we need only determine how large $v_p(x)$ need be to ensure that

$$v_p\left(\sum_{k=1}^{b}\sigma_k x^{k-1}\right) = v_p(\sigma_1).$$

*Theorem 5:* $N(a, b, p) \leq v_p(\sigma_1) + d_1 + d_2 + 1$.

*Proof:* We will show that $v_p(\sigma_k) + v_p(x)(k - 1) > v_p(\sigma_1)$ for $k \geq 2$, as long as $v_p(x) > v_p(\sigma_1) + d_1 + d_2$.

Note that

$$v_p(\sigma_k) \geq -\sum_{i=1}^{k} d_i.$$

We then have

$$\begin{aligned} v_p(\sigma_k) + v_p(x)(k-1) &> -\sum_{i=1}^{k} d_i + (k-1)(v_p(\sigma_1) + d_1 + d_2) \\ &= v_p(\sigma_1) + (k-2)v_p(\sigma_1) + (k-2)(d_1 + d_2) - \sum_{i=3}^{k} d_i \\ &= v_p(\sigma_1) + (k-2)(v_p(\sigma_1) + d_1) + \sum_{i=3}^{k}(d_2 - d_i) \\ &\geq v_p(\sigma_1). \quad \square \end{aligned}$$

## 3. At the Prime 2

Henceforth, let $p = 2$ and let $v$ stand for $v_2$. In this section we will simplify our formula for $f$ in the stable range, show that $N = d_2 + 1$, and give a formula for $N$ that is easily computed from $a$ and $b$. This formula shows that $N$ is almost determined by $b$.

We begin by obtaining more information about the behavior of $v\binom{a+x}{b}$.

*Lemma 6:* The following facts express how the relationship between $v\binom{a+x}{b}$ and $v\binom{a}{b}$ changes as $v(x)$ varies in relation to $d_2$, $d_1$, and $M$:

a. $d_1 > d_2$,

b. $v\binom{a+x}{b} = v(x) + v\binom{a}{b} - d_1$ when $d_2 < v(x) < M - 1 = d_1$,

c. $v\binom{a+x}{b} > v\binom{a}{b}$ when $v(x) = M - 1 = d_1$,

d. $v\binom{a+x}{b} = v\binom{a}{b}$ when $v(x) \geq M = d_1 + 1$.

Notice that Lemma 6 shows that $v\binom{a+x}{b}$ increases predictably for $d_2 < v(x) < d_1$, jumps sharply up when $v(x) = d_1$, and then drops to constancy for $v(x) > d_1$. Later, we will compare this behavior with that of $f(x)$.

*Proof:* We note first that $d_1 > d_2$, since between any two integers exactly divisible by $2^j$ lies one divisible by $2^{j+1}$. For parts (b) and (c), we note that

$$v\binom{a+x}{b} - v\binom{a}{b} = v(s_1 + x) - v(s_1) + \sum_{i>1} v(s_i + x) - v(s_i).$$

Since $v(x) > d_2$, we have $v(s_i + x) = v(s_i)$ for all $i > 1$, so the sum evaporates. Then, if $v(x) = d_1$, we have $v(s_1 + s) > v(s_1)$, so the result is positive, while if $v(x) < d_1$, then $v(s_1 + x) = v(x)$, producing the result $v(x) - d_1$, as claimed. Part (d), which completes our description of the behavior of $v\binom{a+x}{b}$, is merely a restatement of Lemma 2. □

Now we can also strengthen our theorems about $f$ and $N$, since we can actually compute $v(\sigma_1)$.

*Corollary 7:* $f(x) = v(x) + v\binom{a}{b} - d_1$ for $v(x) \geq N$, and $N \leq d_2 + 1 < d_1 + 1 = M$.

*Proof:* From Lemma 6, we know that $d_1 > d_2$. Hence, $v(\sigma_1) = -d_1$ and the result follows. □

This verifies that $N < M$, i.e., $f(x)$ stabilized before $v\binom{a+x}{b}$ becomes constant.

Next, we complete our determination of $N$ with

*Theorem 8:* $N = d_2 + 1$. Moreover $f(x) > v(x) + v\binom{a}{b} - d_1$ whenever $v(x) = N - 1 = d_2$.

*Proof:* In view of Corollary 7, we need only show that

$$f(x) > d_2 + v\binom{a}{b} - d_1 \text{ if } v(x) = d_2.$$

Since

$$v\binom{a}{b} > d_2 + v\binom{a}{b} - d_1$$

from Lemma 6, this will follow if we also show that

$$v\binom{a+x}{b} > d_2 + v\binom{a}{b} - d_1.$$

Recalling that $v(x) = d_2 < d_1$, we have

$$\begin{aligned} v\binom{a+x}{b} - v\binom{a}{b} &= v(s_1 + x) - v(s_1) + \sum_{v(s_i) \leq d_2} (v(s_i + x) - v(s_i)) \\ &= d_2 - d_1 + \sum_{v(s_i) \leq d_2} (v(s_i + x) - v(s_i)) \\ &> d_2 - d_1, \end{aligned}$$

the last inequality holding, since each term in the sum if nonnegative, and at least one [with $v(s_2) = d_2$] is positive. □

We will now provide a formula for $N$ more convenient for calculation. Let

$$k = k(b) = [\log_2(b)],$$

the greatest integer in $\log_2(b)$. Recall that, for any integer $n$, $\overline{n}_\ell$ denotes the residue of $n$ modulo $2^\ell$. Let

$$g(a, b) = \begin{cases} k & \text{if } \overline{a}_k \geq \overline{b}_k, \\ k + 1 & \text{if } \overline{a}_k < \overline{b}_k. \end{cases}$$

Clearly, $g$ is easy to compute from $a$ and $b$, and it is almost determined by $b$.

*Lemma 9:* $N = d_2 + 1 = g$.

*Proof:* We need only show that $g = d_2 + 1$. First we show that $g \geq d_2 + 1$. Since $[\log_2(b)] = k$, we have $b \in [2^k, 2^{k+1})$. Since $S$ is a sequence of $b$ consecutive integers, $S$ must contain exactly one or two multiples of $2^k$. If only one, it is the element of highest two-divisibility $d_1$ in $S$, so $d_2 < k$; hence $d_2 + 1 \leq k \leq g$. If there are two, one is an even multiple of $2^k$, of highest divisibility, the other is an odd multiple of $2^k$. Hence, $d_2 = k$. Thus, we need to show that whenever $g = k$ (rather than $k + 1$), $S$ has only one multiple of $2^k$. But $g = k$ only when $\overline{b}_k \leq \overline{a}_k$. We write $b = 2^k + \overline{b}_k$, $a = \beta 2^k + \overline{a}_k$, with $0 \leq \overline{b}_k \leq \overline{a}_k < 2^k$. Then

$$(\beta - 1)2^k \leq a - b < \beta 2^k \leq a < (\beta + 1)2^k,$$

so $S$ has only one multiple of $2^k$.

To show that $g \leq d_2 + 1$, note that, since $b \in [2^k, 2^{k+1})$, there must be at least two multiples of $2^{k-1}$ in $S$. Thus, $d_2 \geq k - 1$, or $d_2 + 1 \geq k$. So we are done if $g = k$. If $g = k + 1$, then we need $d_2$ to be at least $k$. So we need two multiples of $2^k$ in $S$. We write $a$ and $b$ as before, but now $\overline{a}_k < \overline{b}_k < 2^k$, so we have

$$a - b = (\beta - 1)2^k + (\overline{a}_k - \overline{b}_k) < (\beta - 1)2^k < \beta 2^k \leq a,$$

and we have exhibited two multiples of $2^k$ in $S$. □

## 4. Conclusions

Our results for $p = 2$ provide a complete picture of the relationship among

$$v\binom{a}{b},\ v\binom{a+x}{b},\ \text{and } f(x) = v\left(\binom{a+x}{b} - \binom{a}{b}\right)$$

in the stable range. There are three possibilities:

$$f(x) \text{ will equal } v\binom{a+x}{b} \text{ if } v\binom{a+x}{b} < v\binom{a}{b};$$

$$f(x) \text{ will equal } v\binom{a}{b} \text{ if } v\binom{a}{b} < v\binom{a+x}{b};$$

$f(x)$ will exceed both of the above if they are equal.

We see that all three possibilities actually occur, in the order stated, as $v(x)$ increases through the stable range. This trio and order of behaviors is, in fact, the only way $f(x)$ can possibly achieve the formula

$$v(x) + v\binom{a}{b} - d_1$$

in a range that srarts earlier (at $N = d_2 + 1 = g$) than the constancy of $v\binom{a+x}{b}$ (at $M = d_1 + 1$).

For odd primes, the situation can be quite different. We illustrate the situation in the case of $b = 2$. Then

$$F(x) - F(0) = \binom{a+x}{2} - \binom{a}{2} = x(x + 2a - 1)/2.$$

Let $j$ be a positive integer.

First, choose $a = p^j$. From Lemma 2, we have $M = d_1 + 1 = j + 1$, and since $v_p(\sigma_1) = -j$ and $d_2 = 0$, Theorem 5 says that $N \leq 1$. Since

$$F(x) - F(0) = x(x + 2p^j - 1)/2,$$

we have that $N$ is indeed 1. So, as above, $N < M$ and $N = [\log_p(b)] + 1$.

Next, choose $a = (p^j + 1)/2$. Here the situation is radically different. Since $p$ is odd, $d_1 = d_2 = 0$, but $2a - 1 = p^j$, so $v_p(\sigma_1) = j$, and Theorem 5 says that $N \leq j + 1$. From

$$F(x) - F(0) = x(x + p^j)/2,$$

we see that $N = j + 1$. But $M = d_1 + 1 = 1$.

There are patterns however, and the reader is invited to discover them.

## References

1. L. E. Dickson. *History of the Theory of Numbers*. Vol. I. Washington, D.C.: Carnegie Institute of Washington, 1919.
2. Robert D. Fray. "Congruence Properties of Ordinary and $q$-Binomial Coefficients." *Duke J. Math.* *34* (1967):467-80.
3. V. Giambalvo, D. J. Pengelley, D. C. Ravenel. "A Fractal-Like Algebraic Splitting of the Classifying Space for Vector Bundles." *Trans. Amer. Math. Soc.* *307* (1988):433-55.
4. D. Kummer. "Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen." *Journal für die Reine und Angewandte Mathematik* *44* (1852):93-146.
5. D. Singmaster. "Divisibility of Binomial and Multinomial Coefficients by Primes and Prime Powers." *A Collection of Manuscripts Related to the Fibonacci Sequence: 18th Anniversary Volume*. Ed. V. E. Hoggatt, Jr., & M. Bicknell-Johnson. Santa Clara, Calif.: The Fibonacci Association, 1980, pp. 98-113.

*****