A CONGRUENCE FOR PRODUCTS OF BINOMIAL COEFFICIENTS MODULO A COMPOSITE

Andrew D. Loveless
Department of Mathematics, University of Washington, Box 354350, Seattle, WA 98195-4350, USA
aloveles@math.washington.edu

Received: 8/28/07, Revised: 9/17/07, Accepted: 9/24/07, Published: 10/1/07

Abstract

For a positive composite integer n, we investigate the residues of $\binom{mn}{k}$ for positive integers m and k. First, we discuss divisibility of such coefficients. Then we study congruence identities relating products of binomial coefficients modulo n. Certainly the Chinese Remainder Theorem can be used in combination with prime power results to evaluate binomial coefficients modulo a composite. However, in this study we investigate residues modulo a composite directly without appealing to the Chinese Remainder Theorem. And as a result we get closed form identities modulo a composite.

One of the many consequences of the main result (Theorem 8) is the following: If p, q and r are primes and m is a positive integer, then $mr\binom{mpqr}{pq} \equiv \binom{mqr}{q}\binom{mpr}{p} \pmod{pqr}$. Several numerical examples of these results are included.

Introduction

Several areas of number theory and discrete mathematics make use of arithmetical properties of binomial coefficients. Congruence relations for binomial coefficients have been studied by many prominent mathematicians including Gauss, Kummer, Legendre, and Lucas. Andrew Granville [1] gives a wonderful survey of many of the elegant results pertaining to binomial coefficients modulo prime powers. In addition, Prof. Granville maintains an on-line 'dynamic survey' devoted to these results. In this study, we extend some of these result to composite moduli.

We will focus mainly on binomial coefficients $\binom{a}{b}$ modulo n, where n is a divisor of a. This focus is motivated by their extensive use in the study of probabilistic primality testing (also called compositeness testing). For the remainder of this introduction, we motivate this statement.

The subject of probabilistic primality testing is full of congruence relations that always hold for a prime and rarely hold for a composite. A large portion of these congruences are proved, at least in part, by making use of the following well-known property.

Theorem 1. *The positive integer n is a prime if and only if*

$$\binom{n}{k} \equiv 0 \pmod{n} \text{ for all } k \text{ with } 1 \le k \le n-1.$$

This characterization of primes is not an efficient form of primality testing since it requires the direct computation of binomial coefficients. However, this theorem is used indirectly to give effective probabilistic primality tests. The main goal in researching such tests is to study when and why a composite integer may satisfy a congruence that is *usually* only satisfied by primes.

In this study, we let n be a composite number and we examine the generalizations of Theorem 1. The results naturally extend to the case when the modulus divides the 'top' values in the binomial coefficient so we include this case as well. We believe that these results are interesting and elegant in their own right, but we ultimately hope that they will help in the study of primality testing.

To summarize, we are motivated by the following question:

Question: *For a composite integer n, what can be said about the residue of $\binom{mn}{k}$ modulo n for $1 \le k \le n-1$?*

We will show that such binomial coefficients can be expressed in closed form in terms of products of binomial coefficients in which the divisors of (n, k) are removed in a certain way, where (n, k) is the greatest common divisor of n and k. The techniques are elementary, but the results seem interesting in their own right. The only results of a similar nature that this author could find was in a chapter of the book "Computational Recreations in Mathematica" [2]. On pages 65-66 of this book, the following result is given.

Theorem 2. *If $f(n) := \binom{n-1}{(n-1)/2}$ is defined for odd integers n, then*

$$f(pq) \equiv f(p)f(q) \pmod{pq}, \text{ and}$$

$$f(pqr)f(p)f(q)f(r) \equiv f(pq)f(pr)f(qr) \pmod{pqr}.$$

Although this is not the same class of binomial coefficients that we consider in this study, the nature of our results is similar to Theorem 2.

At the end of this study, we also give some minor extensions to binomial coefficients $\binom{a}{b}$ modulo n, for which n does not divide a, by using well-known binomial coefficient identities.

1. Binomial Coefficients Divisible By n

In this section we characterize all values k, $1 \leq k \leq n-1$, such that $\binom{n}{k} \equiv 0 \pmod{n}$. Various results are known concerning the divisibility of binomial coefficients by a positive integer. One of the most useful of these is the so-called Kummer's Theorem.

Theorem 3. *Kummer's Theorem.*
If n and k are integers and p is a prime, then the largest power of p dividing $\binom{n}{k}$ is given by the number of borrows required when subtracting the base p representations of k from n.

The last part of the theorem is often equivalently stated as the number of carries when k and $n-k$ are added in the base p. For convenience we will use the notation $p^a||n$ to mean that a is the largest power of the prime p dividing n. A simple application of Kummer's Theorem gives the following.

Theorem 4. *If m, n, and k are positive integers with $(n,k)=1$, then $\binom{mn}{k} \equiv 0 \pmod{n}$.*

Proof. Let p be an arbitrary prime divisor of n with $p^a||n$. Write $k = k_rp^r + \cdots + k_1p + k_0$ in the base p and note that $k_0 \neq 0$ because $(n,k)=1$. Since $mn = mn_0p^a$ for some integer n_0, subtracting the base p representation of k from mn requires at least a borrows. Kummer's Theorem gives $\binom{mn}{k} \equiv 0 \pmod{p^a}$. The prime p was an arbitrary divisor of n. Thus, $\binom{mn}{k} \equiv 0 \pmod{n}$. □

The converse of this theorem is not true. In fact, $\binom{63}{48} \equiv 0 \pmod{63}$ and $(63,48) = 3 \neq 1$. A true characterization of binomial coefficients congruent to zero is given by the following corollary to Kummer's result.

Corollary 1. *For a positive integer n, $\binom{n}{k} \equiv 0 \pmod{n}$ if and only if for each $p^a||n$ the subtraction of the base p representation of k from n requires at least a borrows.*

Proof. Note that $\binom{n}{k} \equiv 0 \pmod{n}$ if and only if $\binom{n}{k} \equiv 0 \pmod{p^a}$ for all primes p dividing n, where $p^a||n$. By Kummer's Theorem, $\binom{n}{k} \equiv 0 \pmod{p^a}$ if and only if the number of borrows, when subtracting the base p representation of k from n, is at least a. □

In the example $\binom{63}{48} \equiv 0 \pmod{63}$, we have $n = 63 = 3^2 \cdot 7$ and $k = 48$. Taking $p^a = 3^2$, we have $n = 2 \cdot 3^3 + 3^2$ and $k = 3^3 + 2 \cdot 3^2 + 3$. So $n-k$ requires $2 \geq 2 = a$ borrows in the base $p = 3$. Taking $p^a = 7^1$, we have $n = 7^2 + 2 \cdot 7$ and $k = 6 \cdot 7 + 6$. So $n-k$ requires $2 \geq 1 = a$ borrows in the base $p = 7$. Thus, the binomial coefficient has to be congruent to 0 as predicted by the characterization.

2. Binomial Coefficient Residues Modulo n

In this section we are concerned with finding a way to simplify binomial coefficients modulo n. For a prime p, the following theorem of Lucas is well-known.

Theorem 5. *Lucas Theorem.*
If p is a prime and n and k are positive integers with base p representations $n = n_r p^r + \cdots + n_1 p + n_0$ and $k = k_r p^r + \cdots + k_1 p + k_0$, respectively, then

$$\binom{n}{k} = \binom{n_r p^r + \cdots + n_1 p + n_0}{k_r p^r + \cdots + k_1 p + k_0} \equiv \binom{n_r}{k_r} \cdots \binom{n_1}{k_1} \binom{n_0}{k_0} \pmod{p}.$$

The case with a prime power modulus is considered by Davis and Webb [3]. They determined that binomial coefficients modulo p^a depends on blocks of a consecutive digits in the base p representation of n and k.

In addition, we will make use of the following result which is attributed to Jacobsthal in [1] and [3].

Theorem 6. *If n and k are positive integers and p is prime $p > 3$, then*

$$\binom{np}{kp} \equiv \binom{n}{k} \pmod{p^r},$$

where r is the largest power of p dividing $p^3 nk(n-k)\binom{n}{k}$.

In addition, we will need the following theorem for the cases $p = 2$ and $p = 3$ which are consequences of Proposition 5 of [1].

Theorem 7. *If n and k are positive integers and $p = 2$ or $p = 3$, then*

$$\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p^r},$$

where r is the largest power of 3 dividing $18nk(n-k)$.

Thus, in all cases we have the following general result.

Corollary 2. *If n and k are positive integers and p is a prime, then*

$$\binom{pn}{pk} \equiv \binom{n}{k} \pmod{p^r},$$

where r is the largest power of p dividing $pnk(n-k)$.

The remainder of this study focuses on the simplification of binomial coefficients modulo composites. Certainly, one could apply Lucas' Theorem and prime power generalizations for each prime power dividing n then combine these results using the Chinese Remainder Theorem. However, this approach does not easily lend itself to closed form evaluations. Here we focus on closed form methods for evaluating these binomial coefficients in hopes to build on the general theory.

By combining the prime power results we get the main result. But first, we need some definitions.

Definition 1. For positive integers n and k, define

$$A_{n,k} = \{p \text{ prime } : p|(n,k)\}.$$

For any set A, define

$$O(A) = \{B \subseteq A : |B| \text{ is odd}\}, \text{ and}$$

$$E(A) = \{B \subseteq A : |B| \text{ is even}\}.$$

Finally, for a set of primes B, define

$$d_B = \prod_{p \in B} p$$

In addition, define $d_\emptyset = 1$.

Note that if $(n,k) = 1$, then $E(A_{n,k})$ contain one element (the empty set), while $O(A_{n,k})$ contains no elements, and the product on the right below is defined to be zero. Thus, when $(n,k) = 1$, Theorem 8 reduces to Theorem 1.

Theorem 8. *If n, m, and k are positive integers, then*

$$\prod_{B \in E(A_{n,k})} \binom{mn/d_B}{k/d_B} \equiv \prod_{B \in O(A_{n,k})} \binom{mn/d_B}{k/d_B} \pmod{n}.$$

Proof. Let $p^a || n$, where $a > 0$. Consider the two cases where $p \nmid (n,k)$ and $p|(n,k)$.

If p does not divide (n,k), then p does not divide k, so $(p^a, k/d_B) = 1$ for all $B \subseteq A_{n,k}$. Thus, $\binom{mn/d_B}{k/d_B} \equiv 0 \pmod{p^a}$ by Theorem 4. Thus, the congruence holds modulo p^a.

If $p^b || (n,k)$ for some b, $0 < b \leq a$, then we can use Corollary 2 to give a correspondence between each binomial coefficient on the left-hand side of the congruence and a binomial coefficient on the right-hand side of the congruence modulo p^a.

If $B \subseteq A_{n,k}$ and $p \notin B$, then, letting $B' = B \cup \{p\}$, we obtain $\binom{mn/d_B}{k/d_B} \equiv \binom{mn/d_{B'}}{k/d_{B'}} \pmod{p^a}$. To justify this last congruence, write $mn/d_B = \alpha p$ and $k/d_B = \beta p$

and note that p^a divides $p\alpha\beta$ (in particular p^{a-1} divides α) so Corollary 2 ensures that the congruence holds. Finally, note that one of the cardinalities of B and B' is odd and the other is even.

Similarly, if $B \subseteq A_{n,k}$ and $p \in B$, then, letting $B' = B\backslash\{p\}$, we obtain $\binom{mn/d_B}{k/d_B} \equiv \binom{mn/d_{B'}}{k/d_{B'}} \pmod{p^a}$ in the same manner. Thus, there is a one-to-one correspondence for each binomial coefficient from a set B on the left-hand side yielding a congruent binomial coefficient from a set B' on the right-hand side.

Therefore, for all $p^a||n$, we have $\prod_{B\in E(A)} \binom{mn/d_B}{k/d_B} \equiv \prod_{B\in O(A)} \binom{mn/d_B}{k/d_B} \pmod{p^a}$. Hence, the congruence holds modulo n. □

Note that d_B is always square-free as defined. That is, in the theorem above we only ‘cancel’ one factor of each prime p when $p^a|(n,k)$. We may be able to prove more in special cases by using generalizations of Jacobsthal’s result. We leave such an investigation for a different study. Such results would likely lack the elegance and generality of Theorem 8.

As a quick illustration of the usefulness of Theorem 8, consider the following.

Corollary 3. *If p, q and r are primes and m is a positive integer, then*

$$mr\binom{mpqr}{pq} \equiv \binom{mqr}{q}\binom{mpr}{p} \pmod{pqr}.$$

Proof. Note that

$$\prod_{B\in E(A_{pqr,pq})} \binom{mpqr/d_B}{pq/d_B} = \binom{mr}{1}\binom{mpqr}{pq}$$

and

$$\prod_{B\in O(A_{pqr,pq})} \binom{mpqr/d_B}{pq/d_B} = \binom{mpr}{p}\binom{mqr}{q}.$$

Letting $n = pqr$ and $k = pq$ in Theorem 8, we have the result. □

3. Special Cases and Examples

Here we consider special forms for the prime factorization of n. For these special forms we simplify the corresponding binomial coefficients for all k values.

Corollary 4. *If $n = p^a q^b$ is the product of two odd prime powers and m is a positive integer, then*

$$\binom{mn}{k} \equiv \begin{cases} 0 & \pmod{n}\ , \quad \textit{if } (k,n) = 1; \\ \binom{mn/p}{k/p} & \pmod{n}\ , \quad \textit{if } (n,k) = p^j, 1 \le j \le a; \\ \binom{mn/q}{k/q} & \pmod{n}\ , \quad \textit{if } (n,k) = q^j, 1 \le j \le b; \\ \dfrac{\binom{mn/p}{k/p}\binom{mn/q}{k/q}}{\binom{mn/(pq)}{k/(pq)}} & \pmod{n}\ , \quad \textit{if } pq|(n,k). \end{cases}$$

Proof. The first case follows from Theorem 4, the second and third cases follow from Corollary 2, and the fourth case follows from Theorem 8. □

We must be careful when using formulas such as the fourth case of Corollary 4. It is understood that the evaluation and simplification of the binomial coefficients occurs before the expression is evaluated modulo n. This comment is essential since $\binom{mn/(pq)}{k/(pq)}$ is not guaranteed to have an inverse modulo n. Similar evaluations can be given when n has more than two prime factors.

To illustrate these ideas we give the following examples:

(1) Consider the following binomial coefficient modulo 323. Here, $m = 1$, $n = 323$, $k = 85$, $p = 17$.

$$\binom{323}{85} = \binom{17 \cdot 19}{5 \cdot 17} \equiv \binom{19}{5} \pmod{323}.$$

(2) Consider the following binomial coefficient modulo 30.

$$\binom{30}{15} = \binom{2 \cdot 3 \cdot 5}{3 \cdot 5} \equiv \frac{\binom{2 \cdot 5}{5}\binom{2 \cdot 3}{3}}{\binom{2}{1}} = \frac{1}{2}\binom{10}{5}\binom{6}{3} \pmod{30}.$$

In general, Theorem 8 allows for the evaluation of $\binom{mn}{k}$ in terms of binomial coefficients involving smaller numbers modulo n as is given below.

Theorem 9. *If n, m and k are positive integers, then*

$$\binom{mn}{k} \equiv \begin{cases} 0 \pmod{n} & , \text{ if } (n,k)=1 \\ \dfrac{\prod_{B\in O(A)} \binom{mn/n_B}{k/n_B}}{\prod_{B\in E(A)\setminus\{\varnothing\}} \binom{mn/n_B}{k/n_B}} \pmod{n} & , \text{ if } (n,k)>1. \end{cases}$$

4. Composite Moduli and General Binomial Coefficients

The study so far has only focused on binomial coefficients of the form $\binom{mn}{k}$ modulo n. Now we show how these results can be extended to general coefficients of the form $\binom{a}{b}$ modulo n.

By using the following lemma, we will be able to attack binomial coefficients in general.

Lemma 1. *If a, b, and k are positive integers, then* $\binom{a}{b} = \sum_{j=0}^{k} \binom{k}{j}\binom{a-k}{b-j}$.

Proof. This result is given by repeated application of the identity $\binom{a}{b} = \binom{a-1}{b} + \binom{a-1}{b-1}$. □

Thus, given a binomial coefficient $\binom{a}{b}$ with $a \geq n$ we can use Lemma 1 in combination with our previous results by writing $a = mn + k$.

Corollary 5. *If n, a and b are positive integers such that $a = mn + k$, then*

$$\binom{a}{b} = \binom{mn+k}{b} = \sum_{j=0}^{k} \binom{k}{j}\binom{mn}{b-j}.$$

When evaluating this sum modulo n, Theorem 4 guarantees that the only nonzero terms are those where $(b-j,n) > 1$.

Theorem 10. *If n, a and b are positive integers such that $a = mn + k$, then*

$$\binom{a}{b} = \sum_{\substack{j=0 \\ (b-j,n)>1}}^{k} \binom{k}{j}\binom{mn}{b-j} \pmod{n}.$$

We can draw several conclusions from this. Here is one such result.

Corollary 6. *If n, a and b are positive integer such that $a = mn+k$, $b \geq k$, and $(\frac{b!}{(b-k)!}, n) = 1$, then $\binom{a}{b} \equiv \binom{mn}{b-k} \pmod{n}$.*

Proof. Since $(\frac{b!}{(b-k)!}, n) = 1$, we have $(b-j, n) = 1$ for $j = 0, 1, \dots k-1$. Hence, $\binom{a}{b} = \binom{mn}{b-k}$ $+ \sum_{j=0}^{k-1} \binom{k}{j}\binom{mn}{b-j} \equiv \binom{mn}{b-k}$ $+0 \pmod{n}$, by Theorem 4. □

As a summary example, letting $n = 35$ we evaluate the binomial coefficient:

$$\begin{aligned} \binom{38}{13} &\equiv \binom{35}{10} && \text{, by Corollary 5, since } (35, 13 \cdot 12 \cdot 11) = 1. \\ &= \binom{5 \cdot 7}{2 \cdot 5} \equiv \binom{7}{2} && \text{, by Theorem 8 or Corollary 2.} \\ &= 21 \pmod{35}. \end{aligned}$$

5. Conclusions

Hopefully, these results give added insight into the properties of these important numbers. Thank you to my advisor Prof. William Webb who introduced me to the interesting divisibility properties of binomial coefficients. I also sincerely thank the referee who corrected several small typos and greatly improved the presentation and clarity of this article.

References

[1] A. Granville: *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers.* Organic mathematics (Burnaby, BC, 1995), 253-276. CMS Conf. Proc. 20, Amer. Math. Soc. Providence, RI, 1997.

[2] I. Vardi: *Computational Recreations in Mathematica.* Addison-Wesley Publishing Company, 1991

[3] K.S. Davis and W.A. Webb: *Lucas' Theorem for prime powers.* Europ. J. Combinatorics, 11 (1990), 229-233.