ON BINOMIAL COEFFICIENTS MODULO SQUARES OF PRIMES

Darij Grinberg

School of Mathematics, University of Minnesota, Minneapolis, Minnesota
darijgrinberg@gmail.com

Received: 12/6/17, Revised: 10/8/18, Accepted: 1/6/19, Published: 2/1/19

Abstract

We give elementary proofs for the Apagodu-Zeilberger-Stanton-Amdeberhan-Tauraso congruences

\[
\sum_{n=0}^{rp-1} \binom{2n}{n} \equiv \eta_p \sum_{n=0}^{r-1} \binom{2n}{n} \mod p^2,
\]

\[
\sum_{n=0}^{rp-1} \sum_{m=0}^{sp-1} \binom{n+m}{m}^2 \equiv \eta_p \sum_{n=0}^{r-1} \sum_{m=0}^{s-1} \binom{n+m}{m}^2 \mod p^2,
\]

where \( p \) is an odd prime, \( r \) and \( s \) are nonnegative integers, and

\[
\eta_p = \begin{cases} 
0, & \text{if } p \equiv 0 \mod 3; \\
1, & \text{if } p \equiv 1 \mod 3; \\
-1, & \text{if } p \equiv 2 \mod 3.
\end{cases}
\]

1. Introduction

In this note, we prove that any odd prime \( p \) and any \( r, s \in \mathbb{N} \) satisfy

\[
\sum_{n=0}^{rp-1} \binom{2n}{n} \equiv \eta_p \sum_{n=0}^{r-1} \binom{2n}{n} \mod p^2 \quad \text{(Theorem 3)};
\]

\[
\sum_{n=0}^{rp-1} \sum_{m=0}^{sp-1} \binom{n+m}{m}^2 \equiv \eta_p \sum_{n=0}^{r-1} \sum_{m=0}^{s-1} \binom{n+m}{m}^2 \mod p^2 \quad \text{(Theorem 4)},
\]

where

\[
\eta_p = \begin{cases} 
0, & \text{if } p \equiv 0 \mod 3; \\
1, & \text{if } p \equiv 1 \mod 3; \\
-1, & \text{if } p \equiv 2 \mod 3.
\end{cases}
\]
These two congruences are (slightly extended) versions of the “Super-Conjectures” 1’’ and 4' stated by Apagodu and Zeilberger in [3]1. Our proofs are more elementary than previous proofs by Stanton [16], and Amdeberhan and Tauraso [1].

A more detailed version of the present paper is available on the arXiv [10].

1.1. Binomial Coefficients

Let us first recall the definition of binomial coefficients.2

**Definition 1.** Let \( n \in \mathbb{Z} \) and \( m \in \mathbb{Z} \). Then, the binomial coefficient \( \binom{m}{n} \) is a rational number defined by

\[
\binom{m}{n} = \begin{cases} 
\frac{m(m-1)\cdots(m-n+1)}{n!}, & \text{if } n \in \mathbb{N}; \\
0, & \text{if } n \notin \mathbb{N}.
\end{cases}
\]

This is the definition used in [7] and [9]. Some authors follow other conventions instead.

The following proposition is well-known (see, e.g., [9, Proposition 1.9]), and will be tacitly used below (as we study congruences involving binomial coefficients).

**Proposition 1.** We have \( \binom{m}{n} \in \mathbb{Z} \) for any \( m \in \mathbb{Z} \) and \( n \in \mathbb{Z} \).

1.2. Classical Congruences

The behavior of binomial coefficients modulo primes and prime powers is a classical subject of research; see [14, §2.1] for a survey of much of it. Let us state two of the most basic results in this subject.

**Theorem 1.** Let \( p \) be a prime. Let \( a \) and \( b \) be two integers. Let \( c \) and \( d \) be two elements of \( \{0, 1, \ldots, p-1\} \). Then,

\[
\binom{ap + c}{bp + d} \equiv \frac{a}{b} \binom{c}{d} \mod p.
\]

Theorem 1 is known under the name of *Lucas’s theorem*, and is proven in many places (e.g., [14, §2.1], [11, Proof of §4], [2, proof of Lucas’s theorem] and [7, Exercise 5.61]) at least in the case when \( a \) and \( b \) are nonnegative integers. The standard proof of Theorem 1 in this case uses generating functions; this proof applies (mutatis mutandis) in the general case as well. See [9, Theorem 1.11] for an elementary proof of Theorem 1.

Another fundamental result is the following.

---


2We use the notation \( \mathbb{N} \) for the set \( \{0, 1, 2, \ldots\} \).
**Theorem 2.** Let $p$ be a prime. Let $a$ and $b$ be two integers. Then,

$$\left(\frac{ap}{bp}\right) \equiv \left(\frac{a}{b}\right) \mod p^2.$$ 

Theorem 2 is a known result, often attributed to Charles Babbage. It appears with proof in [9, Theorem 1.12]; again, many sources prove it for nonnegative $a$ and $b$ (such as [15, Exercise 1.14 c] or [7, Exercise 5.62]). Notice that if $p \geq 5$, then the modulus $p^2$ can be replaced by $p^3$ or (depending on $a$, $b$ and $p$) by even higher powers of $p$; see [14, (22) and (23)] for the details. See also [17, Lemma 2.1] for another strengthening of Theorem 2.

**1.3. Modulo-$p^2$ Congruences**

**Definition 2.** For any $p \in \mathbb{Z}$, we define an integer $\eta_p \in \{-1, 0, 1\}$ by

$$\eta_p = \begin{cases} 0, & \text{if } p \equiv 0 \mod 3; \\ 1, & \text{if } p \equiv 1 \mod 3; \\ -1, & \text{if } p \equiv 2 \mod 3. \end{cases}$$

Notice that $\eta_p$ is the so-called Legendre symbol $\left(\frac{p}{3}\right)$ known from number theory.

We are now ready to state two conjectures by Apagodu and Zeilberger, which we shall prove in the sequel. The first one is [3, Super-Conjecture 1”].

**Theorem 3.** Let $p$ be an odd prime. Let $r \in \mathbb{N}$. Set

$$\alpha_r = \sum_{n=0}^{r-1} \binom{2n}{n}.$$ 

Then,

$$\sum_{n=0}^{r-1} \binom{2n}{n} \equiv \eta_p \alpha_r \mod p^2.$$ 

Theorem 3 has been proven by Dennis Stanton [16] using Laurent series (in the case when $p \geq 5$), and by Liu [12, (1.3)] using harmonic numbers. We shall reprove it elementarily. Note that we can apply Theorem 3 to $r = 1$, and obtain the congruence

$$\sum_{n=0}^{p-1} \binom{2n}{n} \equiv \eta_p \mod p^2$$

for each odd prime $p$; this is [3, Super-Conjecture 1].

The next conjecture that we shall prove is [3, Super-Conjecture 5’].

---

3To be precise (and boastful), our Theorem 3 is somewhat stronger than [3, Super-Conjecture 1’], since we only require $p$ to be odd (rather than $p \geq 5$). The same remark applies to Theorem 4. That said, the $p = 3$ case may well fall prey to simpler methods.
Theorem 4. Let \( p \) be an odd prime. Let \( r \in \mathbb{N} \) and \( s \in \mathbb{N} \). Set
\[
e_{r,s} = \sum_{m=0}^{r-1} \sum_{n=0}^{s-1} \binom{n+m}{m}^2.
\]
Then,
\[
r^p \sum_{n=0}^{r-1} \sum_{m=0}^{s-1} \binom{n+m}{m}^2 \equiv n_p \epsilon_{r,s} \mod p^2.
\]
A proof of Theorem 4 has been found by Amdeberhan and Tauraso, and was outlined in [1, §6]; we give a different, elementary proof.

1.4. Bailey’s Congruence and Analogues

On our way to proving the above two theorems, we shall show a modulo-\( p^2 \) congruence for certain binomial coefficients that can be regarded as a counterpart to Theorem 2.

Theorem 5. Let \( p \) be a prime. Let \( N \in \mathbb{Z} \) and \( K \in \mathbb{Z} \) and \( i \in \{1, 2, \ldots, p-1\} \). Then we have

(a) \[
\binom{Np}{Kp+i} \equiv N\binom{N-1}{K} \binom{p}{i} \mod p^2;
\]

(b) \[
\binom{Np}{Kp-i} \equiv N\binom{N-1}{K-1} \binom{p}{i} \mod p^2;
\]

(c) \[
\binom{Np}{Kp+i} + \binom{Np}{Kp-i} \equiv N\binom{N}{K} \binom{p}{i} \mod p^2.
\]

Theorem 5 (a) is essentially the result [4, Theorem 4] by Bailey (see also [14, (26)]); in fact, it transforms into [4, Theorem 4] if we rewrite \( N\binom{N-1}{K} \) as \( (K+1)\binom{N}{K+1} \) (using Proposition 8 below). We shall nevertheless give our own proof for it.

1.5. Polynomial Summation

Let us state two further lemmas that will be crucial to our proofs of Theorems 3 and 4, but are likely to have other uses as well.

Let \( \mathbb{Z}[X] \) be the ring of all polynomials in one indeterminate \( X \) with integer coefficients. It is well-known that all integers \( p, c \) and \( l \) and every polynomial \( P \in \mathbb{Z}[X] \)
Theorem 1. Let \( p \) be a prime. Let \( c \in \mathbb{Z} \). Let \( P \in \mathbb{Z}[X] \) be a polynomial of degree < 2p – 1. Then, \( \sum_{l=0}^{p-1} (P(cp + l) - P(l)) \equiv 0 \pmod{p^2} \).

Lemma 2. Let \( p \) be an odd prime. Let \( c \in \mathbb{Z} \). Let \( P \in \mathbb{Z}[X] \) be a polynomial of degree \( \leq p - 1 \). Then, \( \sum_{l=0}^{p-1} (P(cp + l) - P(l)) P(l) \equiv 0 \pmod{p^2} \).

2. The Proofs

2.1. Identities and Congruences From the Literature

Before we come to the proofs of the above-listed results, let us collect various well-known facts that will prove useful.

We assume that the reader is familiar with standard properties of binomial coefficients (see, e.g., [8, §3.1], [7, Chapter 5] or [9, §1]):

Proposition 2. We have \( \binom{m}{n} = 0 \) for every \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfying \( m < n \).

Proposition 3. Let \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfy \( m \geq n \). Then, \( \binom{m}{n} = \binom{m}{m-n} \).

Proposition 4. Let \( m \in \mathbb{Z} \) and \( n \in \mathbb{N} \). Then, \( \binom{m}{n} = (-1)^n \binom{n-m-1}{n} \).

Proposition 5. Let \( m \in \mathbb{Z} \) and \( n \in \mathbb{Z} \). Then, \( \binom{m}{n} = \binom{m-1}{n-1} + \binom{m-1}{n} \).

Proposition 6. For every \( x \in \mathbb{Z} \) and \( y \in \mathbb{Z} \) and \( n \in \mathbb{N} \), we have

\[
\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k} \binom{y}{n-k}.
\]

Proposition 6 is the so-called Vandermonde convolution identity, and is a particular case of [8, Theorem 3.29].
Proposition 7. For each $n \in \mathbb{N}$, we have
\[
\sum_{i=0}^{n-1} (-1)^i \binom{n-1-i}{i} = (-1)^n \cdot \begin{cases} 
0, & \text{if } n \equiv 0 \mod 3; \\
-1, & \text{if } n \equiv 1 \mod 3; \\
1, & \text{if } n \equiv 2 \mod 3.
\end{cases}
\]
Proposition 7 is [8, Corollary 8.68]. Apart from that, Proposition 7 can be easily derived from [7, §5.2, Problem 3], [5, Identity 172] or [6].

Proposition 8. Let $n \in \mathbb{Z}$ and $k \in \mathbb{Z}$. Then, $k \binom{n}{k} = n \binom{n-1}{k-1}$.

Proposition 8 (sometimes known as the “absorption identity”) appears in [7, (5.6)], and is easily proven just from the definition of binomial coefficients.

Let us also recall a result from elementary number theory:

Theorem 6. Let $p$ be a prime. Let $k \in \mathbb{N}$. Assume that $k$ is not a positive multiple of $p - 1$. Then,
\[
\sum_{i=0}^{p-1} i^k \equiv 0 \mod p.
\]
Theorem 6 is proven, e.g., in [9, Theorem 3.1] and (in a slightly rewritten form) in [13, Theorem 1].

2.2. Variants and Consequences of Vandermonde Convolution

We are now going to state a number of identities that are restatements or particular cases of the Vandermonde convolution identity (Proposition 6). We begin with the following one.

Corollary 1. Let $u \in \mathbb{Z}$ and $l \in \mathbb{N}$ and $w \in \mathbb{N}$. Then,
\[
\sum_{m=0}^{l} \binom{u}{w+m} \binom{l}{m} = \binom{u+l}{w+l}.
\]

Proof of Corollary 1. Proposition 6 (applied to $x = u$, $y = l$ and $n = w+l$) yields
\[
\binom{u+l}{w+l} = \sum_{k=0}^{w+l} \binom{u}{k} \binom{l}{w+l-k} = \sum_{k=0}^{w-1} \binom{u}{k} \binom{l}{w+l-k} + \sum_{k=w}^{w+l} \binom{u}{k} \binom{l}{w+l-k}
\]
(by Proposition 2
(since $l < w+l-k$
(because $k < w$))

\[
= \sum_{k=w}^{w+l} \binom{u}{k} \binom{l}{w+l-k} = \sum_{m=0}^{l} \binom{u}{w+m} \binom{l}{w+l-(w+m)}
\]
(by Proposition 3)
(here, we have substituted $w + m$ for $k$ in the sum)

\[
= \sum_{m=0}^{i} \binom{u}{w + m} \binom{l}{m}.
\]

This proves Corollary 1. \qed

Let us also state another corollary of Proposition 6.

**Corollary 2.** Let $x \in \mathbb{Z}$ and $y \in \mathbb{N}$ and $n \in \mathbb{Z}$. Then,

\[
\binom{x + y}{n} = \sum_{i=0}^{y} \binom{x}{n - i} \binom{y}{i}.
\]

See [9, Corollary 2.2] for a proof of Corollary 2.

**Lemma 3.** Let $u \in \mathbb{Z}$ and $w \in \mathbb{N}$ and $l \in \mathbb{N}$. Then,

\[
\binom{u + 2l}{w + l} = \binom{u}{w} \binom{2l}{l} + \sum_{i=1}^{l} \left( \binom{u}{w + i} + \binom{u}{w - i} \right) \binom{2l}{l - i}.
\]

**Proof of Lemma 3.** Corollary 2 (applied to $x = u$, $y = 2l$, and $n = w + l$) yields

\[
\binom{u + 2l}{w + l} = \sum_{i=0}^{2l} \binom{u}{w + l - i} \binom{2l}{i} = \sum_{i=-l}^{l} \binom{u}{w + i} \binom{2l}{l - i}
\]

(here, we have substituted $l - i$ for $i$ in the sum)

\[
= \sum_{i \in \{-l, \ldots, l-1, \ldots, l\}; i \neq 0} \left( \binom{u}{w + i} \binom{2l}{l - i} + \binom{u}{w} \binom{2l}{l} \right)
\]

(here, we have split off the addend for $i = 0$ from the sum). Hence,

\[
\binom{u + 2l}{w + l} - \binom{u}{w} \binom{2l}{l} = \sum_{i \in \{-l, \ldots, l\}; i \neq 0} \left( \binom{u}{w + i} \binom{2l}{l - i} \right)
\]

\[
= \sum_{i=1}^{l} \binom{u}{w + i} \binom{2l}{l - i} + \sum_{i=-l}^{l-1} \binom{u}{w + i} \binom{2l}{l - i}
\]

\[
= \sum_{i=1}^{l} \binom{u}{w + i} \binom{2l}{l - i} + \sum_{i=1}^{l} \binom{u}{w - i} \binom{2l}{l + i}
\]

(by Proposition 3)
Lemma: 19 (2019)

\[
\integ{\text{here, we have substituted } - i \text{ for } i}
\]
\[
= \sum_{i=1}^{l} \left( \binom{u}{w+i} + \binom{u}{w-i} \right) \binom{2l}{l-i}.
\]

Adding \( \binom{u}{w} \binom{2l}{l} \) to both sides yields the claim of Lemma 3.

Lemma 4. Let \( p \in \mathbb{N} \). Let \( c \in \mathbb{Z} \). Let \( l \in \{0, 1, \ldots, p-1\} \). Then,

\[
\binom{cp+2l}{l} = \sum_{k=0}^{p-1} \binom{cp+l}{k} \binom{l}{k}.
\]

Proof of Lemma 4. Corollary 2 (applied to \( x = cp+l, y = l \) and \( n = l \)) yields

\[
\binom{cp+2l}{l} = \sum_{i=0}^{l} \binom{cp+l}{l-i} \binom{l}{i} = \sum_{k=0}^{l} \binom{cp+l}{k} \binom{l}{l-k} = \binom{l}{k} \quad \text{(by Proposition 3)}
\]

(here, we have substituted \( k \) for \( l-i \) in the sum)

\[
= \sum_{k=0}^{l} \binom{cp+l}{k} \binom{l}{k}.
\]

Comparing this with

\[
\sum_{k=0}^{p-1} \binom{cp+l}{k} \binom{l}{k} = \sum_{k=0}^{l} \binom{cp+l}{k} \binom{l}{k} + \sum_{k=l+1}^{p-1} \binom{cp+l}{k} \binom{l}{k} = \binom{cp+2l}{l} \quad \text{(by Proposition 2)}
\]

(applied to \( m = l \) and \( n = k \))

\[\text{(since } l < k)\]

\[
= \sum_{k=0}^{l} \binom{cp+l}{k} \binom{l}{k},
\]

we obtain \( \sum_{k=0}^{p-1} \binom{cp+l}{k} \binom{l}{k} = \binom{cp+2l}{l} \). This proves Lemma 4.

Lemma 5. Let \( p \in \mathbb{N} \). Let \( l \in \mathbb{N} \). Then,

\[
\sum_{i=1}^{l} \binom{p}{i} \binom{2l}{l-i} = \binom{p+2l}{l} - \binom{2l}{l}.
\]
Proof of Lemma 5. Proposition 6 (applied to $x = p$, $y = 2l$ and $n = l$) yields

\[
\binom{p + 2l}{l} = \sum_{k=0}^{l} \binom{p}{k} \binom{2l}{l-k} = \sum_{i=0}^{l} \binom{p}{i} \binom{2l}{l-i}.
\]

(here, we have renamed the summation index $k$ as $i$)

\[
= \binom{p}{0} \binom{2l}{l-0} + \sum_{i=1}^{l} \binom{p}{i} \binom{2l}{l-i} = \binom{2l}{l} + \sum_{i=1}^{l} \binom{p}{i} \binom{2l}{l-i}.
\]

Solving this equality for $\sum_{i=1}^{l} \binom{p}{i} \binom{2l}{l-i}$, we obtain Lemma 5. \(\square\)

2.3. Proof of Bailey’s Congruence

Proof of Theorem 5. From $i \in \{1, 2, \ldots, p - 1\}$, we conclude that both $i - 1$ and $p - i$ are elements of $\{0, 1, \ldots, p - 1\}$. Notice also that $i$ is not divisible by $p$ (since $i \in \{1, 2, \ldots, p - 1\}$); hence, $i$ is coprime to $p$ (since $p$ is a prime). Therefore, $i$ is also coprime to $p^2$.

(a) Proposition 8 (applied to $n = np$ and $k = kp + i$) yields

\[
(Kp + i) \binom{np}{Kp + i} = np \binom{np - 1}{Kp + i - 1} = np \left( \binom{(N - 1)p + (p - 1)}{Kp + (i - 1)} \right)
\]

\[
\equiv \binom{N - 1}{K} \binom{p - 1}{i - 1} \mod p \equiv \binom{np}{Kp + i} \mod p^2
\]

(1)

(notice that the presence of the $p$ factor has turned a congruence modulo $p$ into a congruence modulo $p^2$). Thus,

\[
(Kp + i) \binom{np}{Kp + i} \equiv np \binom{N - 1}{i - 1} \equiv 0 \mod p,
\]

so that $0 \equiv (Kp + i) \binom{np}{Kp + i} \equiv i \binom{np}{Kp + i} \mod p$. We can cancel $i$ from this congruence (since $i$ is coprime to $p$), and thus obtain $0 \equiv \binom{np}{Kp + i} \mod p$. Hence,
\( \binom{Np}{Kp + i} \) is divisible by \( p \). Thus, \( p \binom{Np}{Kp + i} \) is divisible by \( p^2 \). In other words,

\[
p \binom{Np}{Kp + i} \equiv 0 \mod p^2. \tag{2}
\]

Now,

\[
(Kp + i) \binom{Np}{Kp + i} = Kp \binom{Np}{Kp + i} + i \binom{Np}{Kp + i} \equiv i \binom{Np}{Kp + i} \mod p^2.
\]

Hence,

\[
i \binom{Np}{Kp + i} \equiv (Kp + i) \binom{Np}{Kp + i} \equiv Np \binom{N - 1}{K} \binom{p - 1}{i - 1} \quad \text{(by (1))}
\]

\[
= N \binom{N - 1}{K} \binom{p}{i} \equiv \binom{p}{i} \mod p^2.
\]

(by Proposition 8)

We can cancel \( i \) from this congruence (since \( i \) is coprime to \( p^2 \)), and thus obtain

\[
\binom{Np}{Kp + i} \equiv N \binom{N - 1}{K} \binom{p}{i} \mod p^2.
\]

This proves Theorem 5 (a).

(b) We have \( i \in \{1, 2, \ldots, p - 1\} \) and thus \( p - i \in \{1, 2, \ldots, p - 1\} \). Hence, Theorem 5 (a) (applied to \( K - 1 \) and \( p - i \) instead of \( K \) and \( i \)) yields

\[
\binom{Np}{(K - 1)p + (p - i)} \equiv N \binom{N - 1}{K - 1} \binom{p}{p - i} = N \binom{N - 1}{K - 1} \binom{p}{i} \mod p^2.
\]

(by Proposition 3)

In view of \( (K - 1)p + (p - i) = Kp - i \), this can be rewritten as

\[
\binom{Np}{Kp - i} \equiv N \binom{N - 1}{K - 1} \binom{p}{i} \mod p^2.
\]

This proves Theorem 5 (b).
(c) We have
\[
\binom{Np}{Kp+i} + \binom{Np}{Kp-i} \\
\equiv N \binom{N-1}{K} \left( \frac{p}{i} \right)^{\text{mod } p^2} \quad \text{(by Theorem 5 (a))}
\]
\[
\equiv N \binom{N-1}{K} \left( \frac{p}{i} \right) + \binom{N-1}{K-1} \left( \frac{p}{i} \right) \\
\equiv N \left( \frac{N-1}{K} + \frac{N-1}{K-1} \right) \left( \frac{p}{i} \right) = N \binom{N}{K} \left( \frac{p}{i} \right)^{\text{mod } p^2}.
\]
(by Proposition 5)

This proves Theorem 5 (c).

2.4. Proofs of Lemmas 1 and 2

Proof of Lemma 1. WLOG assume that \( P = X^k \) for some \( k \in \{0, 1, \ldots, 2p-2\} \) (since the congruence we are proving depends \( \mathbb{Z} \)-linearly on \( P \)). If \( k = 0 \), then Lemma 1 is easily checked. Thus, WLOG assume that \( k \neq 0 \). Hence, \( k-1 \in \mathbb{N} \).

We have \( P = X^k \). Thus, each \( l \in \{0, 1, \ldots, p-1\} \) satisfies

\[
P(cp + l) = (cp + l)^k = \sum_{i=0}^{k} \binom{k}{i} (cp)^{i} l^{k-i} \quad \text{(by the binomial formula)}
\]
\[
= (cp)^0 l^{k-0} + \sum_{i=2}^{k} \binom{k}{i} (cp)^{i} l^{k-1} \quad \text{(since \( i \geq 2 \))}
\]
\[
\equiv l^k + kcp^{k-1} \mod p^2
\]
and \( P(l) = l^k \) (since \( P = X^k \)). Thus,

\[
\sum_{l=0}^{p-1} \left( P(cp + l) - P(l) \right) \equiv \sum_{l=0}^{p-1} (l^k + kcp^{k-1} - l^k) = kcp \sum_{l=0}^{p-1} l^{k-1} \mod p^2.
\]

The claim of Lemma 1 now becomes obvious if \( k = p \) (because if \( k = p \), then \( kcp \) is already divisible by \( p^2 \)); thus, we WLOG assume that \( k \neq p \). Hence, \( k-1 \neq p-1 \).

If \( k-1 \) was a positive multiple of \( p-1 \), then we would have \( k-1 = p-1 \) (since \( k \in \{0, 1, \ldots, 2p-2\} \)), which would contradict \( k-1 \neq p-1 \). Hence, \( k-1 \) is not a
positive multiple of \( p - 1 \). Thus, Theorem 6 (applied to \( k - 1 \) instead of \( k \)) yields
\[
\sum_{l=0}^{p-1} l^{k-1} \equiv 0 \mod p.
\]
Thus, \( p \sum_{l=0}^{p-1} l^{k-1} \equiv 0 \mod p^2 \), so that
\[
\sum_{l=0}^{p-1} (P(cp + l) - P(l)) \equiv kcp \sum_{l=0}^{p-1} l^{k-1} \equiv 0 \mod p^2.
\]

This proves Lemma 1.

**Lemma 6.** Let \( p, a \) and \( b \) be integers such that \( a - b \) is divisible by \( p \). Then, \( a^2 - b^2 \equiv 2(a-b)b \mod p^2 \).

**Proof of Lemma 6.** The difference \( (a^2 - b^2) - 2(a-b)b = (a-b)^2 \) is divisible by \( p^2 \) (since \( a-b \) is divisible by \( p \)). In other words, \( a^2 - b^2 \equiv 2(a-b)b \mod p^2 \). Lemma 6 is proven.

**Proof of Lemma 2.** Fix \( l \in \mathbb{Z} \). We have \( P \in \mathbb{Z}[X] \). Thus, \( P(u) - P(v) \) is divisible by \( u - v \) whenever \( u \) and \( v \) are two integers. Applying this to \( u = cp + l \) and \( v = l \), we conclude that \( P(cp + l) - P(l) \) is divisible by \( (cp + l) - l = cp \), and thus also divisible by \( p \). Hence, Lemma 6 (applied to \( a = P(cp + l) \) and \( b = P(l) \)) yields
\[
(P(cp + l))^2 - (P(l))^2 \equiv 2(P(cp + l) - P(l)) P(l) \mod p^2. \tag{3}
\]

Now, forget that we fixed \( l \). We thus have proven (3) for each \( l \in \mathbb{Z} \).

The polynomial \( P \) has degree \( \leq p - 1 \). Hence, the polynomial \( P^2 \) has degree \( \leq 2(p - 1) < 2p - 1 \). Thus, Lemma 1 (applied to \( P^2 \) instead of \( P \)) shows that
\[
\sum_{l=0}^{p-1} (P^2(cp + l) - P^2(l)) \equiv 0 \mod p^2.
\]

Thus,
\[
0 \equiv \sum_{l=0}^{p-1} \underbrace{(P^2(cp + l) - P^2(l))}_{=(P(cp+l))^2 - (P(l))^2} \equiv 2 \sum_{l=0}^{p-1} (P(cp + l) - P(l)) P(l) \mod p^2.
\]

We can cancel 2 from this congruence (since \( p \) is odd), and conclude that
\[
0 \equiv \sum_{l=0}^{p-1} (P(cp + l) - P(l)) P(l) \mod p^2.
\]

This proves Lemma 2.  

\footnote{This is a well-known fact, and easily proven.}
2.5. Applying Lemma 2

Now, let us prepare for the proofs of our results by showing several lemmas.

**Lemma 7.** Let $p$ be an odd prime. Let $c \in \mathbb{Z}$. Let $k \in \{0, 1, \ldots, p - 1\}$. Then,

$$
\sum_{l=0}^{p-1} \left( \binom{cp + l}{k} - \binom{l}{k} \right) \equiv 0 \mod p^2.
$$

*Proof of Lemma 7.* Notice that $k!$ is coprime to $p$ (since $k \leq p - 1$), and thus $k!^2$ is coprime to $p^2$.

Define a polynomial $P \in \mathbb{Z}[X]$ by $P = X(X - 1) \cdots (X - k + 1)$. Then, $P$ has degree $k \leq p - 1$. Thus, Lemma 2 yields

$$
\sum_{l=0}^{p-1} (P(cp + l) - P(l)) \equiv 0 \mod p^2.
$$

Since each $n \in \mathbb{Z}$ satisfies $P(n) = n(n - 1) \cdots (n - k + 1) = k!^2 \binom{n}{k}$, this can be rewritten as

$$
\sum_{l=0}^{p-1} \left( k!(cp + l) - k! \binom{l}{k} \right) \equiv 0 \mod p^2.
$$

We can cancel $k!^2$ from this congruence (since $k!^2$ is coprime to $p^2$), and thus obtain

$$
\sum_{l=0}^{p-1} \left( \binom{cp + l}{k} - \binom{l}{k} \right) \equiv 0 \mod p^2.
$$

This proves Lemma 7.

**Lemma 8.** Let $p$ be an odd prime. Let $c \in \mathbb{Z}$. Then,

$$
\sum_{l=0}^{p-1} \left( \binom{cp + 2l}{l} - \binom{2l}{l} \right) \equiv 0 \mod p^2.
$$

*Proof of Lemma 8.* For each $l \in \{0, 1, \ldots, p - 1\}$, we have

$$
\binom{cp + 2l}{l} - \binom{2l}{l} = \sum_{k=0}^{p-1} \left( \binom{cp + l}{k} - \binom{l}{k} \right) \binom{l}{k}.
$$

(by Lemma 4, applied to $0$ instead of $c$)
Summing these equalities over all \( l \in \{0, 1, \ldots, p - 1\} \), we find
\[
\sum_{l=0}^{p-1} \left( \binom{cp + 2l}{l} - \binom{2l}{l} \right) = \sum_{l=0}^{p-1} \sum_{k=0}^{p-1} \left( \binom{cp + l}{k} - \binom{l}{k} \right) \binom{l}{k} = \sum_{k=0}^{p-1} 0 = 0 \mod p^2.
\]

This proves Lemma 8. \( \square \)

2.6. \( \eta_p \) Appears

Let us now prove the particular case of Theorem 3 for \( r = 1 \):

**Theorem 7.** Let \( p \) be an odd prime. Then,
\[
\sum_{n=0}^{p-1} \binom{2n}{n} \equiv \eta_p \mod p^2.
\]

**Proof of Theorem 7.** Lemma 8 (applied to \( c = -1 \)) yields
\[
\sum_{l=0}^{p-1} \left( \binom{-p + 2l}{l} - \binom{2l}{l} \right) \equiv 0 \mod p^2.
\]

Moving all the \( \binom{2l}{l} \) addends to the right-hand side of this congruence, we obtain
\[
\sum_{l=0}^{p-1} \binom{-p + 2l}{l} \equiv \sum_{l=0}^{p-1} \binom{2l}{l} \mod p^2. \tag{4}
\]

Now,
\[
\sum_{n=0}^{p-1} \binom{2n}{n} = \sum_{l=0}^{p-1} \binom{2l}{l} \equiv \sum_{l=0}^{p-1} \binom{-p + 2l}{l} \equiv (-1)^l \binom{l - (-p + 2l) - 1}{l}, \tag{by (4)}
\]

(by Proposition 4)
\[
= \sum_{l=0}^{p-1} (-1)^l \binom{l - (-p + 2l) - 1}{l} = \sum_{l=0}^{p-1} (-1)^l \binom{p - 1 - l}{l}.
\]
\[\sum_{i=0}^{p-1} (-1)^i \binom{p-1-i}{i} = (-1)^p \cdot \begin{cases} 0, & \text{if } p \equiv 0 \mod 3; \\ -1, & \text{if } p \equiv 1 \mod 3; \\ 1, & \text{if } p \equiv 2 \mod 3 \end{cases}
\]

(by Proposition 7, applied to \(n = p\))

\[= - \begin{cases} 0, & \text{if } p \equiv 0 \mod 3; \\ -1, & \text{if } p \equiv 1 \mod 3; \\ 1, & \text{if } p \equiv 2 \mod 3 \end{cases} \equiv \eta_p \mod p^2. \]

2.7. Proving Theorem 3

**Lemma 9.** Let \(N \in \mathbb{Z}\) and \(K \in \mathbb{N}\). Let \(p\) be a prime. Let \(l \in \{0, 1, \ldots, p-1\}\). Then,

\[
\binom{Np + 2l}{Kp + l} - \binom{N}{K} \binom{2l}{l} = N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \mod p^2.
\]

**Proof of Lemma 9.** Theorem 2 yields \(\binom{Np}{Kp} \equiv \binom{N}{K} \mod p^2\).

Lemma 3 (applied to \(u = Np\) and \(w = Kp\)) yields

\[
\binom{Np + 2l}{Kp + l} = \binom{Np}{Kp} \binom{2l}{l} + \sum_{i=1}^{l} \left( \binom{Np}{Kp + i} + \binom{Np}{Kp - i} \right) \binom{2l}{l - i}
\]

\[\equiv \binom{N}{K} \mod p^2 \equiv \binom{N}{K} \binom{p}{i} \mod p^2 \quad \text{(by Theorem 5 (e))}
\]

\[= \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \sum_{i=1}^{l} \binom{p}{i} \binom{2l}{l - i}
\]

\[= \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \sum_{i=1}^{l} \binom{p + 2l}{l - i} - \binom{2l}{l} \quad \text{(by Lemma 5)}
\]

\[= \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \mod p^2.
\]

Subtracting \(\binom{N}{K} \binom{2l}{l}\) from both sides of this congruence, we obtain the exact claim of Lemma 9. \(\square\)
Lemma 10. Let \( p \) be an odd prime. Let \( N \in \mathbb{Z} \) and \( K \in \mathbb{N} \). Then,

\[
\sum_{l=0}^{p-1} \binom{Np + 2l}{Kp + l} \equiv \binom{N}{K} \eta_p \mod p^2.
\]

Proof of Lemma 10. For any \( l \in \{0, 1, \ldots, p - 1\} \), we have (by Lemma 9)

\[
\binom{Np + 2l}{Kp + l} \equiv \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \mod p^2.
\]

Summing these congruences over all \( l \in \{0, 1, \ldots, p - 1\} \), we prove Lemma 10:

\[
\sum_{l=0}^{p-1} \binom{Np + 2l}{Kp + l} \equiv \sum_{l=0}^{p-1} \left( \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \right) \equiv \binom{N}{K} \sum_{l=0}^{p-1} \binom{2l}{l} \equiv \binom{N}{K} \eta_p \mod p^2.
\]

(by Theorem 7)

Proof of Theorem 3. The map \( \{(l, K) \in \{0, 1, \ldots, p - 1\} \times \{0, 1, \ldots, r - 1\} \rightarrow \{0, 1, \ldots, rp - 1\} \}

\( l \mapsto KP + l \)

is a bijection (since each element of \( \{0, 1, \ldots, rp - 1\} \) can be uniquely divided by \( p \) with remainder, and said remainder will belong to \( \{0, 1, \ldots, r - 1\} \)). Thus, we can substitute \( KP + l \) for \( n \) in the sum \( \sum_{n=0}^{rp-1} \binom{2n}{n} \). This sum thus can be rewritten as

\[
\sum_{n=0}^{rp-1} \binom{2n}{n} = \sum_{(l, K) \in \{0, 1, \ldots, p - 1\} \times \{0, 1, \ldots, r - 1\}} \binom{2(KP + l)}{KP + l} = \sum_{K=0}^{r-1} \sum_{l=0}^{p-1} \binom{2KP + 2l}{KP + l} \equiv \binom{2K}{K} \eta_p \mod p^2
\]

(by Lemma 10, applied to \( N=2K \))

\[
\equiv \sum_{K=0}^{r-1} \binom{2K}{K} \eta_p = \alpha_r \eta_p = \eta_p \alpha_r \mod p^2.
\]
This proves Theorem 3. \qed

2.8. Proving Theorem 4

Lemma 11. Let \( p \) be an odd prime. Let \( N \in \mathbb{Z} \) and \( K \in \mathbb{N} \). Then,

\[
\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left( \left\lfloor \frac{Np + l}{Kp + m} \right\rfloor - \left( \begin{array}{c} N \\ K \end{array} \right) \left( \begin{array}{c} l \\ m \end{array} \right) \right) \equiv 0 \mod p^2.
\]

Proof of Lemma 11. We have

\[
\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left( \left\lfloor \frac{Np + l}{Kp + m} \right\rfloor - \left( \begin{array}{c} N \\ K \end{array} \right) \left( \begin{array}{c} l \\ m \end{array} \right) \right)
= \sum_{l=0}^{p-1} \sum_{m=0}^{l} \left( \left\lfloor \frac{Np + l}{Kp + m} \right\rfloor \left( \begin{array}{c} l \\ m \end{array} \right) \right) - \left( \begin{array}{c} N \\ K \end{array} \right) \sum_{l=0}^{p-1} \left( \begin{array}{c} l \\ m \end{array} \right)
= \sum_{l=0}^{p-1} \left( \left\lfloor \frac{Np + 2l}{Kp + l} \right\rfloor \left( \begin{array}{c} p + 2l \\ l \end{array} \right) - \left( \begin{array}{c} N \\ K \end{array} \right) \left( \begin{array}{c} 2l \\ l \end{array} \right) \right)
\equiv \left( \begin{array}{c} N \\ K \end{array} \right) \left( \left\lfloor \frac{Np + 2l}{Kp + l} \right\rfloor - \left( \begin{array}{c} 2l \\ l \end{array} \right) \right) \mod p^2
\]

\[
\equiv N \left( \begin{array}{c} N \\ K \end{array} \right) \sum_{l=0}^{p-1} \left( \left\lfloor \frac{2l}{l} \right\rfloor - \left( \begin{array}{c} 2l \\ l \end{array} \right) \right) \equiv 0 \mod p^2.
\]

This proves Lemma 11. \qed

Lemma 12. Let \( p \) be an odd prime. Let \( N \in \mathbb{Z} \) and \( K \in \mathbb{N} \). Then,

\[
\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left( \frac{Np + l}{Kp + m} \right)^2 \equiv \left( \begin{array}{c} N \\ K \end{array} \right)^2 \eta_p \mod p^2.
\]

Proof of Lemma 12. Fix \( l \in \{0, 1, \ldots, p-1\} \) and \( m \in \{0, 1, \ldots, p-1\} \). Then, Theorem 1 (applied to \( a = N \), \( b = K \), \( c = l \) and \( d = m \)) yields that

\[
\left( \frac{Np + l}{Kp + m} \right)^2 \equiv \left( \begin{array}{c} N \\ K \end{array} \right) \left( \begin{array}{c} l \\ m \end{array} \right) \mod p.
\]

In other words, \( \left( \frac{Np + l}{Kp + m} \right)^2 \) is divisible by \( p \). Hence,
Lemma 6 (applied to $a = \binom{Np+l}{Kp+m}$ and $b = \binom{N}{K}\binom{l}{m}$) shows that

$$\left(\frac{Np+l}{Kp+m}\right)^2 - \left(\frac{N}{K}\binom{l}{m}\right)^2 = 2\left(\binom{Np+l}{Kp+m} - \frac{N}{K}\binom{l}{m}\right) \mod p^2.$$  

(5)

Now, forget that we fixed $l$ and $m$. We thus have (5) for all $l \in \{0,1,\ldots, p-1\}$ and $m \in \{0,1,\ldots,p-1\}$. Now,

$$\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\frac{Np+l}{Kp+m}\right)^2 - \sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\frac{N}{K}\binom{l}{m}\right)^2$$

$$= \sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\frac{Np+l}{Kp+m}\right)^2 - \sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\frac{N}{K}\binom{l}{m}\right)^2$$

$$= 2\left(\frac{Np+l}{Kp+m} - \frac{N}{K}\binom{l}{m}\right) \mod p^2$$

(by (5))

$$= 2\left(\frac{N}{K}\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\binom{l}{m}\right)^2 - \binom{l}{m}\right) \mod p^2$$

(by Lemma 11)

Thus,

$$\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\frac{Np+l}{Kp+m}\right)^2 = \sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\frac{N}{K}\binom{l}{m}\right)^2$$

$$= \sum_{l=0}^{p-1} \sum_{m=0}^{l} \binom{l}{m}^2$$

(by Corollary 1, applied to $u=l$ and $w=0$)

$$= \sum_{l=0}^{p-1} \binom{2l}{l}$$

(by Theorem 7)

$$\equiv \binom{2n}{n} \mod p^2$$

$$\equiv \binom{N}{K} \eta \mod p^2.$$  

This proves Lemma 12.
**Lemma 13.** Let $p$ be a prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{Z}$. Let $u$ and $v$ be two elements of $\{0, 1, \ldots, p-1\}$ satisfying $u + v \geq p$. Then, $p \mid \left(\frac{Np + u + v}{Kp + u}\right)$.

**Proof of Lemma 13.** We have $u + v \geq p$. Thus, $u + v = p + c$ for some $c \in \mathbb{N}$. Consider this $c$. From $v \in \{0, 1, \ldots, p-1\}$, we obtain $v < p$. Thus, $c + p = p + c = u + \frac{v}{<p} < u + p$, so that $c < u \leq p - 1$ (since $u \in \{0, 1, \ldots, p-1\}$). Thus, $c \in \{0, 1, \ldots, p-1\}$ (since $c \in \mathbb{N}$). Also, $c < u$. Hence, Proposition 2 (applied to $m = c$ and $n = u$) yields \(\binom{c}{u} = 0\).

Theorem 1 (applied to $a = N + 1$, $b = K$ and $d = u$) yields
\[
\left(\frac{(N + 1)p + c}{Kp + u}\right) = \left(\frac{N + 1}{K}\right)\binom{c}{u} = 0 \pmod{p}.
\]
In other words, $p \mid \left(\frac{(N + 1)p + c}{Kp + u}\right)$. In view of $(N + 1)p + c = Np + p + c = Np + u + v$, this can be rewritten as $p \mid \left(\frac{Np + u + v}{Kp + u}\right)$. This proves Lemma 13. \(\square\)

**Lemma 14.** Let $p$ be an odd prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{N}$. Then,
\[
\sum_{u=0}^{N-1} \sum_{v=0}^{p-1} \left(\frac{Np + u + v}{Kp + u}\right)^2 \equiv \left(\frac{N}{K}\right)^2 \eta_p \pmod{p^2}.
\]

**Proof of Lemma 14.** If $u$ and $v$ are two elements of $\{0, 1, \ldots, p-1\}$ satisfying $v \geq p - u$, then
\[
\left(\frac{Np + u + v}{Kp + u}\right)^2 \equiv 0 \pmod{p^2} \tag{6}
\]
5.

Hence, any $u \in \{0, 1, \ldots, p-1\}$ satisfies
\[
\sum_{v=0}^{p-1} \left(\frac{Np + u + v}{Kp + u}\right)^2 = \sum_{v=0}^{p-1} \left(\frac{Np + u + v}{Kp + u}\right)^2 + \sum_{v=p-u}^{p-1} \left(\frac{Np + u + v}{Kp + u}\right)^2 \equiv 0 \pmod{p^2} \tag{by (6)}
\]

5Proof of (6): Let $u$ and $v$ be two elements of $\{0, 1, \ldots, p-1\}$ satisfying $v \geq p - u$. From $v \geq p - u$, we obtain $u + v \geq p$. Thus, Lemma 13 yields $p \mid \left(\frac{Np + u + v}{Kp + u}\right)$. Hence, $p^2 \mid \left(\frac{Np + u + v}{Kp + u}\right)^2$. This proves (6).
\[ (Np + u + v)^2 \mod p^2 \]

(here, we have substituted \( l \) for \( u + v \) in the sum). Summing up these congruences for all \( u \in \{0, 1, \ldots, p-1\} \), we obtain

\[
\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} (Np + u + v)^2 = \sum_{l=0}^{p-1} (Np + l)^2 \mod p^2
\]

(here, we have renamed the index \( u \) as \( m \) in the second sum)

\[
\sum_{u=0}^{p-1} \sum_{l=0}^{p-1} (Np + l)^2 = \sum_{l=0}^{p-1} \sum_{u=0}^{l} (Np + l)^2
\]

(by Lemma 12). This proves Lemma 14.

\[ \square \]

**Proof of Theorem 4.** First, let us observe that

\[
\epsilon_{r,s} = \sum_{m=0}^{r-1} \sum_{n=0}^{s-1} \binom{n+m}{m}^2 = \sum_{n=0}^{s-1} \sum_{m=0}^{r-1} \binom{n+m}{m}^2 = \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \binom{K+L}{K}^2
\]

(since Proposition 3 yields \( \binom{K+L}{K} = \binom{K+L}{L} \) for all \( K \in \mathbb{N} \) and \( L \in \mathbb{N} \)).

Each \( n \in \mathbb{N} \) satisfies

\[
\sum_{m=0}^{sp-1} \binom{n+m}{m}^2 = \sum_{u=0}^{p-1} \sum_{K=0}^{s-1} \binom{n+Kp+u}{Kp+u}^2
\]

(here, we have substituted \( Kp + u \) for \( m \) in the sum, since the map

\[
\{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, s-1\} \to \{0, 1, \ldots, sp-1\},
\]

\[
(u, K) \mapsto Kp + u
\]

is a bijection). Summing up this equality over all \( n \in \{0, 1, \ldots, rp-1\} \), we obtain

\[
\sum_{n=0}^{rp-1} \sum_{m=0}^{sp-1} \binom{n+m}{m}^2 = \sum_{n=0}^{rp-1} \sum_{u=0}^{p-1} \sum_{K=0}^{s-1} \binom{n+Kp+u}{Kp+u}^2
\]
\[
\sum_{v=0}^{p-1} \sum_{L=0}^{r-1} \sum_{u=0}^{p-1} \sum_{K=0}^{s-1} \left( \frac{Lp + v + Kp + u}{Kp + u} \right)^2
\]

(here, we have substituted \(Lp + v \) for \(n \) in the sum, since the map

\[
\{0, 1, \ldots, p - 1\} \times \{0, 1, \ldots, r - 1\} \to \{0, 1, \ldots, rp - 1\},
\]

\((v, L) \mapsto Lp + v\)

is a bijection).

Thus,

\[
\sum_{n=0}^{r-1} \sum_{m=0}^{p-1} \binom{n + m}{m}^2 = \sum_{v=0}^{p-1} \sum_{L=0}^{r-1} \sum_{u=0}^{p-1} \sum_{K=0}^{s-1} \left( \frac{Lp + v + Kp + u}{Kp + u} \right)^2
\]

\[
= \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \sum_{u=0}^{p-1} \left( \frac{(K + L)p + u}{Kp + u} \right)^2
\]

\[
= \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \left( \frac{K + L}{K} \right)^2 \eta_p \text{ mod } p^2
\]

(by Lemma 14, applied to \(N = K + L\))

\[
= \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \left( \frac{K + L}{K} \right)^2 \eta_p = \epsilon_{r, s} \eta_p = \eta_p \epsilon_{r, s} \text{ mod } p^2.
\]

This proves Theorem 4. \(\square\)

**Acknowledgments.** Thanks to Doron Zeilberger and Roberto Tauraso for alerting me to [1] and [17].

**References**


