On binomial coefficients modulo squares of primes

Darij Grinberg

January 10, 2019

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

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

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

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

Contents

1. Introduction ................................................. 2
   1.1. Binomial coefficients .................................. 2
   1.2. Classical congruences .................................. 3
   1.3. The three modulo-\( p^2 \) congruences .................. 4

2. The proofs .................................................. 5
   2.1. Identities and congruences from the literature .......... 5
   2.2. Variants and consequences of Vandermonde convolution .... 7
   2.3. A congruence of Bailey’s ................................ 11
   2.4. Two congruences for polynomials ....................... 13
1. Introduction

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

\[
\sum_{n=0}^{p-1} \binom{2n}{n} \equiv \eta_p \mod p^2 \quad \text{(Theorem 1.8)};
\]

\[
r^p \sum_{n=0}^{r-1} \binom{2n}{n} \equiv \eta_p \sum_{n=0}^{r-1} \binom{2n}{n} \mod p^2 \quad \text{(Theorem 1.9)};
\]

\[
sp \sum_{n=0}^{s-1} \sum_{m=0}^{r-1} \binom{n+m}{m}^2 \equiv \eta_p \sum_{m=0}^{s-1} \sum_{n=0}^{r-1} \binom{n+m}{m}^2 \mod p^2 \quad \text{(Theorem 1.10)},
\]

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 three congruences are (slightly extended versions of) three of the “Super-Conjectures” (namely, 1, 1” and 4”) stated by Apagodu and Zeilberger in \cite{ApaZei16}. Our proofs are more elementary than previous proofs by Stanton \cite{Stanto16} and Amdeberhan and Tauraso \cite{AmdTau16}.

1.1. Binomial coefficients

Let us first recall the definition of binomial coefficients\footnote{In the arXiv preprint version of \cite{ApaZei16} [arXiv:1606.03351v2], these congruences appear as “Super-Conjectures” 1, 1” and 5”, respectively.}

**Definition 1.1.** Let $n \in \mathbb{N}$ and $m \in \mathbb{Z}$. Then, the binomial coefficient \( \binom{m}{n} \) is a rational number defined by

\[
\binom{m}{n} = \frac{m (m-1) \cdots (m-n+1)}{n!}.
\]
Definition 1.2. Let \( n \) be a negative integer. Let \( m \in \mathbb{Z} \). Then, the binomial coefficient \( \binom{m}{n} \) is a rational number defined by \( \binom{m}{n} = 0 \).

(This is the definition used in [GrKnPa94] and [Grinbe17b]. Some authors follow other conventions instead.)

The following proposition is well-known (see, e.g., [Grinbe17b, Proposition 1.9]):

Proposition 1.3. We have \( \binom{m}{n} \in \mathbb{Z} \) for any \( m \in \mathbb{Z} \) and \( n \in \mathbb{Z} \).

Proposition 1.3 shows that \( \binom{m}{n} \) is an integer whenever \( m \in \mathbb{Z} \) and \( n \in \mathbb{Z} \). We shall tacitly use this below, when we study congruences involving binomial coefficients.

One advantage of Definition 1.2 is that it makes the following hold:

Proposition 1.4. For any \( n \in \mathbb{Z} \) and \( m \in \mathbb{Z} \), the binomial coefficient \( \binom{n}{m} \) is the coefficient of \( X^m \) in the formal power series \( (1 + X)^n \in \mathbb{Z}[[X]] \). (Here, the coefficient of \( X^m \) in any formal power series is defined to be 0 when \( m \) is negative.)

1.2. Classical congruences

The behavior of binomial coefficients modulo primes and prime powers is a classical subject of research; see [Mestro14, §2.1] for a survey of much of it. Let us state two of the most basic results in this subject:

Theorem 1.5. 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,

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

Theorem 1.5 is known under the name of Lucas’s theorem, and is proven in many places (e.g., [Mestro14, §2.1] or [Hausne83, Proof of §4] or [AnBeRo05, proof of Lucas’s theorem] or [GrKnPa94, Exercise 5.61]) at least in the case when \( a \) and \( b \) are nonnegative integers. The standard proof of Theorem 1.5 in this case uses generating functions (specifically, Proposition 1.4); this proof applies (mutatis mutandis) in the general case as well. See [Grinbe17b, Theorem 1.11] for an elementary proof of Theorem 1.5.

Another fundamental result is the following:
Theorem 1.6. Let \( p \) be a prime. Let \( a \) and \( b \) be two integers. Then,

\[
\binom{ap}{bp} \equiv \binom{a}{b} \mod p^2.
\]

Theorem 1.6 is a known result, perhaps due to Charles Babbage. It appears with proof in [Grinbe17b, Theorem 1.12]; again, many sources prove it for nonnegative \( a \) and \( b \) (for example [Stanle11, Exercise 1.14 c] or [GrKnPa94, 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 [Mestro14, (22) and (23)] for the details. See also [SunTau11, Lemma 2.1] for another strengthening of Theorem 1.6.

1.3. The three modulo-\( p^2 \) congruences

Definition 1.7. 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 three conjectures by Apagodu and Zeilberger, which we shall prove in the sequel. The first one is [ApaZei16, Super-Conjecture 1].

Theorem 1.8. Let \( p \) be an odd prime. Then,

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

The next one ([ApaZei16, Super-Conjecture 1’]) is a generalization:

Theorem 1.9. Let \( p \) be an odd prime. Let \( r \in \mathbb{N} \). Set

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

\( \text{To be precise (and boastful), our Theorem 1.8 is somewhat stronger than [ApaZei16, Super-Conjecture 1]}, since we only require } p \text{ to be odd (rather than } p \geq 5). \text{ Of course, in the case of Theorem 1.8 this extra generality is insignificant, since it just adds the possibility of } p = 3, \text{ in which case Theorem 1.8 can be checked by hand. However, for Theorems 1.9 and 1.10 further below, we gain somewhat more from this generality.} \)
Then,
\[ \sum_{n=0}^{p-1} \binom{2n}{n} \equiv \eta_p r \mod p^2. \]

Theorem 1.8 and Theorem 1.9 both have been proven by Dennis Stanton [Stanto16] using Laurent series (in the case when \( p \geq 5 \)), and by Liu [Liu16 (1.3)] using harmonic numbers. We shall reprove them elementarily.

The third conjecture that we shall prove is [ApaZei16 Super-Conjecture 5']:

**Theorem 1.10.** Let \( p \) be an odd prime. Let \( r \in \mathbb{N} \) and \( s \in \mathbb{N} \). Set
\[ \epsilon_{r,s} = \sum_{m=0}^{r-1} \sum_{n=0}^{s-1} \binom{n + m}{m}^2. \]
Then,
\[ \sum_{n=0}^{p-1} \sum_{m=0}^{s-1} \binom{n + m}{m}^2 \equiv \eta_p \epsilon_{r,s} \mod p^2. \]

A proof of Theorem 1.10 has been found by Amdeberhan and Tauraso, and was outlined in [AmdTau16 §6]; we give a different, elementary proof.

2. The proofs

2.1. Identities and congruences from the literature

Before we come to the proofs of Theorems 1.8, 1.9, and 1.10 let us collect various well-known results that will prove useful.

The following properties of binomial coefficients are well-known (see, e.g., [Grinbe17 §3.1] and [Grinbe17b §1]):

**Proposition 2.1.** We have \( \binom{m}{0} = 1 \) for every \( m \in \mathbb{Z} \).

**Proposition 2.2.** We have \( \binom{m}{n} = 0 \) for every \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfying \( m < n \).

**Proposition 2.3.** We have \( \binom{m}{n} = \binom{m}{m-n} \) for any \( m \in \mathbb{N} \) and \( n \in \mathbb{N} \) satisfying \( m \geq n \).
Proposition 2.4. We have \( \binom{m}{m} = 1 \) for every \( m \in \mathbb{N} \).

Proposition 2.5. We have
\[
\binom{m}{n} = (-1)^n \binom{n - m - 1}{n}
\]
for any \( m \in \mathbb{Z} \) and \( n \in \mathbb{N} \).

Proposition 2.6. We have
\[
\binom{m}{n} = \binom{m - 1}{n - 1} + \binom{m - 1}{n}
\]
for any \( m \in \mathbb{Z} \) and \( n \in \mathbb{Z} \).

Proposition 2.7. 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 2.7 is the so-called Vandermonde convolution identity, and is a particular case of [Grinbe17, Theorem 3.29].

Corollary 2.8. For each \( n \in \mathbb{N} \), we have
\[
\sum_{i=0}^{n-1} (-1)^i \binom{n - 1 - i}{i} = (-1)^n \begin{cases} 
0, & \text{if } n \equiv 0 \pmod{3}; \\
-1, & \text{if } n \equiv 1 \pmod{3}; \\
1, & \text{if } n \equiv 2 \pmod{3}
\end{cases}
\]
Corollary 2.8 is [Grinbe17, Corollary 7.69]. Apart from that, Corollary 2.8 can be easily derived from [GrKnPa94, §5.2, Problem 3], [BenQui03, Identity 172] or [BenQui08].

Another simple identity (sometimes known as the “absorption identity”) is the following:

Proposition 2.9. Let \( n \in \mathbb{Z} \) and \( k \in \mathbb{Z} \). Then,
\[
k \binom{n}{k} = n \binom{n - 1}{k - 1}.
\]
Proposition 2.9 appears in [GrKnPa94, (5.6)], and is easily proven just from the definition of binomial coefficients.

Finally, we need the following result from elementary number theory:
Theorem 2.10. Let $p$ be a prime. Let $k \in \mathbb{N}$. Assume that $k$ is not a positive multiple of $p - 1$. Then,

$$\sum_{l=0}^{p-1} l^k \equiv 0 \text{ mod } p.$$

Theorem 2.10 is proven, e.g., in [Grinbe17b, Theorem 3.1] and (in a slightly rewritten form) in [MacSon10, 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 2.7). We begin with the following one:

Corollary 2.11. 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 2.11: Proposition 2.7 (applied to $x = u$, $y = l$ and $n = w + l$)
On binomial coefficients modulo squares of primes

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 2.2)

(since \(l < w + l - k\) (because \(k < w\)))

\[
\left( \begin{array}{c} x + y \\ n \end{array} \right) = \sum_{i=0}^{y} \left( \begin{array}{c} x \\ n - i \end{array} \right) \left( \begin{array}{c} y \\ i \end{array} \right).
\]

This proves Corollary 2.11. \(\square\)

Let us also state another corollary of Proposition 2.7:

**Corollary 2.12.** Let \(x \in \mathbb{Z}\) and \(y \in \mathbb{N}\) and \(n \in \mathbb{Z}\). Then,

\[
\left( \begin{array}{c} x + y \\ n \end{array} \right) = \sum_{i=0}^{y} \left( \begin{array}{c} x \\ n - i \end{array} \right) \left( \begin{array}{c} y \\ i \end{array} \right).
\]

See [Grinbe17b, Corollary 2.2] for a proof of Corollary 2.12.

**Lemma 2.13.** 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 2.13. Corollary 2.12 (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)

$$
= \sum_{i \in \{-l, -l + 1, \ldots, l\}; \ i \neq 0} \binom{u}{w + i} \binom{2l}{l - i} + \binom{u}{w} \binom{2l}{l}
$$

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

$$
\binom{u + 2l}{w + l} - \binom{u}{w} \binom{2l}{l} = \sum_{i \neq 0} \binom{u}{w + i} \binom{2l}{l - i}
$$

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

(here, we have split the sum into two: one for “positive $i$” and one for “negative $i$”)

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

(by Proposition 2.3)

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

In other words,

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

This proves Lemma 2.13.

Lemma 2.14. 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 2.14. Corollary 2.12 (applied to $x = cp + l$, $y = l$ and $n = l$) yields
\[
\binom{cp + l + l}{l} = \sum_{i=0}^l \binom{cp + l}{l-i} \binom{l}{i} = \sum_{k=0}^l \binom{cp + l}{k} \binom{l}{l-k}
\]
\[
= \binom{l}{l} \quad \text{(by Proposition 2.3)}
\]
\[
= \sum_{k=0}^l \binom{cp + l}{k} \binom{l}{k}.
\]
(here, we have substituted $k$ for $l - i$ in the sum)

Comparing this with
\[
\sum_{k=0}^{p-1} \binom{cp + l}{k} \binom{l}{k} = \sum_{k=0}^l \binom{cp + l}{k} \binom{l}{k} + \sum_{k=l+1}^{p-1} \binom{cp + l}{k} \binom{l}{k}
\]
\[
= \sum_{k=0}^l \binom{cp + l}{k} \binom{l}{k} + \sum_{k=l+1}^{p-1} \binom{cp + l}{k} 0 = \sum_{k=0}^l \binom{cp + l}{k} \binom{l}{k},
\]
\[
\text{(here, we have split the sum at } k = l, \text{ since } 0 \leq l \leq p - 1\]
\[
= \sum_{k=0}^l \binom{cp + l}{k} \binom{l}{k} = \binom{cp + l + l}{l} = \binom{cp + 2l}{l}.
\]
This proves Lemma 2.14. \qed

Lemma 2.15. 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 2.15. Proposition 2.7 (applied to $x = p$, $y = 2l$ and $n = l$) yields
\[
\binom{p + 2l}{l} = \sum_{k=0}^l \binom{p}{k} \binom{2l}{l-k} = \sum_{i=0}^l \binom{p}{i} \binom{2l}{l-i}
\]
\[
\quad \text{(here, we have renamed the summation index } k \text{ as } i)\]
\[
= \binom{p}{0} \binom{2l}{l-0} + \sum_{i=1}^l \binom{p}{i} \binom{2l}{l-i} = \binom{2l}{l} + \sum_{i=1}^l \binom{p}{i} \binom{2l}{l-i}.
\]
Thus,

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

This proves Lemma 2.15 □

### 2.3. A congruence of Bailey’s

Next, we shall prove a modulo-\(p^2\) congruence for certain binomial coefficients that can be regarded as a counterpart to Theorem 1.6:

**Theorem 2.16.** Let \(p\) be a prime. Let \(N \in \mathbb{Z}\) and \(K \in \mathbb{Z}\) and \(i \in \{1, 2, \ldots, p-1\}\). Then:

(a) We have

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

(b) We have

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

(c) We have

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

**Proof of Theorem 2.16.** From \(i \in \{1, 2, \ldots, p-1\}\), we conclude that both \(i-1\) and \(p-1\) 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 2.9 (applied to \(n = Np\) and \(k = Kp+i\)) yields

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

(by Theorem 1.3, applied to \(a = N-1, b = K, c = p-1\) and \(d = i-1\))

\[
\equiv Np \binom{N-1}{K} \binom{p-1}{i-1} \mod p^2 \tag{1}
\]
(notice that the presence of the $p$ factor has turned a congruence modulo $p$ into a congruence modulo $p^2$). Thus,

$$(Kp + i) \left( \binom{Np}{Kp + i} \right) \equiv Np \left( \binom{N - 1}{K} \right) \left( \binom{p - 1}{i - 1} \right) \equiv 0 \mod p,$$

so that $0 \equiv (Kp + i) \left( \binom{Np}{Kp + i} \right) \equiv i \left( \binom{Np}{Kp + i} \right) \mod p$. We can cancel $i$ from this congruence (since $i$ is coprime to $p$), and thus obtain $0 \equiv \left( \binom{Np}{Kp + i} \right) \mod p$.

Hence, $(Kp + i) \left( \binom{Np}{Kp + i} \right) \equiv N \left( \binom{N - 1}{K} \right) \left( \binom{p - 1}{i - 1} \right) \mod p^2$. (by (1))

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

$$(Kp + i) \left( \binom{Np}{Kp + i} \right) \equiv N \left( \binom{N - 1}{K} \right) \left( \binom{p}{i} \right) \mod p^2.$$

This proves Theorem 2.16 (a).

(b) We have $i \in \{1, 2, \ldots, p - 1\}$ and thus $p - i \in \{1, 2, \ldots, p - 1\}$. Hence, Theorem 2.16 (a) (applied to $K - 1$ and $p - i$ instead of $K$ and $i$) yields

$$\left( \binom{Np}{(K - 1) p + (p - i)} \right) \equiv N \left( \binom{N - 1}{K - 1} \right) \left( \binom{p}{p - i} \right) = N \left( \binom{N - 1}{K - 1} \right) \left( \binom{p}{i} \right) \mod p^2.$$ (by Proposition 2.3)
In view of 

\((K - 1)p + (p - i) = Kp - i\), this rewrites as

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

This proves Theorem 2.16 (b).

(c) We have

\[
\binom{Np}{K + i} + \binom{Np}{K - i} \\
\equiv N \binom{N - 1}{K} \binom{p}{i} \mod p^2 \quad \text{(by Theorem 2.16 (a))}
\]

\[
\equiv N \binom{N - 1}{K - 1} \binom{p}{i} \mod p^2 \quad \text{(by Theorem 2.16 (b))}
\]

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

\[
\equiv \binom{N}{K} \binom{p}{i} \mod p^2. \quad \text{(by Proposition 2.6)}
\]

This proves Theorem 2.16 (c).

\[ \blacksquare \]

2.4. Two congruences for polynomials

Now, we recall that \(\mathbb{Z}[X]\) is the ring of all polynomials in one indeterminate \(X\) with integer coefficients.

**Lemma 2.17.** Let \(p\) be a prime. Let \(c \in \mathbb{Z}\). Let \(P \in \mathbb{Z}[X]\) be a polynomial of degree < \(2p - 1\). Then, \(\sum_{l=0}^{p-1} (P(cp + l) - P(l)) \equiv 0 \mod p^2.\)

**Proof of Lemma 2.17.** 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 2.17 is easily checked (because in this case, \(P\) is constant). Thus, WLOG assume that \(k \neq 0\). Hence, \(k\) is a positive integer (since \(k \in \mathbb{N}\)). Thus, \(k - 1 \in \mathbb{N}\).
Each \( l \in \{0, 1, \ldots, p-1\} \) satisfies

\[
P (cp + l) = (cp + l)^k \quad \text{(since } P = X^k)\]

\[
= \sum_{i=0}^{k} \binom{k}{i} (cp)^i l^{k-i} \quad \text{(by the binomial formula)}
\]

\[
= (cp)^0 l^k + \binom{k}{1} cp l^{k-1} + \sum_{i=2}^{k} \binom{k}{i} (cp)^i l^{k-i} \equiv 0 \mod p^2
\]

\[
\equiv l^k + kcp l^{k-1} + \sum_{i=2}^{k} \binom{k}{i} 0l^{k-i} = l^k + kcp l^{k-1} \mod p^2
\]

and \( P (l) = l^k \) (since \( P = X^k \)). Thus,

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

The claim of Lemma 2.17 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 2.10 (applied to \( k - 1 \) instead of \( k \)) yields

\[
\sum_{l=0}^{p-1} l^{k-1} \equiv 0 \mod p. \text{ Thus, } p \sum_{l=0}^{p-1} l^{k-1} \equiv 0 \mod p^2, \text{ so that}
\]

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

This proves Lemma 2.17.

| Lemma 2.18. | Let \( p, a \) and \( b \) be three 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 2.18. 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 2.18 is proven. |
Lemma 2.19. 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,

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

Proof of Lemma 2.19. 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 2.18 (applied to $a = P(cp + l)$ and $b = P(l)$) shows that

$$
(P(cp + l))^2 - (P(l))^2 \equiv 2 (P(cp + l) - P(l)) P(l) \mod p^2.
$$

(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 2.17 (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,

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

(by (3))

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 2.19. \hfill \square

2.5. Proving Theorem 1.8

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

---

4This is a well-known fact. It can be proven as follows: WLOG assume that $P = X^k$ for some $k \in \mathbb{N}$ (this is a valid assumption, since the claim is $\mathbb{Z}$-linear in $P$); then, $P(u) - P(v) = u^k - v^k = (u - v) \sum_{i=0}^{k-1} u^{k-i} v^{k-i}$ is clearly divisible by $u - v$. 

Lemma 2.20. Let $p$ be an odd prime. Let $c \in \mathbb{Z}$. Let $k \in \{0, 1, \ldots, p-1\}$. Then,

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

Proof of Lemma 2.20. 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 2.19 yields

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

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

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

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

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

This proves Lemma 2.20. \hfill \Box

Lemma 2.21. 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 2.21. For each $l \in \{0, 1, \ldots, p-1\}$, we have

$$
\binom{cp+2l}{l} - \binom{2l}{l} = \sum_{k=0}^{p-1} \binom{cp+l}{k} \binom{l}{k} (by \ Lemma 2.14) \quad \text{(by Lemma 2.14, applied to 0 instead of c)}
$$

and

$$
\sum_{k=0}^{p-1} \binom{l}{k} \binom{l}{k} - \sum_{k=0}^{p-1} \binom{l}{k} \binom{l}{k} = \sum_{k=0}^{p-1} \left( \binom{cp+l}{k} - \binom{l}{k} \right) \binom{l}{k}.
$$
Summing these equalities over all $l \in \{0, 1, \ldots, p - 1\}$, we find
\[
\sum_{l=0}^{p-1} \left( \binom{cp + 2l}{l} - \binom{2l}{l} \right) = \sum_{l=0}^{p-1} \sum_{k=0}^{p-1} \left( \binom{cp + l}{k} - \binom{l}{k} \right) \binom{l}{k} 
\]
\[= \sum_{k=0}^{p-1} \sum_{l=0}^{p-1} \left( \binom{cp + l}{k} - \binom{l}{k} \right) \binom{l}{k} \equiv \sum_{k=0}^{p-1} 0 = 0 \mod p^2.
\]
(by Lemma 2.20)

This proves Lemma 2.21 \hfill \Box

**Proof of Theorem 1.8** Lemma 2.21 (applied to $c = -1$) yields
\[
\sum_{l=0}^{p-1} \left( \binom{-p + 2l}{l} - \binom{2l}{l} \right) \equiv 0 \mod p^2.
\]

Thus,
\[
0 \equiv \sum_{l=0}^{p-1} \left( \binom{-p + 2l}{l} - \binom{2l}{l} \right) = \sum_{l=0}^{p-1} \left( \binom{-p + 2l}{l} \right) - \sum_{l=0}^{p-1} \left( \binom{2l}{l} \right) \mod p^2,
\]
so that
\[
\sum_{l=0}^{p-1} \binom{2l}{l} \equiv \sum_{l=0}^{p-1} \left( \binom{-p + 2l}{l} \right) \mod p^2. \tag{4}
\]
Now,
\[ \sum_{n=0}^{p-1} \binom{2n}{n} = \sum_{l=0}^{p-1} \binom{2l}{l} \equiv \sum_{l=0}^{p-1} \binom{-p+2l}{l} \quad \text{(by (4))} \]
\[ = (-1)^l \left( \frac{l - (-p + 2l) - 1}{l} \right) \quad \text{(by Proposition 2.3)} \]
\[ = \sum_{l=0}^{p-1} (-1)^l \left( \frac{l - (-p + 2l) - 1}{l} \right) = \sum_{l=0}^{p-1} (-1)^l \left( \frac{p - 1 - l}{l} \right) \]
\[ = \sum_{l=0}^{p-1} (-1)^l \left( \frac{p - 1 - l}{l} \right) = (-1)^p \cdot \begin{cases} 0, & \text{if } p \equiv 0 \mod 3; \\ -1, & \text{if } p \equiv 1 \mod 3; \\ 1, & \text{if } p \equiv 2 \mod 3 \end{cases} \]
(by Corollary 2.8, applied to \( n = p \))
\[ = \begin{cases} 0, & \text{if } p \equiv 0 \mod 3; \\ -1, & \text{if } p \equiv 1 \mod 3; \\ 1, & \text{if } p \equiv 2 \mod 3 \end{cases} \]
\[ \equiv \eta_p \mod p^2. \]
This proves Theorem 1.8. \( \Box \)

### 2.6. Proving Theorem 1.9

**Lemma 2.22.** Let \( N \in \mathbb{Z} \) and \( K \in \mathbb{N} \). Let \( p \) be a prime. Let \( l \in \{0, 1, \ldots, p - 1\} \).
Then,
\[ \binom{Np + 2l}{Kp + l} - \binom{N}{K} \binom{2l}{l} \equiv N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \mod p^2. \]

**Proof of Lemma 2.22** Theorem 1.6 yields \( \binom{Np}{Kp} \equiv \binom{N}{K} \mod p^2. \)
Lemma 2.13 (applied to \( u = Np \) and \( w = Kp \)) yields

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

\[
\equiv \binom{N}{K} \mod p^2
\]

\[
\equiv N \binom{N}{K} \binom{p}{i} \mod p^2 \tag{by Theorem 2.16 (c)}
\]

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

Subtracting \( \binom{N}{K} \binom{2l}{l} \) from both sides of this congruence, we obtain

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

This proves Lemma 2.22. \( \square \)

**Lemma 2.23.** 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 2.23.** For any \( l \in \{0, 1, \ldots, p - 1\} \), we have

\[
\binom{Np + 2l}{Kp + l} \equiv \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \mod p^2
\]
(by Lemma 2.22). Summing these congruences over all $l \in \{0, 1, \ldots, p-1\}$, we find
\[
\sum_{l=0}^{p-1} \left( \binom{Np + 2l}{Kp + l} \right) \equiv \sum_{l=0}^{p-1} \left( \binom{N}{K} \binom{2l}{l} + N \binom{N}{K} \left( \binom{p + 2l}{l} - \binom{2l}{l} \right) \right) \equiv 0 \mod p^2
\]
(by Lemma 2.21, applied to $c=1$)
\[
\equiv \left( \binom{N}{K} \sum_{l=0}^{p-1} \binom{2l}{l} \right) \equiv \left( \binom{N}{K} \eta_p \mod p^2 \right).
\]
This proves Lemma 2.23.

Proof of Theorem 1.9

The map
\[
\{0, 1, \ldots, p-1\} \times \{0, 1, \ldots, r-1\} \to \{0, 1, \ldots, rp-1\},
\]
\[
(l, K) \mapsto Kp + l
\]
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 rewrites as follows:
\[
\sum_{n=0}^{rp-1} \binom{2n}{n} = \sum_{(l,K) \in \{0,1,\ldots,p-1\} \times \{0,1,\ldots,r-1\}} \binom{2(Kp + l)}{Kp + l} = \sum_{K=0}^{r-1} \sum_{l=0}^{p-1} \binom{2Kp + 2l}{Kp + l} = \left( \binom{2K}{K} \right) \eta_p \mod p^2
\]
(by Lemma 2.23, 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 1.9.

2.7. Proving Theorem 1.10
**Lemma 2.24.** Let $p$ be an odd prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{N}$. Then,

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

**Proof of Lemma 2.24.** We have

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

(by Corollary 2.11 applied to $u = Np+l$ and $w = Kp$)

$$
= \sum_{l=0}^{p-1} \binom{Np+2l}{Kp+l} - \binom{N}{K} \sum_{l=0}^{p-1} \binom{2l}{l}
$$

(by Corollary 2.11 applied to $u = 1$ and $w = 0$)

$$
= \sum_{l=0}^{p-1} \binom{Np+2l}{Kp+l} - \binom{N}{K} \sum_{l=0}^{p-1} \binom{2l}{l}
$$

(by Lemma 2.22)

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

(by Lemma 2.21 applied to $c = 1$)

This proves Lemma 2.24.

**Lemma 2.25.** Let $p$ be an odd prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{N}$. Then,

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

**Proof of Lemma 2.25.** Fix $l \in \{0, 1, \ldots, p-1\}$ and $m \in \{0, 1, \ldots, p-1\}$. Then, Theorem 1.5 (applied to $a = N$, $b = K$, $c = l$ and $d = m$) yields that $\binom{Np+l}{Kp+m} \equiv \binom{N}{K} \binom{l}{m} \mod p$. In other words, $\binom{Np+l}{Kp+m} - \binom{N}{K} \binom{l}{m}$ is divisible by $p$. Hence,
Lemma 2.18 (applied to $a = \binom{Np + l}{Kp + m}$ and $b = \binom{N}{K} \binom{l}{m}$) shows that
\[
\binom{Np + l}{Kp + m}^2 - \binom{N}{K} \binom{l}{m}^2 \\
\equiv 2 \left( \binom{Np + l}{Kp + m} - \binom{N}{K} \binom{l}{m} \right) \binom{N}{K} \binom{l}{m} \mod p^2. \tag{5}
\]

Now, forget that we fixed $l$ and $m$. We thus have proven (5) for all $l \in \{0, 1, \ldots, p - 1\}$ and $m \in \{0, 1, \ldots, p - 1\}$. Now,
\[
\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left( \binom{Np + l}{Kp + m}^2 - \binom{N}{K} \binom{l}{m}^2 \right) \\
\equiv 2 \sum_{l=0}^{p-1} \sum_{m=0}^{l} \left( \binom{Np + l}{Kp + m} - \binom{N}{K} \binom{l}{m} \right) \binom{N}{K} \binom{l}{m} \mod p^2 \\
\equiv 0 \mod p^2 \tag{by Lemma 2.24}
\]

Thus,
\[
\sum_{l=0}^{p-1} \sum_{m=0}^{l} \binom{Np + l}{Kp + m}^2 \\
= \sum_{l=0}^{p-1} \sum_{m=0}^{l} \binom{N}{K} \binom{l}{m}^2 = \binom{N}{K} \sum_{l=0}^{p-1} \sum_{m=0}^{l} \binom{l}{m}^2 \\
= \sum_{m=0}^{l} \binom{l}{m}^2 = 2l \\
\tag{by Corollary 2.11, applied to $u = l$ and $w = 0$}
\]
\[
= \binom{N}{K}^2 \sum_{l=0}^{p-1} \binom{2l}{l} = \binom{N}{K}^2 \eta_p \mod p^2. \\
\tag{by Theorem 1.8}
\]
This proves Lemma 2.25. \qed
Lemma 2.26. 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, $p \mid \binom{Np + u + v}{Kp + u}$.

Proof of Lemma 2.26. 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, $c + p = p + c = u + \underbrace{v}_{<p} < u + p$, 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 2.2 (applied to $m = c$ and $n = u$) yields \(\binom{c}{u} = 0\).

Now, $u + v = p + c$, so that $Np + u + v = Np + p + c = (N + 1)p + c$. Hence,
\[
\binom{Np + u + v}{Kp + u} = \binom{(N + 1)p + c}{Kp + u} = \binom{N + 1}{K} \binom{c}{u} = 0
\]
(by Theorem 1.5, applied to $a = N + 1$, $b = K$ and $d = u$)
\[= 0 \mod p.\]

In other words, $p \mid \binom{Np + u + v}{Kp + u}$. This proves Lemma 2.26. \hfill \Box

Lemma 2.27. Let $p$ be an odd prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{N}$. Then,
\[
\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \left(\frac{Np + u + v}{Kp + u}\right)^2 \equiv \left(\frac{N}{K}\right)^2 \eta_p \mod p^2.
\]

Proof of Lemma 2.27. If $u$ and $v$ are two elements of \{0, 1, \ldots, p - 1\} satisfying $v \geq p - u$, then
\[
\left(\frac{Np + u + v}{Kp + u}\right)^2 \equiv 0 \mod p^2 \quad (6)
\]

\[\text{Proof of (6): Let } u \text{ and } v \text{ be two elements of } \{0, 1, \ldots, p - 1\} \text{ satisfying } v \geq p - u. \text{ From } v \geq p - u, \text{ we obtain } u + v \geq p. \text{ Thus, Lemma 2.26 yields } p \mid \binom{Np + u + v}{Kp + u}. \text{ Hence, } p^2 \mid \left(\frac{Np + u + v}{Kp + u}\right)^2. \text{ This proves (6).}\]
Hence, any \( u \in \{0, 1, \ldots, p - 1\} \) satisfies
\[
\sum_{v=0}^{p-1} \left( \binom{Np + u + v}{Kp + u} \right)^2 = \sum_{v=0}^{p-1} \left( \binom{Np + u + v}{Kp + u} \right)^2 + \sum_{v=p-u}^{p-1} \left( \binom{Np + u + v}{Kp + u} \right)^2 = 0 \mod p^2
\]
(by (6))

(here, we have split the sum at \( v = p - u \))
\[
\equiv \sum_{v=0}^{p-1} \left( \binom{Np + u + v}{Kp + u} \right)^2 = \sum_{l=0}^{p-1} \left( \binom{Np + l}{Kp + u} \right)^2 \mod p^2
\]
(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
\[
\sum_{u=0}^{p-1} \sum_{v=0}^{p-u-1} \left( \binom{Np + u + v}{Kp + u} \right)^2 = \sum_{u=0}^{p-1} \sum_{l=0}^{p-1} \left( \binom{Np + l}{Kp + u} \right)^2 \equiv \left( \frac{N}{K} \right)^2 \eta_p \mod p^2
\]
(by Lemma 2.25). This proves Lemma 2.27.

**Proof of Theorem 1.10.** First, let us observe that
\[
\epsilon_{r,s} = \sum_{m=0}^{r-1} \sum_{n=0}^{s-1} \left( \binom{n+m}{m} \right)^2 = \sum_{n=0}^{s-1} \sum_{m=0}^{r-1} \left( \binom{n+m}{m} \right)^2 = \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \left( \binom{K+L}{K} \right)^2
\]
(since Proposition 2.3 yields \( \left( \begin{array}{c} K+L \\ L \end{array} \right) = \left( \begin{array}{c} K+L \\ K \end{array} \right) \) for all \( K \in \mathbb{N} \) and \( L \in \mathbb{N} \).

Each \( n \in \mathbb{N} \) satisfies
\[
\sum_{m=0}^{sp-1} \left( \binom{n+m}{m} \right)^2 = \sum_{u=0}^{p-1} \sum_{K=0}^{s-1} \left( \binom{n+Kp+u}{Kp+u} \right)^2
\]
(here, we have substituted \( Kp + u \) for \( m \) in the sum, since the map
\[
\{0, 1, \ldots, p - 1\} \times \{0, 1, \ldots, s - 1\} \to \{0, 1, \ldots, sp - 1\}, \quad (u, K) \mapsto Kp + u
\]
is a bijection). Summing up this equality over all \( n \in \{0, 1, \ldots, rp - 1\} \), we obtain

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

\[
= \sum_{v=0}^{p-1} \sum_{L=0}^{r-1} \sum_{u=0}^{s-1} \sum_{K=0}^{p-1} \binom{Lp+v+Kp+u}{Kp+u}^2
\]

(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,

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

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

\[
\equiv \left( \frac{K+L}{K} \right)^2 \eta_p \mod p^2
\]

(by Lemma 2.27 applied to \( N=K+L \))

\[
\equiv \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \binom{K+L}{K}^2 \eta_p = \epsilon_{r,s} \eta_p = \eta_p \epsilon_{r,s} \mod p^2.
\]

This proves Theorem 1.10. \( \square \)

### 2.8. Acknowledgments

Thanks to Doron Zeilberger and Roberto Tauraso for alerting me to [AmdTau16] and [SunTau11].

### References


[Stanto16] Dennis Stanton, *Addendum to “Using the “Freshman’s Dream” to Prove Combinatorial Congruences*”,
http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/freshmanDennisStanton.pdf