#A14 INTEGERS 19 (2019)

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

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

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

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

1. Introduction

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

$$\sum_{n=0}^{rp-1} \binom{2n}{n} \equiv \eta_p \sum_{n=0}^{r-1} \binom{2n}{n} \bmod p^2 \qquad \text{(Theorem 3)};$$
$$\sum_{n=0}^{rp-1} \sum_{m=0}^{sp-1} \binom{n+m}{m}^2 \equiv \eta_p \sum_{m=0}^{r-1} \sum_{n=0}^{s-1} \binom{n+m}{m}^2 \bmod p^2 \qquad \text{(Theorem 4)},$$

where

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

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* $\dbinom{m}{n}$ is a rational number defined by

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

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* $\dbinom{m}{n} \in \mathbb{Z}$ *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,*

$$\binom{ap+c}{bp+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p.$$

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.

---

[1] In the arXiv preprint version of [3] (`https://arxiv.org/abs/1606.03351v2`arXiv:1606.03351v2), these congruences appear as "Super-Conjectures" 1" and $5'$, respectively.

[2] We 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,*

$$\binom{ap}{bp} \equiv \binom{a}{b} \bmod p^2.$$

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

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

Notice that η_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″]:[3]

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,

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

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 $\sum\limits_{n=0}^{p-1} \binom{2n}{n} \equiv \eta_p \bmod p^2$ for each odd prime p; this is [3, Super-Conjecture 1].

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

[3]To 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*

$$\epsilon_{r,s} = \sum_{m=0}^{r-1} \sum_{n=0}^{s-1} \binom{n+m}{m}^2 .$$

Then,

$$\sum_{n=0}^{rp-1} \sum_{m=0}^{sp-1} \binom{n+m}{m}^2 \equiv \eta_p \epsilon_{r,s} \bmod p^2.$$

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)

$$\binom{Np}{Kp+i} \equiv N \binom{N-1}{K} \binom{p}{i} \bmod p^2;$$

(b)

$$\binom{Np}{Kp-i} \equiv N \binom{N-1}{K-1} \binom{p}{i} \bmod p^2;$$

(c)

$$\binom{Np}{Kp+i} + \binom{Np}{Kp-i} \equiv N \binom{N}{K} \binom{p}{i} \bmod p^2.$$

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 $P \in$

$\mathbb{Z}[X]$ satisfy $P(cp+l) \equiv P(l) \bmod p$. Thus, polynomials in $\mathbb{Z}[X]$ can be applied to modulo-p congruences, yielding new modulo-p congruences. More interesting is the fact that sometimes polynomials can be used to turn modulo-p congruences into modulo-p^2 congruences. Two vehicles for such "lifting" of congruences are the following two lemmas (proven further below).

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

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,*

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

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*

$$\sum_{i=0}^{n-1} (-1)^i \binom{n-1-i}{i} = (-1)^n \cdot \begin{cases} 0, & \text{if } n \equiv 0 \bmod 3; \\ -1, & \text{if } n \equiv 1 \bmod 3; \\ 1, & \text{if } n \equiv 2 \bmod 3. \end{cases}$$

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,*

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

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

$$\binom{u+l}{w+l} = \sum_{k=0}^{w+l} \binom{u}{k}\binom{l}{w+l-k} = \sum_{k=0}^{w-1} \binom{u}{k} \underbrace{\binom{l}{w+l-k}}_{\substack{=0 \\ \text{(by Proposition 2} \\ \text{(since } l<w+l-k \\ \text{(because } k<w\text{)))}}} + \sum_{k=w}^{w+l} \binom{u}{k}\binom{l}{w+l-k}$$

$$= \sum_{k=w}^{w+l} \binom{u}{k}\binom{l}{w+l-k} = \sum_{m=0}^{l} \binom{u}{w+m} \underbrace{\binom{l}{w+l-(w+m)}}_{\substack{=\binom{l}{l-m}=\binom{l}{m} \\ \text{(by Proposition 3)}}}$$

$$\text{(here, we have substituted } w+m \text{ for } k \text{ in the sum)}$$
$$= \sum_{m=0}^{l} \binom{u}{w+m} \binom{l}{m}.$$

This proves Corollary 1. $\square$

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

$$\binom{u+2l}{w+l} = \sum_{i=0}^{2l} \binom{u}{w+l-i} \binom{2l}{i} = \sum_{i=-l}^{l} \binom{u}{w+i} \binom{2l}{l-i}$$
$$\text{(here, we have substituted } l-i \text{ for } i \text{ in the sum)}$$
$$= \sum_{\substack{i \in \{-l, -l+1, \ldots, l\}; \\ i \neq 0}} \binom{u}{w+i} \binom{2l}{l-i} + \binom{u}{w}\binom{2l}{l}$$

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

$$\binom{u+2l}{w+l} - \binom{u}{w}\binom{2l}{l} = \sum_{\substack{i \in \{-l, -l+1, \ldots, l\}; \\ i \neq 0}} \binom{u}{w+i} \binom{2l}{l-i}$$
$$= \sum_{i=1}^{l} \binom{u}{w+i} \binom{2l}{l-i} + \sum_{i=-l}^{-1} \binom{u}{w+i} \binom{2l}{l-i}$$
$$= \sum_{i=1}^{l} \binom{u}{w+i} \binom{2l}{l-i} + \sum_{i=1}^{l} \binom{u}{w-i} \underbrace{\binom{2l}{l+i}}_{\substack{= \binom{2l}{l-i} \\ \text{(by Proposition 3)}}}$$

$$\left(\begin{array}{c}\text{here, we have substituted } -i \text{ for } i\\ \text{in the second sum}\end{array}\right)$$

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

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

$$\binom{cp+2l}{l} = \sum_{i=0}^{l} \binom{cp+l}{l-i} \binom{l}{i} = \sum_{k=0}^{l} \binom{cp+l}{k} \underbrace{\binom{l}{l-k}}_{\substack{=\binom{l}{k} \\ \text{(by Proposition 3)}}}$$

(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

$$\sum_{k=0}^{p-1} \binom{cp+l}{k} \binom{l}{k} = \sum_{k=0}^{l} \binom{cp+l}{k} \binom{l}{k} + \sum_{k=l+1}^{p-1} \binom{cp+l}{k} \underbrace{\binom{l}{k}}_{\substack{=0 \\ \text{(by Proposition 2} \\ \text{(applied to } m=l \text{ and } n=k) \\ \text{(since } l<k))}}$$

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

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)

$$= \underbrace{\binom{p}{0}}_{=1}\underbrace{\binom{2l}{l-0}}_{=\binom{2l}{l}} + \sum_{i=1}^{l}\binom{p}{i}\binom{2l}{l-i} = \binom{2l}{l} + \sum_{i=1}^{l}\binom{p}{i}\binom{2l}{l-i}.$$

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

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

$$\begin{aligned}(Kp+i)\binom{Np}{Kp+i} &= Np\binom{Np-1}{Kp+i-1} = Np\underbrace{\binom{(N-1)\,p+(p-1)}{Kp+(i-1)}}_{\substack{\equiv\binom{N-1}{K}\binom{p-1}{i-1} \bmod p \\ \text{(by Theorem 1, applied to} \\ a=N-1,\ b=K,\ c=p-1 \text{ and } d=i-1)}} \\ &\equiv Np\binom{N-1}{K}\binom{p-1}{i-1} \bmod p^2 \qquad (1)\end{aligned}$$

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

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

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

$\binom{Np}{Kp+i}$ is divisible by p. Thus, $p\binom{Np}{Kp+i}$ is divisible by p^2. In other words,

$$p\binom{Np}{Kp+i} \equiv 0 \bmod p^2. \tag{2}$$

Now,

$$(Kp+i)\binom{Np}{Kp+i} = K\underbrace{p\binom{Np}{Kp+i}}_{\substack{\equiv 0 \bmod p^2 \\ \text{(by (2))}}} + i\binom{Np}{Kp+i} \equiv i\binom{Np}{Kp+i} \bmod p^2.$$

Hence,

$$\begin{aligned} i\binom{Np}{Kp+i} &\equiv (Kp+i)\binom{Np}{Kp+i} \equiv Np\binom{N-1}{K}\binom{p-1}{i-1} \qquad \text{(by (1))} \\ &= N\binom{N-1}{K}\underbrace{p\binom{p-1}{i-1}}_{\substack{=i\binom{p}{i} \\ \text{(by Proposition 8)}}} = N\binom{N-1}{K}i\binom{p}{i} \bmod p^2. \end{aligned}$$

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

$$\binom{Np}{Kp+i} \equiv N\binom{N-1}{K}\binom{p}{i} \bmod p^2.$$

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

$$\binom{Np}{(K-1)p+(p-i)} \equiv N\binom{N-1}{K-1}\underbrace{\binom{p}{p-i}}_{\substack{=\binom{p}{i} \\ \text{(by Proposition 3)}}} = N\binom{N-1}{K-1}\binom{p}{i} \bmod p^2.$$

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

$$\binom{Np}{Kp-i} \equiv N\binom{N-1}{K-1}\binom{p}{i} \bmod p^2.$$

This proves Theorem 5 **(b)**.

(c) We have

$$\begin{aligned}
&\underbrace{\binom{Np}{Kp+i}}_{\substack{\equiv N\binom{N-1}{K}\binom{p}{i} \bmod p^2 \\ \text{(by Theorem 5 \textbf{(a)})}}} \quad + \quad \underbrace{\binom{Np}{Kp-i}}_{\substack{\equiv N\binom{N-1}{K-1}\binom{p}{i} \bmod p^2 \\ \text{(by Theorem 5 \textbf{(b)})}}} \\
&\equiv N\binom{N-1}{K}\binom{p}{i} + N\binom{N-1}{K-1}\binom{p}{i} \\
&= N\underbrace{\left(\binom{N-1}{K-1}+\binom{N-1}{K}\right)}_{\substack{=\binom{N}{K} \\ \text{(by Proposition 5)}}}\binom{p}{i} = N\binom{N}{K}\binom{p}{i} \bmod p^2.
\end{aligned}$$

This proves Theorem 5 **(c)**. $\square$

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

$$\begin{aligned}
P(cp+l) = (cp+l)^k &= \sum_{i=0}^{k}\binom{k}{i}(cp)^i l^{k-i} \qquad \text{(by the binomial formula)} \\
&= \underbrace{(cp)^0 l^{k-0}}_{=l^k} + k\underbrace{(cp)^1}_{=cp} l^{k-1} + \sum_{i=2}^{k}\binom{k}{i}\underbrace{(cp)^i}_{\substack{\equiv 0 \bmod p^2 \\ \text{(since } i\geq 2)}} l^{k-i} \\
&\equiv l^k + kcpl^{k-1} \bmod p^2
\end{aligned}$$

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

$$\sum_{l=0}^{p-1}\left(\underbrace{P(cp+l)}_{\equiv l^k + kcpl^{k-1} \bmod p^2} - \underbrace{P(l)}_{=l^k}\right) \equiv \sum_{l=0}^{p-1}\underbrace{\left(l^k + kcpl^{k-1} - l^k\right)}_{=kcpl^{k-1}} = kcp\sum_{l=0}^{p-1} l^{k-1} \bmod p^2.$$

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

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

This proves Lemma 1. $\square$

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

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

Proof of Lemma 2. Fix $l \in \mathbb{Z}$. We have $P \in \mathbb{Z}\left[X\right]$. Thus, $P\left(u\right) - P\left(v\right)$ is divisible by $u - v$ whenever u and v are two integers[4]. Applying this to $u = cp + l$ and $v = l$, we conclude that $P\left(cp+l\right) - P\left(l\right)$ is divisible by $\left(cp+l\right) - l = cp$, and thus also divisible by p. Hence, Lemma 6 (applied to $a = P\left(cp+l\right)$ and $b = P\left(l\right)$) yields

$$\left(P\left(cp+l\right)\right)^2 - \left(P\left(l\right)\right)^2 \equiv 2\left(P\left(cp+l\right) - P\left(l\right)\right) P\left(l\right) \mod p^2. \tag{3}$$

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 $\leq 2\left(p-1\right) < 2p-1$. Thus, Lemma 1 (applied to P^2 instead of P) shows that

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

Thus,

$$0 \equiv \sum_{l=0}^{p-1} \underbrace{\left(P^2\left(cp+l\right) - P^2\left(l\right)\right)}_{\substack{=\left(P\left(cp+l\right)\right)^2 - \left(P\left(l\right)\right)^2 \\ \equiv 2\left(P\left(cp+l\right) - P\left(l\right)\right) P\left(l\right) \mod p^2 \\ \text{(by (3))}}} \equiv 2 \sum_{l=0}^{p-1} \left(P\left(cp+l\right) - P\left(l\right)\right) P\left(l\right) \mod p^2.$$

We can cancel 2 from this congruence (since p is odd), and conclude that

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

This proves Lemma 2. $\square$

[4]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,*

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

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

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

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

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

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

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

This proves Lemma 7. $\square$

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

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

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

$$\underbrace{\binom{cp+2l}{l}}_{\substack{=\sum_{k=0}^{p-1}\binom{cp+l}{k}\binom{l}{k} \\ \text{(by Lemma 4)}}} - \underbrace{\binom{2l}{l}}_{\substack{=\sum_{k=0}^{p-1}\binom{l}{k}\binom{l}{k} \\ \text{(by Lemma 4,} \\ \text{applied to 0 instead of } c\text{)}}} = \sum_{k=0}^{p-1} \left(\binom{cp+l}{k} - \binom{l}{k} \right) \binom{l}{k}.$$

Summing these equalities over all $l \in \{0, 1, \ldots, p-1\}$, we find

$$\sum_{l=0}^{p-1} \left(\binom{cp+2l}{l} - \binom{2l}{l} \right) = \sum_{l=0}^{p-1} \sum_{k=0}^{p-1} \left(\binom{cp+l}{k} - \binom{l}{k} \right) \binom{l}{k}$$
$$= \sum_{k=0}^{p-1} \underbrace{\sum_{l=0}^{p-1} \left(\binom{cp+l}{k} - \binom{l}{k} \right) \binom{l}{k}}_{\substack{\equiv 0 \bmod p^2 \\ \text{(by Lemma 7)}}} \equiv \sum_{k=0}^{p-1} 0 = 0 \bmod p^2.$$

This proves Lemma 8. ☐

2.6. η_p Appears

Let us now prove the particular case of Theorem 3 for $r = 1$:

Theorem 7. *Let p be an odd prime. Then,*

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

Proof of Theorem 7. Lemma 8 (applied to $c = -1$) yields

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

Moving all the $\binom{2l}{l}$ addends to the right-hand side of this congruence, we obtain

$$\sum_{l=0}^{p-1} \binom{-p+2l}{l} \equiv \sum_{l=0}^{p-1} \binom{2l}{l} \bmod p^2. \tag{4}$$

Now,

$$\sum_{n=0}^{p-1} \binom{2n}{n} = \sum_{l=0}^{p-1} \binom{2l}{l} \equiv \sum_{l=0}^{p-1} \underbrace{\binom{-p+2l}{l}}_{\substack{=(-1)^l \binom{l-(-p+2l)-1}{l} \\ \text{(by Proposition 4)}}} \qquad \text{(by (4))}$$
$$= \sum_{l=0}^{p-1} (-1)^l \underbrace{\binom{l-(-p+2l)-1}{l}}_{=\binom{p-1-l}{l}} = \sum_{l=0}^{p-1} (-1)^l \binom{p-1-l}{l}$$

$$= \sum_{i=0}^{p-1} (-1)^i \binom{p-1-i}{i} = \underbrace{(-1)^p}_{\substack{=-1 \\ \text{(since } p \text{ is odd)}}} \cdot \begin{cases} 0, & \text{if } p \equiv 0 \bmod 3; \\ -1, & \text{if } p \equiv 1 \bmod 3; \\ 1, & \text{if } p \equiv 2 \bmod 3 \end{cases}$$

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

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

□

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,*

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

Proof of Lemma 9. Theorem 2 yields $\binom{Np}{Kp} \equiv \binom{N}{K} \bmod p^2$.

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

$$\binom{Np+2l}{Kp+l} = \underbrace{\binom{Np}{Kp}}_{\equiv \binom{N}{K} \bmod p^2} \binom{2l}{l} + \sum_{i=1}^{l} \underbrace{\left(\binom{Np}{Kp+i} + \binom{Np}{Kp-i}\right)}_{\substack{\equiv N\binom{N}{K}\binom{p}{i} \bmod p^2 \\ \text{(by Theorem 5 (c))}}} \binom{2l}{l-i}$$

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

$$= \binom{N}{K}\binom{2l}{l} + N\binom{N}{K} \underbrace{\sum_{i=1}^{l} \binom{p}{i}\binom{2l}{l-i}}_{\substack{=\binom{p+2l}{l} - \binom{2l}{l} \\ \text{(by Lemma 5)}}}$$

$$= \binom{N}{K}\binom{2l}{l} + N\binom{N}{K}\left(\binom{p+2l}{l} - \binom{2l}{l}\right) \bmod p^2.$$

Subtracting $\binom{N}{K}\binom{2l}{l}$ from both sides of this congruence, we obtain the exact claim of Lemma 9. □

Lemma 10. *Let p be an odd prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{N}$. Then,*

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

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

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

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

$$\begin{aligned}
\sum_{l=0}^{p-1} \binom{Np+2l}{Kp+l} &\equiv \sum_{l=0}^{p-1} \left(\binom{N}{K}\binom{2l}{l} + N\binom{N}{K}\left(\binom{p+2l}{l} - \binom{2l}{l}\right)\right) \\
&= \binom{N}{K} \sum_{l=0}^{p-1} \binom{2l}{l} + N\binom{N}{K} \underbrace{\sum_{l=0}^{p-1} \left(\binom{p+2l}{l} - \binom{2l}{l}\right)}_{\substack{\equiv 0 \bmod p^2 \\ \text{(by Lemma 8, applied to } c=1)}} \\
&\equiv \binom{N}{K} \underbrace{\sum_{l=0}^{p-1} \binom{2l}{l}}_{\substack{= \sum_{n=0}^{p-1} \binom{2n}{n} \equiv \eta_p \bmod p^2 \\ \text{(by Theorem 7)}}} \equiv \binom{N}{K} \eta_p \bmod p^2.
\end{aligned}$$

□

Proof of Theorem 3. 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 can be rewritten as

$$\begin{aligned}
\sum_{n=0}^{rp-1} \binom{2n}{n} &= \underbrace{\sum_{(l,K) \in \{0,1,\ldots,p-1\} \times \{0,1,\ldots,r-1\}}}_{= \sum_{K=0}^{r-1} \sum_{l=0}^{p-1}} \underbrace{\binom{2(Kp+l)}{Kp+l}}_{= \binom{2Kp+2l}{Kp+l}} = \sum_{K=0}^{r-1} \underbrace{\sum_{l=0}^{p-1} \binom{2Kp+2l}{Kp+l}}_{\substack{\equiv \binom{2K}{K} \eta_p \bmod p^2 \\ \text{(by Lemma 10,} \\ \text{applied to } N=2K)}} \\
&\equiv \underbrace{\sum_{K=0}^{r-1} \binom{2K}{K}}_{= \sum_{n=0}^{r-1} \binom{2n}{n} = \alpha_r} \eta_p = \alpha_r \eta_p = \eta_p \alpha_r \bmod p^2.
\end{aligned}$$

This proves Theorem 3. $\square$

2.8. Proving Theorem 4

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

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

Proof of Lemma 11. We have

$$\begin{aligned}
&\sum_{l=0}^{p-1} \sum_{m=0}^{l} \left(\binom{Np+l}{Kp+m} - \binom{N}{K}\binom{l}{m} \right) \binom{l}{m} \\
&= \sum_{l=0}^{p-1} \underbrace{\sum_{m=0}^{l} \binom{Np+l}{Kp+m}\binom{l}{m}}_{\substack{=\binom{Np+2l}{Kp+l} \\ \text{(by Corollary 1,} \\ \text{applied to } u=Np+l \text{ and } w=Kp)}} - \binom{N}{K} \sum_{l=0}^{p-1} \underbrace{\sum_{m=0}^{l} \binom{l}{m}\binom{l}{m}}_{\substack{=\binom{2l}{l} \\ \text{(by Corollary 1,} \\ \text{applied to } u=l \text{ and } w=0)}} \\
&= \sum_{l=0}^{p-1} \binom{Np+2l}{Kp+l} - \binom{N}{K} \sum_{l=0}^{p-1} \binom{2l}{l} = \sum_{l=0}^{p-1} \underbrace{\left(\binom{Np+2l}{Kp+l} - \binom{N}{K}\binom{2l}{l} \right)}_{\substack{\equiv N\binom{N}{K}\left(\binom{p+2l}{l} - \binom{2l}{l}\right) \bmod p^2 \\ \text{(by Lemma 9)}}} \\
&\equiv N \binom{N}{K} \underbrace{\sum_{l=0}^{p-1} \left(\binom{p+2l}{l} - \binom{2l}{l} \right)}_{\substack{\equiv 0 \bmod p^2 \\ \text{(by Lemma 8, applied to } c=1)}} \equiv 0 \bmod p^2.
\end{aligned}$$

This proves Lemma 11. $\square$

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

$$\sum_{l=0}^{p-1} \sum_{m=0}^{l} \binom{Np+l}{Kp+m}^2 \equiv \binom{N}{K}^2 \eta_p \bmod p^2.$$

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 $\binom{Np+l}{Kp+m} \equiv \binom{N}{K}\binom{l}{m} \bmod p$. In other words, $\binom{Np+l}{Kp+m} - \binom{N}{K}\binom{l}{m}$ 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

$$\binom{Np+l}{Kp+m}^2 - \left(\binom{N}{K}\binom{l}{m}\right)^2 \equiv 2\left(\binom{Np+l}{Kp+m} - \binom{N}{K}\binom{l}{m}\right)\binom{N}{K}\binom{l}{m} \bmod p^2. \tag{5}$$

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,

$$\begin{aligned}
&\sum_{l=0}^{p-1}\sum_{m=0}^{l}\binom{Np+l}{Kp+m}^2 - \sum_{l=0}^{p-1}\sum_{m=0}^{l}\left(\binom{N}{K}\binom{l}{m}\right)^2 \\
&= \sum_{l=0}^{p-1}\sum_{m=0}^{l} \underbrace{\left(\binom{Np+l}{Kp+m}^2 - \left(\binom{N}{K}\binom{l}{m}\right)^2\right)}_{\substack{\equiv 2\left(\binom{Np+l}{Kp+m} - \binom{N}{K}\binom{l}{m}\right)\binom{N}{K}\binom{l}{m} \bmod p^2 \\ \text{(by (5))}}} \\
&\equiv 2\binom{N}{K} \underbrace{\sum_{l=0}^{p-1}\sum_{m=0}^{l}\left(\binom{Np+l}{Kp+m} - \binom{N}{K}\binom{l}{m}\right)\binom{l}{m}}_{\substack{\equiv 0 \bmod p^2 \\ \text{(by Lemma 11)}}} \equiv 0 \bmod p^2.
\end{aligned}$$

Thus,

$$\begin{aligned}
\sum_{l=0}^{p-1}\sum_{m=0}^{l}\binom{Np+l}{Kp+m}^2 &\equiv \sum_{l=0}^{p-1}\sum_{m=0}^{l}\left(\binom{N}{K}\binom{l}{m}\right)^2 = \binom{N}{K}^2 \sum_{l=0}^{p-1} \underbrace{\sum_{m=0}^{l}\binom{l}{m}^2}_{\substack{= \sum_{m=0}^{l}\binom{l}{m}\binom{l}{m} = \binom{2l}{l} \\ \text{(by Corollary 1,} \\ \text{applied to } u=l \text{ and } w=0\text{)}}} \\
&= \binom{N}{K}^2 \underbrace{\sum_{l=0}^{p-1}\binom{2l}{l}}_{\substack{= \sum_{n=0}^{p-1}\binom{2n}{n} \equiv \eta_p \bmod p^2 \\ \text{(by Theorem 7)}}} \\
&\equiv \binom{N}{K}^2 \eta_p \bmod p^2.
\end{aligned}$$

This proves Lemma 12. $\square$

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, $p \mid \dbinom{Np+u+v}{Kp+u}$.*

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, $c + p = p + c = u + \underbrace{v}_{<p} < u + p$, 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 (applied to $m = c$ and $n = u$) yields $\dbinom{c}{u} = 0$.

Theorem 1 (applied to $a = N + 1$, $b = K$ and $d = u$) yields

$$\binom{(N+1)\,p+c}{Kp+u} \equiv \binom{N+1}{K} \underbrace{\binom{c}{u}}_{=0} = 0 \bmod p.$$

In other words, $p \mid \dbinom{(N+1)\,p+c}{Kp+u}$. In view of $(N+1)\,p + c = Np + \underbrace{p+c}_{=u+v} = Np + u + v$, this can be rewritten as $p \mid \dbinom{Np+u+v}{Kp+u}$. This proves Lemma 13. ☐

Lemma 14. *Let p be an odd prime. Let $N \in \mathbb{Z}$ and $K \in \mathbb{N}$. Then,*

$$\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \binom{Np+u+v}{Kp+u}^2 \equiv \binom{N}{K}^2 \eta_p \bmod p^2.$$

Proof of Lemma 14. If u and v are two elements of $\{0, 1, \ldots, p-1\}$ satisfying $v \geq p - u$, then

$$\binom{Np+u+v}{Kp+u}^2 \equiv 0 \bmod p^2 \tag{6}$$

[5].

Hence, any $u \in \{0, 1, \ldots, p-1\}$ satisfies

$$\sum_{v=0}^{p-1} \binom{Np+u+v}{Kp+u}^2 = \sum_{v=0}^{p-u-1} \binom{Np+u+v}{Kp+u}^2 + \sum_{v=p-u}^{p-1} \underbrace{\binom{Np+u+v}{Kp+u}^2}_{\substack{\equiv 0 \bmod p^2 \\ \text{(by (6))}}}$$

[5] *Proof 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 $p \mid \binom{Np+u+v}{Kp+u}$. Hence, $p^2 \mid \binom{Np+u+v}{Kp+u}^2$. This proves (6).

$$\equiv \sum_{v=0}^{p-u-1} \binom{Np+u+v}{Kp+u}^2 = \sum_{l=u}^{p-1} \binom{Np+l}{Kp+u}^2 \operatorname{mod} p^2$$

(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

$$\begin{aligned}
&\sum_{u=0}^{p-1}\sum_{v=0}^{p-1} \binom{Np+u+v}{Kp+u}^2 \\
&\equiv \underbrace{\sum_{u=0}^{p-1}\sum_{l=u}^{p-1}}_{=\sum_{l=0}^{p-1}\sum_{u=0}^{l}} \binom{Np+l}{Kp+u}^2 = \sum_{l=0}^{p-1}\sum_{u=0}^{l} \binom{Np+l}{Kp+u}^2 = \sum_{l=0}^{p-1}\sum_{m=0}^{l} \binom{Np+l}{Kp+m}^2 \\
&\qquad \text{(here, we have renamed the index } u \text{ as } m \text{ in the second sum)} \\
&\equiv \binom{N}{K}^2 \eta_p \operatorname{mod} p^2
\end{aligned}$$

(by Lemma 12). This proves Lemma 14. □

Proof of Theorem 4. First, let us observe that

$$\begin{aligned}
\epsilon_{r,s} &= \sum_{m=0}^{r-1}\sum_{n=0}^{s-1} \binom{n+m}{m}^2 = \sum_{n=0}^{s-1}\sum_{m=0}^{r-1} \binom{n+m}{m}^2 = \sum_{K=0}^{s-1}\sum_{L=0}^{r-1} \binom{K+L}{L}^2 \\
&= \sum_{K=0}^{s-1}\sum_{L=0}^{r-1} \binom{K+L}{K}^2 \qquad (7)
\end{aligned}$$

(since Proposition 3 yields $\binom{K+L}{L} = \binom{K+L}{K}$ 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

$$\begin{aligned}
\{0,1,\ldots,p-1\} \times \{0,1,\ldots,s-1\} &\to \{0,1,\ldots,sp-1\}, \\
(u,K) &\mapsto Kp+u
\end{aligned}$$

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

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

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

(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,

$$\sum_{n=0}^{rp-1} \sum_{m=0}^{sp-1} \binom{n+m}{m}^2 = \underbrace{\sum_{v=0}^{p-1} \sum_{L=0}^{r-1} \sum_{u=0}^{p-1} \sum_{K=0}^{s-1}}_{=\sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1}} \underbrace{\binom{Lp+v+Kp+u}{Kp+u}^2}_{=\binom{(K+L)p+u+v}{Kp+u}^2}$$

$$= \sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \underbrace{\sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \binom{(K+L)p+u+v}{Kp+u}^2}_{\substack{\equiv \binom{K+L}{K}^2 \eta_p \bmod p^2 \\ \text{(by Lemma 14, applied to } N=K+L)}}$$

$$\equiv \underbrace{\sum_{K=0}^{s-1} \sum_{L=0}^{r-1} \binom{K+L}{K}^2}_{\substack{=\epsilon_{r,s} \\ \text{(by (7))}}} \eta_p = \epsilon_{r,s}\eta_p = \eta_p \epsilon_{r,s} \bmod p^2.$$

This proves Theorem 4. □

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

References

[1] Tewodros Amdeberhan, Roberto Tauraso, Two triple binomial sum supercongruences, *J. Number Theory* **175** (2017), 140-157. A preprint is available at `https://arxiv.org/abs/1607.02483v1`arXiv:1607.02483v1.

[2] Peter G. Anderson, Arthur T. Benjamin and Jeremy A. Rouse, Combinatorial proofs of Fermat's, Lucas's, and Wilson's theorems, *Amer. Math. Monthly* **112** (2005), 266-268.

[3] Moa Apagodu, Doron Zeilberger, Using the "Freshman's Dream" to prove combinatorial congruences, *Amer. Math. Monthly* **124** (2017), 597-608. (A preprint can be found at `https://arxiv.org/abs/1606.03351v2`, but is less up-to-date and uses a different numbering of the conjectures.)

[4] D. F. Bailey, Some binomial coefficient congruences, *Appl. Math. Lett.* **4** (1991), 1-5. `https://doi.org/10.1016/0893-9659(91)90043-U`

[5] Arthur T. Benjamin and Jennifer J. Quinn, *Proofs that Really Count: The Art of Combinatorial Proof*, The Mathematical Association of America, 2003.

[6] Arthur T. Benjamin and Jennifer J. Quinn, An alternate approach to alternating sums: A method to DIE for, *College Math. J.* **39** (2008) 191-202.

[7] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.

[8] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, available at `https://github.com/darijgr/detnotes/releases/tag/2018-11-07` (accessed 7 November 2018). See also `http://www.cip.ifi.lmu.de/~grinberg/ primes2015/sols.pdf` for a version that is getting updates.

[9] Darij Grinberg, *The Lucas and Babbage congruences*, available at `http://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf` (accessed 3 October 2018).

[10] Darij Grinberg, *On binomial coefficients modulo squares of primes*, `arXiv:1712.02095v2` (more detailed version of this paper).

[11] Melvin Hausner, Applications of a simple counting technique, *Amer. Math. Monthly* **90** (1983), 127-129.

[12] Ji-Cai Liu, *On two conjectural supercongruences of Apagodu and Zeilberger*, `arXiv:1606.08432v3`.

[13] Kieren MacMillan and Jonathan Sondow, Proofs of power sum and binomial coefficient congruences via Pascal's identity, *Amer. Math. Monthly* **118** (2011), 549-551, `arXiv:1011.0076v1`.

[14] Romeo Meštrović, *Lucas' theorem: its generalizations, extensions and applications (1878–2014)*, `arXiv:1409.3820v1`.

[15] Richard Stanley, *Enumerative Combinatorics, volume 1*, 2nd edition, Cambridge University Press 2012. A preprint is available at `http://math.mit.edu/~rstan/ec/` .

[16] Dennis Stanton, *Addendum to "Using the "Freshman's Dream" to prove combinatorial congruences"*, `http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/freshmanDennisStanton.pdf`.

[17] Zhi-Wei Sun, Roberto Tauraso, On some new congruences for binomial coefficients, *Int. J. Number Theory* **7**, (2011), 645–662. A preprint is available at `https://arxiv.org/abs/0709.1665v10`.