SUPER CONGRUENCES AND ELLIPTIC CURVES OVER $\mathbb{F}_p$

ZHI-WEI SUN

Department of Mathematics, Nanjing University
Nanjing 210093, People’s Republic of China
zwsun@nju.edu.cn

Abstract. In this paper we deduce some new super-congruences motivated by elliptic curves over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where $p > 3$ is a prime. Let $d \in \{0, 1, \ldots, (p-1)/2\}$. We show that
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k)(2k+d)}{8^k} \equiv 0 \pmod{p}
\]
whenever $d \equiv \frac{p+1}{2} \pmod{2}$,

and
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k)(2k+d)}{16^k} \equiv \frac{-1}{p} \quad + \quad p^2 \frac{(-1)^d}{4} E_{p-3} \left( \frac{d + 1}{2} \right) \pmod{p^3},
\]
where $E_{p-3}(x)$ denotes the Euler polynomial of degree $p - 3$, and $(-)$ stands for the Legendre symbol. The paper also contains some other results such as
\[
\sum_{k=0}^{p-1} k^{1+\left(\frac{-1}{p}\right)/2} \frac{(6k)(3k)}{864^k} \equiv 0 \pmod{p^2}.
\]

1. Introduction

Let $p > 3$ be a prime and let $\lambda$ be a rational $p$-adic integer (whose denominator is not divisible by $p$). Consider the cubic curve in the Legendre form
\[
\mathbb{E}_p(\lambda) : y^2 = x(x - 1)(x - \bar{\lambda})
\]

2010 Mathematics Subject Classification. Primary 11B65; Secondary 05A10, 11A07, 11E25.

Keywords. Central binomial coefficients, super congruences, Catalan numbers, binary quadratic forms.

Supported by the National Natural Science Foundation (grant 11171140) of China.
over the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, where $\bar{\lambda}$ is the residue class of $\lambda \mod p$. This is an elliptic curve if $\lambda \not\equiv 0, 1 \pmod{p}$. Clearly the number of points on $\mathbb{E}_p(\lambda)$ (including the point at infinity) is

$$\#\mathbb{E}_p(\lambda) = 1 + \#\{(x, y) : 0 \leq x, y < p \text{ and } y^2 \equiv x(x-1)(x-\lambda) \pmod{p}\} = 1 + \sum_{x=0}^{p-1} \left(1 + \left(\frac{x(x-1)(x-\lambda)}{p}\right)\right) = p + 1 + a_p(\lambda),$$

where $(\cdot|_p)$ denotes the Legendre symbol and

$$a_p(\lambda) := \sum_{x=0}^{p-1} \left(\frac{x(x-1)(x-\lambda)}{p}\right).$$

In this paper we propose the study of the weighted number $N_p^{(d)}(\lambda)$ of points $(x, y)$ in $\mathbb{E}_p(\lambda)$ with weight $x^d$ where $d \in \mathbb{N} = \{0, 1, 2, \ldots\}$ and $d \leq (p-1)/2$. For $d = 1, \ldots, (p-1)/2$, Clearly

$$N_p^{(d)}(\lambda) = 1 + \sum_{x=0}^{p-1} x^d \left(1 + \left(\frac{x(x-1)(x-\lambda)}{p}\right)\right) \equiv 1 + a_p^{(d)}(\lambda) \pmod{p}$$

where

$$a_p^{(d)}(\lambda) := \sum_{x=0}^{p-1} x^d \left(\frac{x(x-1)(x-\lambda)}{p}\right). \tag{1.1}$$

Concerning $a_p^{(d)}(\lambda) \pmod{p}$ we have the following result.

**Theorem 1.1.** Let $p$ be an odd prime and let $d \in \{0, \ldots, (p-1)/2\}$. Then, for any rational $p$-adic integer $\lambda$ we have

$$a_p^{(d)}(\lambda) \equiv (-1)^{(p+1)/2} \lambda^d \sum_{k=0}^{(p-1)/2} \left(\frac{2^k \binom{2k}{k} \binom{2k+d}{k+d}}{16^k}\right) \lambda^k - \delta_{d,(p-1)/2} \pmod{p}. \tag{1.2}$$

Let $p$ be an odd prime and let $d \in \{0, \ldots, (p-1)/2\}$. Clearly

$$a_p^{(d)}(1) = \sum_{x=0}^{p-1} x^d \left(\frac{x}{p}\right) - 1 \equiv \sum_{x=1}^{p-1} x^d + (p-1)/2 - 1 \equiv -\delta_{d,(p-1)/2} - 1 \pmod{p}.$$ 

Thus (1.2) with $\lambda = 1$ gives the congruence

$$\sum_{k=0}^{(p-1)/2} \left(\frac{2^k \binom{2k}{k} \binom{2k+d}{k+d}}{16^k}\right) \equiv 4^d \left(\frac{-1}{p}\right) \pmod{p}. \tag{1.2}$$

However, we find that this congruence even holds modulo $p^2$. 
Theorem 1.2. Let $p > 3$ be a prime and let $d \in \{0, \ldots, (p-1)/2\}$. Then
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(k/8)^2} \equiv 4^d \left(\frac{-1}{p}\right) \pmod{p^2},
\]
(1.3)
and moreover
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(k/8)^2} \equiv \left(\frac{-1}{p}\right) + p^2 \left(\frac{-1}{4}\right) E_{p-3} \left(d + \frac{1}{2}\right) \pmod{p^3},
\]
(1.4)
where $E_{p-3}(x)$ denotes the Euler polynomial of degree $p-3$.

(1.3) in the case $d = 0$ was first conjectured by Rodriguez-Villegas [RV] in 2003 and later proved by Mortenson [M1] via an advanced tool involving the $p$-adic Gamma function and the Gross-Koblitz formula for character sums. (See also S. Ahlgren [A] and K. Ono [O] for such an approach.) (1.4) with $d = 0$ yields the congruence
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(k/8)^2} \equiv \left(\frac{-1}{p}\right) + p^2 E_{p-3} \left(d + \frac{1}{2}\right) \pmod{p^3},
\]
which was first proved in [S4] with the help of the software Sigma.

Let $p \equiv 1 \pmod{4}$ be a prime. It is well known that $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ with $x \equiv 1 \pmod{4}$ and $y \equiv 0 \pmod{2}$. A celebrated result of Gauss asserts that \((p-1)/2 \equiv 2x \pmod{p}\). This was refined in [CDP] as follows:
\[
\left(\frac{(p-1)/2}{p-1}/4\right) \equiv \frac{2p+1}{2} \left(2x - \frac{p}{2x}\right) \pmod{p^2}.
\]

Recently the author’s twin brother Z. H. Sun [Su] confirmed the author’s following conjecture (cf. [S3, Conjecture 5.5]):
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(k/8)^2} \equiv \sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(-16)^k} \equiv \left(\frac{2}{p}\right) \sum_{k=0}^{(p-1)/2} \frac{2k/8^2}{32k} \equiv \left(\frac{2}{p}\right) \left(2x - \frac{p}{2x}\right) \pmod{p^2}.
\]

In [S5] the author showed that
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(k/8)^2} \equiv -2 \sum_{k=0}^{p-1} \frac{k(2k/8)^2}{8k} \equiv \frac{1}{2} \sum_{k=0}^{(p-1)/2} \frac{(2k/8)^2}{(-16)^k} \equiv -4 \sum_{k=0}^{(p-1)/2} \frac{k(2k/8)^2}{(-16)^k} \equiv \left(\frac{2}{p}\right) \left(2x - \frac{p}{x}\right) \pmod{p^2},
\]
where $C_k$ denotes the Catalan number $(\frac{2k}{k})/(k+1) = \binom{2k}{k} - \binom{2k}{k+1}$. (Note that Catalan numbers occur naturally in many enumeration problems in combinatorics, see, e.g., [St, pp. 219–229].)

Motivated by (1.2) in the cases $\lambda = -1, 2$ we obtain the following result.

**Theorem 1.3.** Let $p$ be an odd prime.

(i) If $p \equiv 3 \pmod{4}$, then
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k)C_k}{8^k} \equiv -2 \sum_{k=0}^{(p-1)/2} \frac{k(2k)^2}{8^k} \equiv -\frac{1}{2} \sum_{k=0}^{(p-1)/2} \frac{(2k)C_k}{(-16)^k} \equiv 4 \sum_{k=0}^{(p-1)/2} \frac{k(2k)^2}{(-16)^k} \equiv (-1)^{(p+1)/4} \frac{(p+1)/2}{(p+1)/4} \pmod{p} \tag{1.5}
\]
and
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k)^2}{8^k} \equiv -\sum_{k=0}^{(p-1)/2} \frac{(2k)^2}{(-16)^k} \equiv \frac{2p(-1)^{(p+1)/4}}{(p+1)/2} \pmod{p^2}. \tag{1.6}
\]

(ii) We have
\[
\sum_{k=0}^{(p-1)/2} \frac{(2k)(2k)}{8^k(k+d)} \equiv 0 \pmod{p} \tag{1.7}
\]
for all $d \in \{0, \ldots, (p-1)/2\}$ with $d \equiv (p+1)/2 \pmod{2}$.

Besides (1.3) with $d = 0$, Rodriguez-Villegas [RV] also raised the following similar conjectures (confirmed in [M1-M3]) on super congruences with $p$ a prime greater than 3:

\[
\sum_{k=0}^{p-1} \frac{(3k)(2k)}{27^k} \equiv \frac{p}{3} \pmod{p^2}, \tag{1.8}
\]
\[
\sum_{k=0}^{p-1} \frac{(4k)(2k)}{64^k} \equiv \frac{-2}{p} \pmod{p^2}, \tag{1.9}
\]
\[
\sum_{k=0}^{p-1} \frac{(6k)(3k)}{432^k} \equiv \frac{-1}{p} \pmod{p^2}. \tag{1.10}
\]

Note that the denominators 27, 64, 432 come from the following observation via the Stirling formula:

\[
\binom{3k}{k} \binom{2k}{k} \sim \frac{\sqrt{3}}{2k\pi}, \quad \binom{4k}{2k} \binom{2k}{k} \sim \frac{64^k}{\sqrt{2k\pi}}, \quad \binom{6k}{3k} \binom{3k}{k} \sim \frac{432^k}{2k\pi}.
\]
Up to now no simple proofs of (1.8)-(1.10) have been found. Motivated by the work in [PS] and [ST], the author [S2] determined \( \sum_{k=0}^{p-1} \binom{2k}{k}/m^k \) modulo \( p^2 \) in terms of Lucas sequences, where \( p \) is an odd prime and \( m \) is an integer not divisible by \( p \). In [S3] and [S4] the author raised many conjectures on sums of terms involving central binomial coefficients.

Let \( \mathbb{N} = \{0, 1, 2, \ldots \} \). For a sequence of \( (a_n)_{n \in \mathbb{N}} \) of numbers, as in [S1] we introduce its dual sequence \( (a^*_n)_{n \in \mathbb{N}} \) by defining

\[
a^*_n := \sum_{k=0}^{n} \binom{n}{k}(-1)^k a_k \quad (n = 0, 1, 2, \ldots).
\]

It is well-known that \( (a^*_n)^* = a_n \) for all \( n \in \mathbb{N} \) (see, e.g., (5.48) of [GKP, p. 192]). For Bernoulli numbers \( B_0, B_1, B_2, \ldots \), the sequence \( ((-1)^n B_n)_{n \in \mathbb{N}} \) is self-dual.

**Theorem 1.4.** Let \( p > 3 \) be a prime and let \( (a_n)_{n \in \mathbb{N}} \) be any sequence of \( p \)-adic integers. Then we have

\[
\begin{align*}
\sum_{k=0}^{p-1} \frac{\binom{3k}{k}}{27^k} a_k & \equiv \left(\frac{p}{3}\right) \sum_{k=0}^{p-1} \frac{\binom{3k}{k}}{27^k} a^*_k \pmod{p^2}, \\
\sum_{k=0}^{p-1} \frac{\binom{4k}{2k}}{64^k} a_k & \equiv \left(-\frac{2}{p}\right) \sum_{k=0}^{p-1} \frac{\binom{4k}{2k}}{64^k} a^*_k \pmod{p^2}, \\
\sum_{k=0}^{p-1} \frac{\binom{6k}{3k}}{432^k} a_k & \equiv \left(-\frac{1}{p}\right) \sum_{k=0}^{p-1} \frac{\binom{6k}{3k}}{432^k} a^*_k \pmod{p^2}.
\end{align*}
\]

**Remark.** Z. H. Sun [Su] recently proved that

\[
\sum_{k=0}^{\frac{p-1}{2}} \frac{\binom{2k}{k}}{16^k} \left( a_k - \left(-\frac{1}{p}\right) a^*_k \right) \equiv 0 \pmod{p^2}
\]

for any odd prime \( p \) via Legendre polynomials. We can also show for any odd prime \( p > 3 \) the following result similar to (1.3) and (1.4): If \( d \in \{0, \ldots, \lfloor p/3 \rfloor \} \) then

\[
\frac{1}{4^d} \sum_{k=0}^{\frac{p-1}{2}} \frac{\binom{3k}{k}}{27^k} \equiv \frac{\left(-\frac{1}{p}\right)}{3} \pmod{p};
\]

if \( d \in \{0, \ldots, \lfloor p/4 \rfloor \} \) then

\[
\frac{1}{4^d} \sum_{k=0}^{\frac{p-1}{2}} \frac{\binom{4k}{2k}}{64^k} \equiv \frac{\left(-\frac{2}{p}\right)}{p} \pmod{p}.
\]

Since \((1-x)^k = \sum_{j=0}^{k} \binom{k}{j} (-1)^j x^j\), by Theorem 1.4 we have the following result.
Theorem 1.5. Let \( p > 3 \) be a prime. Then, in the ring \( \mathbb{Z}_p[x] \) we have

\[
\sum_{k=0}^{p-1} \frac{3k \choose k} {27 k} \left( x^k - \left( \frac{p}{3} \right) (1-x)^k \right) \equiv 0 \pmod{p^2},
\] (1.14)

\[
\sum_{k=0}^{p-1} \frac{4k \choose 2k} {64 k} \left( x^k - \left( \frac{-2}{p} \right) (1-x)^k \right) \equiv 0 \pmod{p^2},
\] (1.15)

\[
\sum_{k=0}^{p-1} \frac{6k \choose 3k} {432 k} \left( x^k - \left( \frac{-1}{p} \right) (1-x)^k \right) \equiv 0 \pmod{p^2}.
\] (1.16)

Also,

\[
\sum_{k=1}^{p-1} \frac{k \choose k} {27 k} \left( x^{k-1} + \left( \frac{p}{3} \right) (1-x)^{k-1} \right) \equiv 0 \pmod{p^2},
\] (1.17)

\[
\sum_{k=1}^{p-1} \frac{4k \choose 2k} {64 k} \left( x^{k-1} + \left( \frac{-2}{p} \right) (1-x)^{k-1} \right) \equiv 0 \pmod{p^2},
\] (1.18)

\[
\sum_{k=1}^{p-1} \frac{6k \choose 3k} {432 k} \left( x^{k-1} + \left( \frac{-1}{p} \right) (1-x)^{k-1} \right) \equiv 0 \pmod{p^2}.
\] (1.19)

Remark. (1.17)-(1.19) can be easily deduced from (1.14)-(1.16) by taking derivations. Z. H. Sun [Su, Theorem 2.4] noted that for any prime \( p > 3 \) we have

\[
\sum_{k=0}^{\lfloor p/3 \rfloor} \frac{3k \choose k} {27 k} (x^k - (-1)^{\lfloor p/3 \rfloor} (1-x)^k) \equiv 0 \pmod{p}.
\]

Taking \( x = 1/2 \) in (1.14)-(1.19) we immediately get the following result.

Corollary 1.1. Let \( p > 3 \) be a prime. Then

\[
\sum_{k=0}^{p-1} \frac{k \choose k} {54 k} \equiv 0 \pmod{p^2} \quad \text{if} \ p \equiv 1 \pmod{3},
\]

\[
\sum_{k=0}^{p-1} \frac{3k \choose 2k} {54 k} \equiv 0 \pmod{p^2} \quad \text{if} \ p \equiv 1, 3 \pmod{8},
\]

\[
\sum_{k=0}^{p-1} \frac{4k \choose 2k} {128 k} \equiv 0 \pmod{p^2} \quad \text{if} \ p \equiv 1, 3 \pmod{8},
\]

\[
\sum_{k=0}^{p-1} \frac{4k \choose 2k} {128 k} \equiv 0 \pmod{p^2} \quad \text{if} \ p \equiv 5, 7 \pmod{8};
\]
Corollary 1.2. Let \( x = \frac{9}{8} \) be a prime. Then

\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{24^k} \equiv \left( \frac{p}{3} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{216^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{24^k} \equiv -9 \left( \frac{p}{3} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{216^k} \pmod{p^2};
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{48^k} \equiv \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{(-192)^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{48^k} \equiv 4 \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{(-192)^k} \pmod{p^2};
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{72^k} \equiv \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{576^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{72^k} \equiv -8 \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{576^k} \pmod{p^2}.
\]

If \( p \neq 7 \) then

\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{63^k} \equiv \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{(-4032)^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{63^k} \equiv 64 \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{(-4032)^k} \pmod{p^2}.
\]

Remark. The first and the second congruences mod \( p \) were obtained by Z. H. Sun [Su]. The author [S4] and Z. H. Sun [Su] conjectured the first and the second congruences respectively. Mathematica yields that

\[
\sum_{k=0}^{\infty} \frac{k(2k)(3k)}{54^k} = \frac{\sqrt{\pi}}{9\Gamma\left(\frac{4}{3}\right)\Gamma\left(\frac{2}{3}\right)}.
\]

(1.14) and (1.17) in the case \( x = 9/8 \), and (1.15) and (1.18) in the cases \( x = 4/3, 8/9, 64/63 \), yield the following result.

Corollary 1.2. Let \( p > 3 \) be a prime. Then

\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{24^k} \equiv \left( \frac{p}{3} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{216^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{24^k} \equiv -9 \left( \frac{p}{3} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{216^k} \pmod{p^2};
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{48^k} \equiv \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{(-192)^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{48^k} \equiv 4 \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{(-192)^k} \pmod{p^2};
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{72^k} \equiv \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{576^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \frac{k(3k)(2k)}{72^k} \equiv -8 \left( \frac{p}{2} \right) \sum_{k=0}^{p-1} \frac{k(3k)(2k)}{576^k} \pmod{p^2}.
\]
Remark. In [S4, Conjecture 5.13] the author conjectured that
\[
\sum_{k=0}^{p-1} \binom{2k}{k} \binom{3k}{k} \frac{2^{4k}}{24k} \equiv \sum_{k=0}^{p-1} \binom{2k}{k} \binom{3k}{k} \frac{(-216)^k}{24k} \equiv \begin{cases} \frac{2^{(p-1)/3}}{(p-1)/3} \pmod{p^2} & \text{if } p \equiv 1 \pmod{6}, \\ 0 \pmod{p} & \text{if } p \equiv 5 \pmod{6}. \end{cases}
\]

The author [S4] also made conjectures on \(\sum_{k=0}^{p-1} \binom{2k}{k} \binom{3k}{k} C_k m^k \pmod{p^2}\) or \(p\) with \(m = 48, 63, 72, 128\); the mod \(p\) case has been confirmed by Z. H. Sun recently.

For any prime \(p > 3\) and integer \(m \not\equiv 0 \pmod{p}\), we have
\[
\sum_{k=0}^{p-1} \binom{3k}{k} C_k \frac{m^k}{m^k} \equiv p + \frac{m - 27}{6} \sum_{k=0}^{p-1} \binom{2k}{k} \binom{3k}{k} \frac{k}{m^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \binom{4k}{2k} C_k \frac{m^k}{m^k} \equiv p + \frac{m - 64}{12} \sum_{k=0}^{p-1} \binom{2k}{k} \binom{3k}{k} \frac{k}{m^k} \pmod{p^2},
\]
\[
\sum_{k=0}^{p-1} \binom{6k}{3k} \binom{3k}{k} \frac{m^k}{m^k} \equiv p + \frac{m - 432}{60} \sum_{k=0}^{p-1} \binom{2k}{k} \binom{3k}{k} \frac{k}{m^k} \pmod{p^2},
\]
due to the identities
\[
\sum_{k=0}^{n-1} \left( 6C_k + (27 - m)k \binom{2k}{k} \right) \frac{(3k)^k}{m^k} = \frac{n}{m^{n-1}} \binom{2n}{n} \binom{3n}{n},
\]
\[
\sum_{k=0}^{n-1} \left( 12C_k + (64 - m)k \binom{2k}{k} \right) \frac{(4k)^k}{m^k} = \frac{n}{m^{n-1}} \binom{4n}{2n} \binom{2n}{n},
\]
\[
\sum_{k=0}^{n-1} \left( \frac{60}{k+1} + (432 - m)k \right) \frac{(6k)^k}{m^k} = \frac{n}{m^{n-1}} \binom{6n}{3n} \binom{3n}{n},
\]
which can be easily proved by induction on \(n\). So, the following result follows from Corollary 1.1 and the second congruence in Corollary 1.2.

Corollary 1.3. Let \(p > 3\) be a prime. Then
\[
\sum_{k=0}^{p-1} \binom{3k}{k} C_k \frac{54^k}{54^k} \equiv p \pmod{p^2} \text{ if } p \equiv 1 \pmod{3}, \tag{1.20}
\]
\[
\sum_{k=0}^{p-1} \binom{4k}{2k} C_k \frac{128^k}{128^k} \equiv p \pmod{p^2} \text{ if } p \equiv 1, 3 \pmod{8}, \tag{1.21}
\]
\[
\sum_{k=0}^{p-1} \binom{6k}{3k} \binom{3k}{k} \frac{(k+1)864^k}{(k+1)864^k} \equiv p \pmod{p^2} \text{ if } p \equiv 1 \pmod{4}. \tag{1.22}
\]
We also have
\[ \sum_{k=0}^{p-1} \frac{(3k)_C k}{24k} \equiv p + \frac{1}{9} \left( \frac{p}{3} \right) \left( \sum_{k=0}^{p-1} \frac{(3k)_C k}{(-216)^k} - p \right) \pmod{p^2}. \] (1.23)

Remark. Via Mathematica we find that
\[ \sum_{k=0}^{\infty} \frac{(3k)_C k}{54^k} = \frac{3\sqrt{\pi}}{\Gamma(\frac{4}{3})\Gamma(\frac{1}{6})}, \quad \sum_{k=0}^{\infty} \frac{(4k)_C k}{128^k} = \frac{4\sqrt{\pi}}{\Gamma(\frac{1}{8})\Gamma(\frac{17}{8})}, \]
and
\[ \sum_{k=0}^{\infty} \frac{(6k)_C (3k)_C k}{(k+1)864^k} = \frac{6\sqrt{\pi}}{\Gamma(\frac{1}{12})\Gamma(\frac{11}{12})}. \]

**Theorem 1.6.** Let \( p > 3 \) be a prime. Then
\[ \sum_{k=0}^{p-1} k \frac{(4k)_C (2k)_C k}{72^k} \equiv \frac{3}{2} \sum_{k=0}^{p-1} \frac{(4k)_C k}{72^k} \equiv \begin{cases} \frac{6}{p}x \pmod{p}, & \text{if } p = x^2 + y^2 \ (4 \mid x-1 \& 2 \mid y), \\ \frac{3}{4} \left( \frac{6}{p} \right) \left( \frac{p+1}{2} \right) \pmod{p}, & \text{if } p \equiv 3 \pmod{4}. \end{cases} \]

---

2. Proofs of Theorems 1.1-1.3

**Proof of Theorem 1.1.** Set \( n = (p-1)/2 \). Then
\[ a_p^{(d)}(\lambda) \equiv \sum_{k=0}^{p-1} x^d (x(x-1)(x-\lambda))^n \]
\[ = \sum_{k=0}^{p-1} x^{n+d} \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} x^k \sum_{l=0}^{n} \binom{n}{l} (-\lambda)^l x^{n-l} \]
\[ = \sum_{k,l=0}^{n} \binom{n}{k} \binom{n}{l} (-1)^{n-k} (-\lambda)^l \sum_{x=1}^{p-1} x^{p-1+d+k-l} \]
\[ \equiv \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} \sum_{0 \leq l \leq n} \binom{n}{l} (-\lambda)^l (p-1) \]
\[ \equiv -\sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} \binom{n}{d+k} (-\lambda)^{d+k} - \delta_{d,n} \binom{n}{0} (-\lambda)^0 \pmod{p}. \]
Since
\[ \binom{n}{k} \equiv (-1/2)^k \binom{2k}{k} \pmod{p} \quad \text{for all } k = 0, \ldots, p - 1, \]
we immediately obtain (1.2) from the above. □

Proof of Theorem 1.2. Let \( n = (p - 1)/2 \). By Mathematica, for \( m = 0, \ldots, n \) we have
\[
\sum_{k=0}^{n} \frac{\binom{2k}{k}}{16^k} \left( \binom{2k}{k + m} - \binom{2k}{k + m + 1} \right) = \frac{2n + 1}{(2m + 1)16^n} \binom{2n}{n} \binom{2n + 1}{n - m}.
\]
If \( 0 \leq m < n \), then for the right-hand side \( R_m \) of the last identity we have
\[
R_m = p^2 \left( \frac{p - 1}{(2m + 1)((p - 1)/2 - m)4^{p-1}} \right) \binom{p - 1}{n} \binom{p - 1}{n - m - 1}
\equiv 2p^2 \binom{(-1)^m}{(2m + 1)^2} \pmod{p^3}.
\]
As \( d \leq n \), we have
\[
\sum_{k=0}^{n} \frac{\binom{2k}{k}}{16^k} \left( \binom{2k}{k} - \binom{2k}{k + d} \right)
= \sum_{0 \leq m < d} \sum_{k=0}^{n} \frac{\binom{2k}{k}}{16^k} \left( \binom{2k}{k + m} - \binom{2k}{k + m + 1} \right)
\equiv 2p^2 \sum_{0 \leq m < d} \frac{(-1)^m}{(2m + 1)^2} \equiv \frac{p^2}{2} \sum_{0 \leq m < d} (-1)^m \left( m + \frac{1}{2} \right)^{p-3}
\equiv \frac{p^2}{4} \sum_{0 \leq m < d} (-1)^m \left( E_{p-3} \left( m + \frac{1}{2} \right) + E_{p-3} \left( m + 1 + \frac{1}{2} \right) \right)
\equiv \frac{p^2}{4} \left( E_{p-3} \left( \frac{1}{2} \right) - (-1)^d E_{p-3} \left( d + \frac{1}{2} \right) \right) \pmod{p^3}.
\]
Note that
\[
\sum_{k=0}^{n} \frac{\binom{2k}{k} \binom{2k}{k+n}}{16^k} = \frac{\binom{2n}{n}}{16^n} = \frac{\binom{p-1}{(p-1)/2}}{4^{p-1}} \equiv \frac{(-1)}{p} = (-1)^n \pmod{p^3}
\]
by Morley’s congruence ([M]), and \( E_{p-3}(n+1/2) = E_{p-3}(p/2) \equiv E_{p-3}(0) = 0 \pmod{p} \). Therefore
\[
\sum_{k=0}^{n} \frac{\binom{2k}{k}^2}{16^k} - (-1)^n \equiv \frac{p^2}{4} E_{p-3} \left( \frac{1}{2} \right) \equiv (-1)^n + p^2 E_{p-3} \pmod{p^3}
\]
and hence (1.4) follows from the above. For \( k = 0, 1, \ldots \), we have

\[
\binom{2k + 2d}{k + d} = \sum_{c=-d}^{d} \binom{2k}{k + c} \binom{2d}{d - c}
\]

by the Chu-Vandermonde identity. Therefore

\[
\sum_{k=0}^{n} \binom{2k}{k+d} \binom{2k}{k/d} = \sum_{c=-d}^{d} \binom{2d}{d-c} \sum_{k=0}^{n} \binom{2k}{k+c} \frac{2}{16^k} \\
\equiv \sum_{c=-d}^{d} \binom{2d}{d-c} \frac{-1}{p} = 2^{2d} \left( \frac{-1}{p} \right) \pmod{p^2}.
\]

So (1.3) is valid and we are done. □

**Proof of Theorem 1.3.** (i) For \( m \in \mathbb{Z} \setminus \{0\} \) and \( n \in \mathbb{N} \) we have the combinatorial identity

\[
\sum_{k=0}^{n} \left( \frac{16 - m}{4} k + 1 \right) \binom{2k}{k} m^k = \frac{(2n + 1)^2}{(n+1)n} \left( \binom{2n}{n} \right)^2
\]

which can be easily proved by induction on \( n \). Setting \( n = (p - 1)/2 \) we obtain from the identity that

\[
\sum_{k=0}^{n} \frac{(2k) C_k}{m^k} \equiv m - 16 \sum_{k=0}^{n} \frac{k(2k)^2}{m^k} \pmod{p^2}
\]

for any integer \( m \not\equiv 0 \pmod{p} \).

As \( n = (p - 1)/2 \) is odd, by a result of Z. H. Sun [Su],

\[
\sum_{k=0}^{n} \frac{(2k)^2}{16^k} \left( x^k + (1-x)^k \right) = p^2 f(x)
\]

for some polynomial \( f(x) \) of degree at most \( (p - 1)/2 \) with rational \( p \)-adic integer coefficients. In particular, \( \sum_{k=0}^{n} \frac{(2k)^2}{8^k} \equiv - \sum_{k=0}^{n} \frac{(2k)^2}{(-16)^k} \pmod{p^2} \). By integration,

\[
\sum_{k=0}^{n} \frac{(2k)^2}{(k+1)16^k} x^{k+1} - \sum_{k=0}^{n} \frac{(2k)^2}{(k+1)16^k} ((1-x)^{k+1} - 1) = p^2 \int_{0}^{x} f(t) dt.
\]
Putting $x = -1$ we obtain

$$- \sum_{k=0}^{n} \frac{(2^k)C_k}{(-16)^k} - \sum_{k=0}^{n} \frac{(2^k)C_k}{16^k} (2^{k+1} - 1) \equiv 0 \pmod{p^2}.$$ 

Since

$$\sum_{k=0}^{n} \frac{(2^k)C_k}{16^k} = \frac{(2n+1)^2}{16(n+1)} \left( \frac{2n}{n} \right)^2 \equiv 0 \pmod{p^2},$$

as observed by van Hammer [vH], we have

$$\sum_{k=0}^{n} \frac{(2^k)C_k}{(-16)^k} \equiv -2 \sum_{k=0}^{n} \frac{(2^k)C_k}{8^k} \pmod{p^2}.$$ 

Clearly,

$$\sum_{k=0}^{n} \frac{(2^k)^2}{(-16)^k} = \sum_{k=0}^{n} (-1)^k \frac{(-1)^k}{k} \equiv \sum_{k=0}^{n} (-1)^k \frac{n^2}{k} = 0 \pmod{p}.$$ 

(Note that $(-1)^n-k = (-1)^k$.) Thus

$$\sum_{h=0}^{p-1} \frac{2h+1}{(-16)^h} \sum_{k=0}^{h} \frac{(2^k)^2}{k} \left( \frac{2(h-k)}{h-k} \right)^2 \equiv \sum_{k=0}^{n} \frac{(2^k)^2}{(-16)^k} \sum_{j=0}^{n} \frac{j(2^j)^2}{(-16)^j} \pmod{p^2}.$$ 

By [S5, Lemma 3.1],

$$\sum_{h=0}^{p-1} \frac{2h+1}{(-16)^h} \sum_{k=0}^{h} \frac{(2^k)^2}{k} \left( \frac{2(h-k)}{h-k} \right)^2 \equiv p \left( \frac{-1}{p} \right) = -p \pmod{p^2}.$$ 

Therefore

$$\frac{1}{p} \sum_{k=0}^{n} \frac{(2^k)^2}{(-16)^k} \times \sum_{k=0}^{n} k(2^k)^2 \equiv -\frac{1}{4} \pmod{p}.$$ 

In view of the above, both (1.5) and (1.6) hold if

$$\sum_{k=0}^{n} \frac{(2^k)C_k}{8^k} \equiv \frac{(-1)^{(p+1)/4}}{2} \left( \frac{(p+1)/2}{(p+1)/4} \right) \pmod{p}. \quad (2.1)$$
For $d = 0, 1$ clearly
\[ a_p^{(d)}(2) = \sum_{x=1}^{p} x^d \left( \frac{x(x-1)(x-2)}{p} \right) = \sum_{r=0}^{p-1} (r+1)^d \left( \frac{r^2 - 1}{p} \right) \]

and
\[ a_p^{(d)}(-1) = \sum_{r=0}^{p-1} r^d \left( \frac{r^2 - 1}{p} \right) \]
\[ \equiv \sum_{r=0}^{p-1} r^{d+n} (r^2 - 1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} \sum_{r=1}^{p-1} r^{n+d+2k} \]
\[ \equiv - \sum_{0 \leq k \leq n \atop p-1 | n+d+2k} \binom{n}{k} (-1)^{n-k} \equiv \begin{cases} 0 \pmod{p} & \text{if } d = 0, \\ (-1)^{(p-3)/4} \binom{n}{(n-1)/2} \pmod{p} & \text{if } d = 1. \end{cases} \]

Thus we have
\[ a_p^{(0)}(2) = a_p^{(0)}(-1) \equiv 0 \pmod{p} \]

and
\[ a_p^{(1)}(2) = a_p^{(0)}(-1) + a_p^{(1)}(-1) \equiv (-1)^{(p-3)/4} \binom{n}{(n-1)/2} \pmod{p}. \]

Applying Theorem 1.1 with $\lambda = 2$ and $d = 0, 1$, and noting that
\[ \frac{1}{2} \binom{2k+2}{k+1} = \binom{2k+1}{k+1} = \binom{2k}{k} + \binom{2k}{k+1} = 2 \binom{2k}{k} - C_k \quad (k = 0, 1, \ldots), \]
we get
\[ \sum_{k=0}^{n} \frac{(2k)C_k}{8^k} + \delta_{p,3} \equiv 2a_p^{(0)}(2) - a_p^{(1)}(2) \pmod{p}. \]

So (2.1) follows.

(ii) Now we prove (1.7) for all $d \in \{0, \ldots, n\}$ with $d \equiv n+1 \pmod{2}$, where $n = (p-1)/2$. (1.7) is valid for $d = n-1$ since
\[ \sum_{k=0}^{n} \frac{(2k)C_{k+n-1}}{8^k} = \frac{(2^{n-1})}{8^{n-1}} + \frac{2n(2n)}{8^n} = \frac{2n+1}{2 \times 8^{n-1}} \binom{2n-2}{n-1} \equiv 0 \pmod{p}. \]
Define
\[ f(d) := \sum_{k=0}^{n} \binom{n+k}{2k} \binom{2k}{k+d} (-2)^k \quad \text{for } d = 0, 1, \ldots . \]

Since
\[ \binom{n+k}{2k} \equiv \frac{(2k)}{(-16)^k} \quad \text{(mod } p^2) \quad \text{for } k = 0, \ldots , n \]
(see, e.g., [Su, Lemma 2.2]), we have
\[ f(d) \equiv \sum_{k=0}^{n} \frac{(2k)(2k)}{8k} \quad \text{(mod } p^2) \]
for all \( d = 0, \ldots , n \). By the Zeilberger algorithm,
\[ (n - d - 1)(n + d + 2)(2d + 1)f(d + 2) \]
\[ = (2n + 1)^2(d + 1)f(d + 1) - (n - d)(n + d + 1)(2d + 3)f(d). \]

Note that \( 2n + 1 = p \). So, if \( 0 \leq d \leq n - 2 \), then
\[ f(d) \equiv -\frac{(n - d - 1)(n + d + 2)(2d + 1)}{(n - d)(n + d + 1)(2d + 3)}f(d + 2) \quad \text{(mod } p^2) \]
and hence
\[ f(d + 2) \equiv 0 \quad \text{(mod } p) \implies f(d) \equiv 0 \quad \text{(mod } p). \]

Now it is clear that (1.7) holds for all \( d \in \{0, \ldots , n\} \) with \( d \equiv n+1 \) (mod 2).

3. Proof of Theorem 1.4

Proof of (1.11). Observe that
\[ \sum_{k=0}^{p-1} \frac{\binom{3k}{k} \binom{2k}{k}}{27^k} a_k^2 = \sum_{k=0}^{p-1} \frac{\binom{3k}{k} \binom{2k}{k}}{27^k} \sum_{m=0}^{k} \binom{k}{m} (-1)^m \]
\[ = \sum_{m=0}^{p-1} (-1)^m a_m \sum_{k=m}^{p-1} \frac{\binom{3k}{k} \binom{2k}{k}}{27^k} \binom{k}{m} . \]

So it suffices to show that
\[ \sum_{k=m}^{p-1} \frac{\binom{3k}{k} \binom{2k}{k}}{27^k} \binom{k}{m} \equiv \left( \frac{p}{3} \right) \frac{\binom{3m}{m} \binom{2m}{m}}{(-27)^m} \quad \text{(mod } p^2) \]
for all \( m = 0, 1, \ldots, p - 1 \).

For \( 0 \leq m < n \) define

\[ f_n(m) = \sum_{k=m}^{n-1} \frac{\binom{3k}{k} \binom{2k}{k}}{27^k} \binom{k}{m}. \]

By Zeilberger’s algorithm (see, e.g., [PWZ] for this method) via the software Mathematica 7 (version 7),

\[ 9(m + 1)^2 f_n(m + 1) + (3m + 1)(3m + 2)f_n(m) \]

\[ = \frac{(3n - 1)(3n - 2)}{27^n - 1} \binom{n - 1}{m} \binom{2n - 2}{n - 1} \binom{3n - 3}{n - 1}. \]

Applying this with \( n = p > m + 1 \geq 1 \) and noting that

\[ \binom{2p - 2}{p - 1} = \frac{p}{2p - 1} \binom{2p - 1}{p - 1} \equiv -p \pmod{p^2} \]

and

\[ \binom{3p - 3}{p - 1} = \frac{p}{3p - 2} \binom{3p - 2}{p - 2} \equiv -\frac{p}{2} \pmod{p^2}, \]

we get

\[ 9(m + 1)^2 f_p(m + 1) + (3m + 1)(3m + 2)f_p(m) \]

\[ \equiv \frac{(3p - 1)(3p - 2)}{27^{p-1}} \binom{p - 1}{m} \frac{p^2}{2} \equiv (-1)^m p^2 \pmod{p^3} \]

and hence

\[ f_p(m + 1) - \left( \frac{p}{3} \right) \frac{\binom{3m+3}{m+1} \binom{2m+2}{m+1}}{(-27)^{m+1}} \]

\[ + \frac{(3m + 1)(3m + 2)}{9(m + 1)^2} \left( f_p(m) - \left( \frac{p}{3} \right) \frac{\binom{3m}{m} \binom{2m}{m}}{(-27)^m} \right) \]

\[ = f_p(m + 1) + \frac{(3m + 1)(3m + 2)}{9(m + 1)^2} f_p(m) \equiv p^2 \frac{(-1)^m}{9(m + 1)^2} \pmod{p^3}. \]

Thus

\[ f_p(m) \equiv \left( \frac{p}{3} \right) \frac{\binom{3m}{m} \binom{2m}{m}}{(-27)^m} \pmod{p^2} \]

\[ \implies f_p(m + 1) \equiv \left( \frac{p}{3} \right) \frac{\binom{3(m+1)}{m+1} \binom{2(m+1)}{m+1}}{(-27)^{m+1}} \pmod{p^2}. \] (3.1)
Since
\[ f_p(0) = \sum_{k=0}^{p-1} \frac{\binom{3k}{k} \binom{2k}{k}}{27^k} \equiv \left( \frac{2}{3} \right) \binom{3 \times 0}{0} \binom{2 \times 0}{0} \pmod{p^2} \]
by (1.8), from the above we obtain that
\[ f_p(m) \equiv \left( \frac{2}{3} \right) \binom{3m}{m} \binom{2m}{m} \pmod{p^2} \]
for all \( m = 0, 1, \ldots, p - 1 \).

This concludes the proof. \( \square \)

**Proof of (1.12).** Similar to the proof of (1.6), we only need to show that
\[ \sum_{k=m}^{p-1} \frac{\binom{4k}{2k} \binom{2k}{k}}{64^k} \binom{k}{m} \equiv \left( \frac{-2}{p} \right) \binom{2m}{m} \pmod{p^2} \]
for all \( m = 0, 1, \ldots, p - 1 \). Since the last congruence holds for \( m = 0 \) by (1.3), it suffices to prove that for any fixed \( 0 \leq m < p - 1 \) we have
\[ g_p(m) \equiv \left( \frac{-2}{p} \right) \binom{4m}{2m} \pmod{p^2} \]
where
\[ g_n(m) := \sum_{k=m}^{n-1} \frac{\binom{4k}{2k} \binom{2k}{k}}{64^k} \binom{k}{m} \]
with \( n > m \). By the Zeilberger algorithm, we find that
\[ 16(m+1)^2 g_n(m+1) + (4m+1)(4m+3)g_n(m) = \frac{(4n-1)(4n-3)}{64^{n-1}} \binom{n-1}{m} \binom{2n-2}{n-1} \binom{4n-4}{2n-2}. \]
Recall the congruence \( \binom{2p-2}{p-1} \equiv -p \pmod{p^2} \) and note that
\[ \binom{4p-4}{2p-2} = \frac{2p(2p-1)}{(4p-2)(4p-3)} \binom{4p-2}{2p-2} \equiv p \pmod{p^2}. \]
So we have
\[ 16(m+1)^2 g_p(m+1) + (4m+1)(4m+3)g_p(m) \equiv 3(-1)^m (-p^2) \pmod{p^3}. \]
This implies (3.2) since
\[- \frac{(4m + 1)(4m + 3)}{16(m + 1)^2} \cdot \frac{(4m)}{2m}(\frac{2m}{m}) = \frac{(4(m+1))}{2(m+1)}(\frac{2(m+1)}{m+1})\cdot (-64)^m = (-64)^{m+1}.
\]

We are done.  □

**Proof of (1.13).** For 0 \(\leq m < n\) define
\[h_n(m) := \sum_{k=m}^{n-1} \frac{6k}{3k} \binom{3k}{k} \binom{k}{m}.
\]

By the Zeilberger algorithm we have
\[36(m + 1)^2 h_n(m + 1) + (6m + 1)(6m + 5) h_n(m) = \frac{(6n - 1)(6n - 5)}{432^{n-1}} \binom{n-1}{m} \binom{3n - 3}{n-1} \binom{6n - 6}{3n - 3}.
\]

Recall the congruence \(\frac{3p-3}{p-1} \equiv -p/2 \pmod{p^2}\) and note that
\[
\binom{6p - 6}{3p - 3} = \frac{3p(3p-1)(3p-2)}{(6p-3)(6p-4)(6p-5)} \binom{6p - 3}{3p - 3}
\equiv - \frac{p}{10} \binom{5p + (p - 3)}{2p + (p - 3)} \equiv - \frac{p}{10} \binom{5}{2} = -p \pmod{p^2}
\]
if \(p > 5\). Whether \(p = 5\) or not, we always have
\[36(m + 1)^2 h_p(m + 1) + (6m + 1)(6m + 5) h_p(m) \equiv 0 \pmod{p^2}.
\]

For 0 \(\leq m < p - 1\), since
\[- \frac{(6m + 1)(6m + 5)}{36(m + 1)^2} \cdot \frac{(6m)}{3m} \binom{3m}{m} = \frac{(6(m+1))}{3(m+1)} \binom{3(m+1)}{m+1} \cdot (-432)^m = (-432)^{m+1},
\]
by the above we have
\[h_p(m) \equiv \left(\frac{-1}{p}\right) \frac{(6m)}{3m} \binom{3m}{m} \binom{m}{-432}^m \pmod{p^2}
\]
\[\Rightarrow h_p(m + 1) \equiv \left(\frac{-1}{p}\right) \frac{(6(m+1))}{3(m+1)} \binom{3(m+1)}{m+1} \binom{m+1}{-432}^{m+1} \pmod{p^2}.
\]

This together with (1.4) yields that
\[h_p(m) \equiv \left(\frac{-1}{p}\right) \frac{(6m)}{3m} \binom{3m}{m} \binom{m}{-432}^m \pmod{p^2}
\]
for all \( m = 0, \ldots, m - 1 \). It follows that

\[
\sum_{k=0}^{p-1} \frac{(6k)(3k)}{432^k} \sum_{m=0}^{k} \binom{k}{m} (-1)^m a_m
\]

\[=
\sum_{m=0}^{p-1} (-1)^m a_m h_p(m) \equiv \left( \frac{-1}{p} \right) \sum_{m=0}^{p-1} a_m \binom{6m}{3m} \binom{3m}{m} (-432)^m \pmod{p^2}.
\]

This proves (1.13). \( \square \)

### 4. Proof of Theorem 1.5

Recall that

\[
\sum_{k=0}^{p-1} \frac{(4k)(2k)}{72^k} \equiv p + \frac{72 - 64}{12} \sum_{k=0}^{p-1} \frac{k(4k)(2k)}{72^k} \pmod{p^2}
\]

and hence

\[
\sum_{k=0}^{p-1} \frac{k(4k)(2k)}{72^k} \equiv \frac{3}{2} \sum_{k=0}^{p-1} \frac{(4k)(2k)}{72^k} \pmod{p}.
\]

Below we determine \( \sum_{k=0}^{n} k(4k)(2k)/72k \pmod{p} \), where \( n = (p - 1)/2 \).

(Note that \( p \mid (2k) \) for \( k = n + 1, \ldots, p - 1 \).)

The Legendre polynomial of degree \( n \) is given by

\[
P_n(x) := \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} \left( \frac{x-1}{2} \right)^k = \sum_{k=0}^{n} \binom{n+k}{2k} \frac{(x-1)^k}{2^k}.
\]

It is known that

\[
\sum_{k=0}^{n} \binom{n}{2k} \frac{(2k)^k}{k!} x^k = (\sqrt{1 - 4x})^n P_n \left( \frac{1}{\sqrt{1 - 4x}} \right).
\]

(Note that the left-hand side is the coefficient of \( t^n \) in \( (t^2 + t + x)^n \).) Taking derivations of both sides of the last equality, we get

\[
\sum_{k=0}^{n} \binom{n}{2k} \frac{(2k)^k}{k!} x^k = -2n(1 - 4x)^{n/2-1} \sum_{k=0}^{n} \binom{n+k}{2k} \frac{(1-4x)^{-1/2} - 1}{2}^k
\]

\[
+ (1-4x)^{(n-3)/2} \sum_{k=0}^{n} \binom{n+k}{2k} \frac{(1-4x)^{-1/2} - 1}{2}^{k-1}
\]
Since
\[
\binom{n}{2k} \equiv \left( -\frac{1}{2} \right) \binom{4k}{2k} \left( -\frac{1}{4} \right)^{2k} \pmod{p}
\]
and
\[
\binom{n+k}{2k} \equiv \binom{2k}{k} \left( -\frac{1}{16} \right)^k \pmod{p^2}
\]
for all \(k = 0, \ldots, n\), by putting \(x = 2/9\) in the last equality we obtain
\[
\frac{1}{2} \sum_{k=0}^{n} \frac{k \binom{4k}{2k} \binom{2k}{k}}{72^k} \equiv \frac{1}{3^n} \sum_{k=0}^{n} \binom{2k}{k}^2 \left( -\frac{1}{16} \right)^k + \frac{3}{3^n} \sum_{k=0}^{n} \frac{k \binom{2k}{k}^2}{(-16)^k} \pmod{p}
\]
and hence
\[
\left( \frac{3}{p} \right) \sum_{k=0}^{n} \frac{k \binom{4k}{2k} \binom{2k}{k}}{72^k} \equiv 2 \sum_{k=0}^{n} \frac{k \binom{2k}{k}^2}{16^k} + 6 \sum_{k=0}^{n} \frac{k \binom{2k}{k}^2}{(-16)^k} \pmod{p}.
\]

Thus, with the help of Theorem 1.5 and the related known results for the case \(p \equiv 1 \pmod{4}\), we finally obtain the desired result.

The proof of Theorem 1.5 is now complete.

**References**

[A] S. Ahlgren, *Gaussian hypergeometric series and combinatorial congruences*, in: Symbolic computation, number theory, special functions, physics and combinatorics (Gainesville, FL, 1999), pp. 1-12, Dev. Math., Vol. 4, Kluwer, Dordrecht, 2001.

[BEW] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley & Sons, 1998.

[C] D. A. Cox, *Primes of the Form \(x^2 + ny^2\)*, John Wiley & Sons, 1989.

[G] H. W. Gould, *Combinatorial Identities*, Morgantown Printing and Binding Co., 1972.

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, 2nd ed., Addison-Wesley, New York, 1994.

[HW] R. H. Hudson and K. S. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. 281 (1984), 431–505.

[M1] E. Mortenson, *A supercongruence conjecture of Rodriguez-Villegas for a certain truncated hypergeometric function*, J. Number Theory 99 (2003), 139–147.

[M2] E. Mortenson, *Supercongruences between truncated \(2F_1\) by geometric functions and their Gaussian analogs*, Trans. Amer. Math. Soc. 355 (2003), 987–1007.

[M3] E. Mortenson, *Supercongruences for truncated \(n+1F_n\) hypergeometric series with applications to certain weight three newforms*, Proc. Amer. Math. Soc. 133 (2005), 321–330.

[M4] E. Mortenson, *A p-adic supercongruence conjecture of van Hamme*, Proc. Amer. Math. Soc. 136 (2008), 4321–4328.

[O] K. Ono, *Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-series*, Amer. Math. Soc., Providence, R.I., 2003.

[PS] H. Pan and Z. W. Sun, *A combinatorial identity with application to Catalan numbers*, Discrete Math. 306 (2006), 1921–1940.

[PWZ] M. Petkovšek, H. S. Wilf and D. Zeilberger, *A = B*, A K Peters, Wellesley, 1996.
[RV] F. Rodriguez-Villegas, *Hypergeometric families of Calabi-Yau manifolds*, in: Calabi-Yau Varieties and Mirror Symmetry (Toronto, ON, 2001), pp. 223-231, Fields Inst. Commun., 38, Amer. Math. Soc., Providence, RI, 2003.

[St] R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge Univ. Press, Cambridge, 1999.

[Su] Z. H. Sun, *Congruences concerning Legendre polynomials*, Proc. Amer. Math. Soc. 139 (2011), 1915–1929.

[S1] Z. W. Sun, *Combinatorial identities in dual sequences*, European J. Combin. 24 (2003), 709–718.

[S2] Z. W. Sun, *Binomial coefficients, Catalan numbers and Lucas quotients*, Sci. China Math. 53 (2010), 2473–2488.

[S3] Z. W. Sun, *On congruences related to central binomial coefficients*, J. Number Theory 131 (2011), 2219–2238.

[S4] Z. W. Sun, *Super congruences and Euler numbers*, Sci. China Math. 54 (2011), in press.

[S5] Z. W. Sun, *On sums involving products of three binomial coefficients*, preprint, arXiv:1012.3141. http://arxiv.org/abs/1012.3141.

[ST] Z. W. Sun and R. Tauraso, *New congruences for central binomial coefficients*, Adv. in Appl. Math. 45 (2010), 125–148.