Int. J. Number Theory 12(2016), no.1, 143-164.

Cubic congruences and sums involving $\binom{3k}{k}$

Zhi-Hong Sun

School of Mathematical Sciences
Huaiyin Normal University
Huaian, Jiangsu 223001, P.R. China
zhihongsun@yahoo.com
http://www.hytc.edu.cn/xsjl/szh

Let p be a prime greater than 3 and let a be a rational p-adic integer. In this paper we try to determine $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k \pmod p$, and reveal the connection between cubic congruences and the sum $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k$, where $[x]$ is the greatest integer not exceeding x. Suppose that a_1,a_2,a_3 are rational p-adic integers, $P=-2a_1^3+9a_1a_2-27a_3$, $Q=(a_1^2-3a_2)^3$ and $PQ(P^2-Q)(P^2-3Q)(P^2-4Q)\not\equiv 0 \pmod p$. In this paper we show that the number of solutions of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$ depends only on $\sum_{k=1}^{[p/3]}\binom{3k}{k}(\frac{4Q-P^2}{27Q})^k \pmod p$. Let q be a prime of the form $3k+1$ and so $4q=L^2+27M^2$ with $L,M\in\mathbb{Z}$. When $p\neq q$ and $p\nmid LM$, we establish congruences for $\sum_{k=1}^{[p/3]}\binom{3k}{k}(\frac{M^2}{q})^k$ and $\sum_{k=1}^{[p/3]}\binom{3k}{k}(\frac{L^2}{27q})^k$ modulo p. As a consequence, when $q\not\equiv 9M^2, 27M^2 \pmod p$ we show that $x^3-qx-qM\equiv 0 \pmod p$ has three solutions if and only if p is a cubic residue of q.

Keywords: congruence; Lucas sequence; cubic residue; binary quadratic forms.

Mathematics Subject Classification 2010: Primary 11A07; Secondary 11A15,11B39,11B65,11E25

1. Introduction

Congruences involving binomial coefficients are interesting, and they are concerned with Fermat quotients, Lucas sequences, Legendre polynomials, binary quadratic forms and cubic congruences. Let $\mathbb{Z}$ be the set of integers, and for a prime p let $\mathbb{Z}_p$ denote the set of those rational numbers whose denominator is not divisible by p. Let $p>5$ be a prime. In [12] Zhao, Pan and Sun proved that

$$\sum_{k=1}^{p-1}\binom{3k}{k}2^k\equiv\frac{6}{5}((-1)^{(p-1)/2}-1) \pmod p.$$

In [10] the author's brother Z.W. Sun investigated $\sum_{k=0}^{p-1}\binom{3k}{k}a^k \pmod p$ for $a\in\mathbb{Z}_p$. He gave explicit congruences for $a=-4,\frac{1}{6},\frac{1}{7},\frac{1}{8},\frac{1}{9},\frac{1}{13},\frac{3}{8},\frac{4}{27}$.

Suppose that $p>3$ is a prime and $k\in\{1,2,\ldots,p-1\}$. It is easy to see that $p\mid\binom{3k}{k}$ if and only if $\frac{p}{3}<k<\frac{p}{2}$ or $\frac{2p}{3}<k<p$. Thus, for any $a\in\mathbb{Z}_p$,

$$\sum_{k=1}^{p-1}\binom{3k}{k}a^k\equiv\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k+\sum_{k=(p+1)/2}^{[2p/3]}\binom{3k}{k}a^k\pmod p,$$

where $[x]$ is the greatest integer not exceeding x. In [9] the author investigated congruences for $\sum_{k=0}^{[p/3]}\binom{3k}{k}a^k$ modulo p. In this paper we reveal the connection between cubic congruences and the sum $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k$. Let p be an odd prime. For $m\in\mathbb{Z}$ let $(\frac{m}{p})$ be the Legendre symbol. For $m,n\in\mathbb{Z}$ with $p\nmid n$ define $(\frac{m/n}{p})=(\frac{x}{p})$, where $x\in\mathbb{Z}$ satisfies the congruence $nx\equiv m\pmod p$. Then $(\frac{m/n}{p})=(\frac{mn/n^2}{p})=(\frac{mn}{p})$. For $p>3$ and $a_0,a_1,a_2,a_3\in\mathbb{Z}_p$ with $a_0\not\equiv0\pmod p$ let $N_p(a_0x^3+a_1x^2+a_2x+a_3)$ denote the number of solutions of the cubic congruence $a_0x^3+a_1x^2+a_2x+a_3\equiv0\pmod p$. It is well known (see for example [2,4,5] and [7, Lemma 2.3]) that

$$N_p(x^3+a_1x^2+a_2x+a_3)=1\iff\Big(\frac{D}{p}\Big)=-1,\tag{1.1}$$

where D is the discriminant of $x^3+a_1x^2+a_2x+a_3$ given by

$$D=a_1^2a_2^2-4a_2^3-4a_1^3a_3-27a_3^2+18a_1a_2a_3.\tag{1.2}$$

In this paper we establish many congruences for $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k\pmod p$. Here are some typical results:

⋆ Let $p>3$ be a prime and $a_1,a_2,a_3\in\mathbb{Z}_p$. Suppose $P=-2a_1^3+9a_1a_2-27a_3$, $Q=(a_1^2-3a_2)^3$ and $PQ(P^2-Q)(P^2-3Q)(P^2-4Q)\not\equiv0\pmod p$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=3$ if and only if $\sum_{k=1}^{[p/3]}\binom{3k}{k}\big(\frac{4Q-P^2}{27Q}\big)^k\equiv0\pmod p$.

⋆ Let $p>3$ be a prime, $n\in\mathbb{Z}_p$ and $3n+2\not\equiv0\pmod p$. Then

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}(n^2(n+1))^k\equiv\frac{3(n+1)}{2(3n+2)}\Big(\Big(\frac{(1+n)(1-3n)}{p}\Big)-1\Big)\pmod p.$$

⋆ Let p be a prime of the form $3k+1$, $m\in\mathbb{Z}_p$ and $m\not\equiv1,-2,-\frac12\pmod p$. Then

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}$$
$$\equiv\begin{cases}0\pmod p & \text{if }\big(\frac{m-1}{m+2}\big)^{\frac{p-1}{3}}\equiv1\pmod p,\\ -\dfrac{3}{2m+1}\big(m+1+\big(\frac{m-1}{m+2}\big)^{\frac{p-1}{3}}\big)\pmod p & \text{if }\big(\frac{m-1}{m+2}\big)^{\frac{p-1}{3}}\not\equiv1\pmod p.\end{cases}$$

⋆ Let q be a prime of the form $3m+1$ and so $4q=L^2+27M^2$ with $L,M\in\mathbb{Z}$ and $L\equiv1\pmod3$. Let p be a prime with $p\neq2,3,q$ and $p\nmid L$. Then

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{M^{2k}}{q^k}\equiv\begin{cases}0\pmod p & \text{if }p^{\frac{q-1}{3}}\equiv1\pmod q,\\ \dfrac{-3\mp9M/L}{2}\pmod p & \text{if }p^{\frac{q-1}{3}}\equiv\frac{-1\pm9M/L}{2}\pmod q.\end{cases}$$

Let $\omega=\frac{-1+\sqrt{-3}}{2}$. For a prime $p>3$ and $a,b\in\mathbb{Z}_p$ let $\left(\frac{a+b\omega}{p}\right)_3$ be the cubic Jacobi symbol defined in [6]. For $c\in\mathbb{Z}_p$ with $c^2+3\not\equiv 0\pmod p$ and $r\in\{0,1,2\}$ following [6] we define $c\in C_r(p)$ if and only if $\left(\frac{c+1+2\omega}{p}\right)_3=\omega^r$. According to [6], $C_r(p)$ $(r=0,1,2)$ play a central role in the theory of cubic residues and nonresidues. In this paper, using the sum $\sum_{k=1}^{[p/3]}\binom{3k}{k}\left(\frac{4}{9(c^2+3)}\right)^k$ we give a simple criterion for $c\in C_r(p)$. In particular, for $c\not\equiv 0,\pm1\pmod p$, $c\in C_0(p)$ if and only if $\sum_{k=1}^{[p/3]}\binom{3k}{k}\left(\frac{4}{9(c^2+3)}\right)^k\equiv 0\pmod p$.

For $a,b,c\in\mathbb{Z}$ and a prime p, if there are integers x and y such that $p=ax^2+bxy+cy^2$, throughout this paper we briefly write that $p=ax^2+bxy+cy^2$.

2. Main results

For any numbers P and Q, let $\{U_n(P,Q)\}$ be the Lucas sequence given by

$$U_0(P,Q)=0,\ U_1(P,Q)=1,\ U_{n+1}(P,Q)=PU_n(P,Q)-QU_{n-1}(P,Q)\ (n\ge 1).$$

It is well known (see [11]) that

$$U_n(P,Q)=\begin{cases}\dfrac{1}{\sqrt{P^2-4Q}}\left\{\left(\dfrac{P+\sqrt{P^2-4Q}}{2}\right)^n-\left(\dfrac{P-\sqrt{P^2-4Q}}{2}\right)^n\right\} & \text{if } P^2-4Q\ne 0,\\ n\left(\dfrac{P}{2}\right)^{n-1} & \text{if } P^2-4Q=0.\end{cases}\tag{2.1}$$

Let $U_n=U_n(P,Q)$. Using (2.1) we see that (see [11, (4.2.24) and (4.2.26)]) for any positive integer n,

$$U_{n+1}U_{n-1}-U_n^2=-Q^{n-1}\quad\text{and}\quad U_{2n+1}=U_{n+1}^2-QU_n^2.\tag{2.2}$$

Lemma 2.1 ([9, Lemma 3.3]). *Let $p>3$ be a prime, $P,Q\in\mathbb{Z}_p$ and $PQ(P^2-4Q)\not\equiv 0\pmod p$. Then*

$$U_{2[\frac{p}{3}]+1}(P,Q)\equiv\begin{cases}-Q^{1-\frac{p-(\frac{p}{3})}{3}}U_{\frac{p-(\frac{p}{3})}{3}-1}(P,Q)\pmod p & \text{if } \left(\dfrac{P^2-4Q}{p}\right)=1,\\ -Q^{-\frac{p-(\frac{p}{3})}{3}}U_{\frac{p-(\frac{p}{3})}{3}+1}(P,Q)\pmod p & \text{if } \left(\dfrac{P^2-4Q}{p}\right)=-1.\end{cases}$$

Lemma 2.2. *Let $p>3$ be a prime and $P,Q\in\mathbb{Z}_p$ with $PQ\not\equiv 0\pmod p$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(P,Q)\equiv 0\pmod p\quad\textit{implies}\quad U_{2[\frac{p}{3}]+1}(P,Q)\equiv(-Q)^{[\frac{p}{3}]}\pmod p.$$

Moreover, if $P^2-3Q\not\equiv 0\pmod p$, then

$$U_{2[\frac{p}{3}]+1}(P,Q)\equiv(-Q)^{[\frac{p}{3}]}\pmod p\quad\textit{implies}\quad U_{\frac{p-(\frac{p}{3})}{3}}(P,Q)\equiv 0\pmod p.$$

Proof. Set $U_m=U_m(P,Q)$ and $n=(p-(\frac{p}{3}))/3$. Then $2[\frac{p}{3}]+1=p-n$. We first assume $U_n\equiv 0\pmod p$. If $p\equiv 1\pmod 3$, by (2.2) we have $U_{n+1}(PU_n-U_{n+1})/Q-U_n^2=-Q^{n-1}$

and so $U_{n+1}^2 \equiv Q^n \pmod p$. Hence $U_{2n+1} = U_{n+1}^2 - QU_n^2 \equiv Q^n = (-Q)^n \pmod p$. If $p \equiv 2 \pmod 3$, by (2.2) we have $(PU_n - QU_{n-1})U_{n-1} - U_n^2 = -Q^{n-1}$ and so $U_{n-1}^2 \equiv Q^{n-2} \pmod p$. Thus, $U_{2[\frac{p}{3}]+1} = U_{2n-1} = U_n^2 - QU_{n-1}^2 \equiv -Q \cdot Q^{n-2} = (-Q)^{[\frac{p}{3}]} \pmod p$.

Now we assume that $P^2 - 3Q \not\equiv 0 \pmod p$ and $U_{2[\frac{p}{3}]+1}(P,Q) \equiv (-Q)^{[\frac{p}{3}]} \pmod p$. We claim that $P^2 - 4Q \not\equiv 0 \pmod p$. If $P^2 - 4Q \equiv 0 \pmod p$, by (2.1) we have

$$\begin{aligned} U_{2[\frac{p}{3}]+1} &\equiv U_{2[\frac{p}{3}]+1}(P, P^2/4) = \Big(2\big[\frac{p}{3}\big] + 1\Big)\Big(\frac{P}{2}\Big)^{2[\frac{p}{3}]} \\ &\equiv \Big(2\big[\frac{p}{3}\big] + 1\Big)Q^{[\frac{p}{3}]} \equiv \frac{1}{3}(-Q)^{[\frac{p}{3}]} \not\equiv (-Q)^{[\frac{p}{3}]} \pmod p, \end{aligned}$$

which contradicts the assumption. Hence $P^2 - 4Q \not\equiv 0 \pmod p$. Suppose $p \equiv 1 \pmod 3$. By Lemma 2.1 we have

$$\begin{aligned} &U_{n-1} \equiv -Q^{2n-1} \pmod p \quad \text{for} \quad \big(\frac{P^2-4Q}{p}\big) = 1, \\ &U_{n+1} \equiv -Q^{2n} \pmod p \quad \text{for} \quad \big(\frac{P^2-4Q}{p}\big) = -1. \end{aligned} \tag{2.3}$$

When $(\frac{P^2-4Q}{p}) = -1$ we have

$$Q^n \equiv U_{2n+1} = U_{n+1}^2 - QU_n^2 \equiv Q^{4n} - QU_n^2 \pmod p.$$

As $Q^{3n} = Q^{p-1} \equiv 1 \pmod p$ we have $Q^{4n} \equiv Q^n \pmod p$. Thus $QU_n^2 \equiv 0 \pmod p$ and so $U_n \equiv 0 \pmod p$. When $(\frac{P^2-4Q}{p}) = 1$ we have

$$\begin{aligned} Q^n &\equiv U_{2n+1} = U_{n+1}^2 - QU_n^2 = (PU_n - QU_{n-1})^2 - QU_n^2 \\ &\equiv (PU_n + Q^{2n})^2 - QU_n^2 = U_n((P^2 - Q)U_n + 2PQ^{2n}) + Q^{4n} \pmod p. \end{aligned}$$

As $Q^{4n} \equiv Q^n \pmod p$ we have

$$U_n((P^2 - Q)U_n + 2PQ^{2n}) \equiv 0 \pmod p.$$

If $P^2 \equiv Q \pmod p$, as $p \nmid PQ$ we have $U_n \equiv 0 \pmod p$. Now assume $P^2 - Q \not\equiv 0 \pmod p$. If $U_n \equiv -\frac{2PQ^{2n}}{P^2-Q} \pmod p$, then

$$U_{n+1} = PU_n - QU_{n-1} \equiv -\frac{2P^2Q^{2n}}{P^2 - Q} + Q^{2n} = \frac{Q + P^2}{Q - P^2}Q^{2n} \pmod p.$$

Hence

$$\begin{aligned} -Q^{n-1} = U_{n+1}U_{n-1} - U_n^2 &\equiv \frac{Q + P^2}{Q - P^2}Q^{2n}(-Q^{2n-1}) - \frac{4P^2Q^{4n}}{(P^2 - Q)^2} \\ &= \frac{Q^{4n-1}}{(P^2 - Q)^2}(P^4 - Q^2 - 4P^2Q) \pmod p. \end{aligned}$$

As $Q^{4n-1} \equiv Q^{n-1} \pmod p$ we must have

$$P^4 - Q^2 - 4P^2Q \equiv -(P^2 - Q)^2 \pmod p.$$

That is, $2P^2(P^2 - 3Q) \equiv 0 \pmod p$. This contradicts the assumption. Thus, $(P^2 - Q)U_n + 2PQ^{2n} \not\equiv 0 \pmod p$ and so $U_n \equiv 0 \pmod p$.

Now we assume $p \equiv 2 \pmod 3$. As $U_{2n-1} = U_{2[\frac{p}{3}]+1} \equiv (-Q)^{[\frac{p}{3}]} = -Q^{n-1} \pmod p$, by Lemma 2.1 we have

$$\begin{aligned} &U_{n-1} \equiv Q^{2n-2} \pmod p \quad \text{for} \quad \big(\frac{P^2 - 4Q}{p}\big) = 1, \\ &U_{n+1} \equiv Q^{2n-1} \pmod p \quad \text{for} \quad \big(\frac{P^2 - 4Q}{p}\big) = -1. \end{aligned} \tag{2.4}$$

When $(\frac{P^2-4Q}{p}) = 1$ we have

$$-Q^{n-1} \equiv U_{2n-1} = U_n^2 - QU_{n-1}^2 \equiv U_n^2 - Q^{4n-3} \pmod p.$$

As $Q^{4n-3-(n-1)} = Q^{3n-2} = Q^{p-1} \equiv 1 \pmod p$ we have $Q^{4n-3} \equiv Q^{n-1} \pmod p$. Thus $U_n^2 \equiv 0 \pmod p$ and so $U_n \equiv 0 \pmod p$. When $(\frac{P^2-4Q}{p}) = -1$ we have

$$\begin{aligned} -Q^{n-1} \equiv U_{2n-1} = U_n^2 - QU_{n-1}^2 &= U_n^2 - Q\Big(\frac{PU_n - U_{n+1}}{Q}\Big)^2 \equiv U_n^2 - \frac{(PU_n - Q^{2n-1})^2}{Q} \\ &= -\frac{U_n((P^2 - Q)U_n - 2PQ^{2n-1})}{Q} - Q^{4n-3} \pmod p. \end{aligned}$$

As $Q^{4n-3} \equiv Q^{n-1} \pmod p$ we have

$$U_n((P^2 - Q)U_n - 2PQ^{2n-1}) \equiv 0 \pmod p.$$

If $P^2 - Q \equiv 0 \pmod p$, as $p \nmid PQ$ we have $U_n \equiv 0 \pmod p$. Now assume $P^2 - Q \not\equiv 0 \pmod p$. If $U_n \equiv \frac{2PQ^{2n-1}}{P^2-Q} \pmod p$, then

$$U_{n-1} = \frac{PU_n - U_{n+1}}{Q} \equiv \frac{P}{Q} \cdot \frac{2PQ^{2n-1}}{P^2 - Q} - Q^{2n-2} = Q^{2n-2}\frac{2P^2 - (P^2 - Q)}{P^2 - Q} \pmod p.$$

Hence

$$\begin{aligned} -Q^{n-1} = U_{n+1}U_{n-1} - U_n^2 &\equiv Q^{4n-3}\Big(\frac{2P^2 - (P^2 - Q)}{P^2 - Q} - \frac{4P^2Q}{(P^2 - Q)^2}\Big) \\ &\equiv \frac{Q^{n-1}}{(P^2 - Q)^2}(-(P^2 - Q)^2 + 2P^2(P^2 - 3Q)) \pmod p. \end{aligned}$$

This yields $2P^2(P^2 - 3Q) \equiv 0 \pmod p$, which contradicts the assumption. Thus, $(P^2 - Q)U_n - 2PQ^{2n-1} \not\equiv 0 \pmod p$ and so $U_n \equiv 0 \pmod p$.

Summarizing all the above we prove the lemma.

Lemma 2.3 ([9, (3.1)]. *Let $p>3$ be a prime and $P,Q\in\mathbb{Z}_p$ with $PQ\not\equiv 0 \pmod p$. Then*

$$U_{2[\frac{p}{3}]+1}(P,Q)\equiv(-Q)^{[\frac{p}{3}]}\sum_{k=0}^{[p/3]}\binom{3k}{k}\Big(\frac{P^2}{27Q}\Big)^k \pmod p.$$

From (2.1) we know that for odd m,

$$\begin{aligned}U_m(1,\frac{1}{3})&=\sqrt{-3}\Big\{\Big(\frac{1+\frac{1}{\sqrt{-3}}}{2}\Big)^m-\Big(\frac{1-\frac{1}{\sqrt{-3}}}{2}\Big)^m\Big\}\\&=(-3)^{-\frac{m-1}{2}}((-\omega^2)^m-\omega^m)=\begin{cases}-2\cdot(-3)^{-\frac{m-1}{2}} & \text{if } 3\mid m,\\ (-3)^{-\frac{m-1}{2}} & \text{if } 3\nmid m.\end{cases}\end{aligned}$$

Thus, putting $P=1$ and $Q=\frac{1}{3}$ in Lemma 2.3 we see that

$$\frac{1}{(-3)^{[\frac{p}{3}]}}\sum_{k=0}^{[p/3]}\binom{3k}{k}\frac{1}{9^k}\equiv U_{2[\frac{p}{3}]+1}(1,\frac{1}{3})\equiv\begin{cases}-2(-3)^{-[\frac{p}{3}]} \pmod p & \text{if } p\equiv\pm4 \pmod 9,\\ (-3)^{-[\frac{p}{3}]} \pmod p & \text{if } p\not\equiv\pm4 \pmod 9.\end{cases}$$

Hence,

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{9^k}\equiv\begin{cases}-3 \pmod p & \text{if } p\equiv\pm4 \pmod 9,\\ 0 \pmod p & \text{if } p\not\equiv\pm4 \pmod 9.\end{cases}\tag{2.5}$$

Lemma 2.4. *Let $p>3$ be a prime and $P,Q\in\mathbb{Z}_p$ with $PQ(P^2-3Q)(P^2-4Q)\not\equiv 0 \pmod p$. Then the following statements are equivalent:*

(i) $U_{(p-(\frac{p}{3}))/3}(P,Q)\equiv 0 \pmod p$.

(ii) $\sum_{k=1}^{[p/3]}\binom{3k}{k}\big(\frac{P^2}{27Q}\big)^k\equiv 0 \pmod p$.

(iii) *The congruence $x^3-3Qx-PQ\equiv 0 \pmod p$ has three solutions.*

Proof. By Lemmas 2.2 and 2.3,

$$\begin{aligned}U_{\frac{p-(\frac{p}{3})}{3}}(P,Q)\equiv 0 \pmod p &\iff U_{2[\frac{p}{3}]+1}(P,Q)\equiv(-Q)^{[\frac{p}{3}]} \pmod p\\&\iff\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{P^2}{27Q}\Big)^k\equiv 0 \pmod p.\end{aligned}$$

Thus (i) is equivalent to (ii). By [8, (7.4)] or [6, Corollary 6.3], (i) is equivalent to (iii).

Theorem 2.1. *Let $p>3$ be a prime and $a\in\mathbb{Z}_p$ with $a\not\equiv 0,\frac{1}{9},\frac{1}{27},\frac{4}{27} \pmod p$. Then the following statements are equivalent:*

(i) $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k\equiv 0 \pmod p$,

(ii) $U_{(p-(\frac{p}{3}))/3}(9a,3a)\equiv 0 \pmod p$,

(iii) $\big(\frac{27a-2+3\sqrt{81a^2-12a}}{2}\big)^{(p-(\frac{p}{3}))/3}\equiv 1 \pmod p$,

(iv) $ax^3-x-1\equiv 0 \pmod p$ *has three solutions,*

(v) $\sum_{k=1}^{[p/3]}\binom{3k}{k}\big(\frac{4-27a}{27}\big)^k\equiv 0 \pmod p$,

(vi) $(27a-4)x^3+3x+1\equiv 0 \pmod p$ *has three solutions.*

Proof. Taking $P=9a$ and $Q=3a$ in Lemma 2.4 we see that (i) and (ii) are equivalent. By (2.1),

$$U_{\frac{p-(\frac{p}{3})}{3}}(9a,3a)\equiv 0 \pmod p \iff \Big(\frac{9a+\sqrt{(9a)^2-4\cdot 3a}}{9a-\sqrt{(9a)^2-4\cdot 3a}}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1 \pmod p.$$

As

$$\frac{9a+\sqrt{81a^2-12a}}{9a-\sqrt{81a^2-12a}}=\frac{(9a+\sqrt{81a^2-12a})^2}{12a}=\frac{27a-2+3\sqrt{81a^2-12a}}{2},$$

we see that (ii) is equivalent to (iii). For $x=3ay$ we see that

$$x^3-3\cdot 3ax-9a\cdot 3a=(3ay)^3-9a\cdot 3ay-27a^2=27a^2(ay^3-y-1).$$

Thus, $x^3-3\cdot 3ax-9a\cdot 3a\equiv 0 \pmod p$ has three solutions if and only if $ay^3-y-1\equiv 0 \pmod p$ has three solutions. Hence applying Lemma 2.4 we see that (ii) is equivalent to (iv). It is clear that

$$\begin{aligned}&\frac{27(\frac{4}{27}-a)-2+3\sqrt{81(\frac{4}{27}-a)^2-12(\frac{4}{27}-a)}}{2}\cdot\frac{27a-2+3\sqrt{81a^2-12a}}{2}\\&=\frac{2-27a+3\sqrt{81a^2-12a}}{2}\cdot\frac{27a-2+3\sqrt{81a^2-12a}}{2}=-1.\end{aligned}$$

Thus,

$$\begin{aligned}&\Big(\frac{27(\frac{4}{27}-a)-2+3\sqrt{81(\frac{4}{27}-a)^2-12(\frac{4}{27}-a)}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1 \pmod p\\&\iff \Big(\frac{27a-2+3\sqrt{81a^2-12a}}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}}\equiv 1 \pmod p.\end{aligned}$$

Since $\frac{4}{27}-a\not\equiv 0,\frac{1}{9},\frac{4}{27} \pmod p$ and (iii) is equivalent to (i) and (iv), using the above we see that (iii) is equivalent to (v) and that

$$\begin{aligned}&ax^3-x-1\equiv 0 \pmod p \quad \text{has three solutions}\\&\iff (\frac{4}{27}-a)x^3-x-1\equiv 0 \pmod p \quad \text{has three solutions}\\&\iff (\frac{4}{27}-a)(3x)^3-3x-1\equiv 0 \pmod p \quad \text{has three solutions}\\&\iff (27a-4)x^3+3x+1\equiv 0 \pmod p \quad \text{has three solutions.}\end{aligned}$$

Thus (iv) and (vi) are equivalent. Now the proof is complete.

Lemma 2.5. *Let $p>3$ be a prime and $a\in\mathbb{Z}_p$ with $a(27a-4)\not\equiv 0 \pmod p$. Then the cubic congruence $(27a-4)x^3+3x+1\equiv 0 \pmod p$ has one and only one solution if and only if $x\equiv\sum_{k=0}^{[p/3]}\binom{3k}{k}a^k \pmod p$ is a solution of the congruence.*

Proof. As $27a-4 \not\equiv 0 \pmod p$ and $(27a-4)^2((27a-4)x^3+3x+1) = ((27a-4)x)^3 + 3(27a-4)\cdot(27a-4)x + (27a-4)^2$, we see that

$$N_p((27a-4)x^3+3x+1) = N_p(x^3+3(27a-4)x+(27a-4)^2).$$

By (1.2), the discriminant of $x^3+3(27a-4)x+(27a-4)^2$ is $27^2a(4-27a)^3$. If $N_p((27a-4)x^3+3x+1)=1$, by (1.1) and the above we must have $(\frac{a(4-27a)}{p})=-1$. Now applying [9, Theorem 3.10] we see that the unique solution of $(27a-4)x^3+3x+1\equiv 0 \pmod p$ is given by $x\equiv\sum_{k=0}^{[p/3]}\binom{3k}{k}a^k \pmod p$. Conversely, suppose that $x\equiv\sum_{k=0}^{[p/3]}\binom{3k}{k}a^k \pmod p$ is a solution of the congruence $(27a-4)x^3+3x+1\equiv 0 \pmod p$. By (2.5) and [9, Theorem 3.2] we have $a\not\equiv\frac{1}{9},\frac{1}{27} \pmod p$. If $N_p((27a-4)x^3+3x+1)=3$, by Theorem 2.1 we have $\sum_{k=0}^{[p/3]}\binom{3k}{k}a^k\equiv 1 \pmod p$. But $x\equiv 1 \pmod p$ is not a solution of the congruence $(27a-4)x^3+3x+1\equiv 0 \pmod p$. This contradicts the assumption. Hence $N_p((27a-4)x^3+3x+1)=1$. This proves the lemma.

Remark 2.1 Let $p>3$ be a prime, $a\in\mathbb{Z}_p$ and $(\frac{a(4-27a)}{p})=-1$. By [9, Theorem 3.10], $x\equiv\sum_{k=0}^{[p/3]}\binom{3k}{k}a^k \pmod p$ is the unique solution of the congruence $(27a-4)x^3+3x+1\equiv 0 \pmod p$. Hence $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k\not\equiv 0 \pmod p$.

Theorem 2.2. *Let $p>3$ be a prime and $a_1,a_2,a_3\in\mathbb{Z}_p$. Suppose $P=-2a_1^3+9a_1a_2-27a_3$, $Q=(a_1^2-3a_2)^3$ and $PQ(P^2-4Q)\not\equiv 0 \pmod p$. Then $N_p(x^3+a_1x^2+a_2x+a_3)=1$ if and only if*

$$x\equiv\frac{P}{3(a_1^2-3a_2)}\sum_{k=0}^{[p/3]}\binom{3k}{k}\Big(\frac{4Q-P^2}{27Q}\Big)^k-\frac{a_1}{3} \pmod p$$

is a solution of the congruence $x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p$. If $P^2\not\equiv Q, 3Q \pmod p$, then $N_p(x^3+a_1x^2+a_2x+a_3)=3$ if and only if $\sum_{k=1}^{[p/3]}\binom{3k}{k}\big(\frac{4Q-P^2}{27Q}\big)^k\equiv 0 \pmod p$.

Proof. Set $x=\frac{P}{3(a_1^2-3a_2)}y-\frac{a_1}{3}$. Then $x^3+a_1x^2+a_2x+a_3=-\frac{P}{27}(-\frac{P^2}{Q}y^3+3y+1)$. Thus,

$$\begin{aligned}&N_p(x^3+a_1x^2+a_2x+a_3)\\&=N_p\Big(-\frac{P^2}{Q}x^3+3x+1\Big)=N_p\Big(\Big(27\cdot\frac{4Q-P^2}{27Q}-4\Big)x^3+3x+1\Big).\end{aligned}$$

From the above and Lemma 2.5 we see that

$$\begin{aligned}&N_p(x^3+a_1x^2+a_2x+a_3)=1\\&\iff N_p\Big(-\frac{P^2}{Q}y^3+3y+1\Big)=1\\&\iff y\equiv\sum_{k=0}^{[p/3]}\binom{3k}{k}\Big(\frac{4Q-P^2}{27Q}\Big)^k \pmod p \text{ satisfying } -\frac{P^2}{Q}y^3+3y+1\equiv 0 \pmod p\\&\iff x\equiv\frac{P}{3(a_1^2-3a_2)}\sum_{k=0}^{[p/3]}\binom{3k}{k}\Big(\frac{4Q-P^2}{27Q}\Big)^k-\frac{a_1}{3} \pmod p\\&\qquad\text{satisfying}\quad x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p.\end{aligned}$$

If $P^2 \not\equiv Q, 3Q \pmod p$, from the above and Theorem 2.1 we see that

$$\begin{aligned} & x^3+a_1x^2+a_2x+a_3\equiv 0 \pmod p \quad \text{has three solutions} \\ \iff & \Big(27\cdot\frac{4Q-P^2}{27Q}-4\Big)x^3+3x+1\equiv 0 \pmod p \quad \text{has three solutions} \\ \iff & \sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{4Q-P^2}{27Q}\Big)^k\equiv 0 \pmod p. \end{aligned}$$

This completes the proof.

Corollary 2.1. *Let $p>3$ be a prime.*

(i) *If $p\neq 11$, then $\sum_{k=1}^{[p/3]}\binom{3k}{k}(-\frac{32}{9})^k\equiv 0 \pmod p$ if and only if $p=x^2+162y^2$ or $p=2x^2+81y^2$.*

(ii) $\sum_{k=1}^{[p/3]}\binom{3k}{k}(\frac{68}{27})^k\equiv 0 \pmod p$ *if and only if $p=x^2+xy+115y^2$ or $p=11x^2+5xy+11y^2$.*

(iii) *If $p\neq 5, 241$, then $\sum_{k=1}^{[p/3]}\binom{3k}{k}(\frac{4100}{27})^k\equiv 0 \pmod p$ if and only if $p=x^2+xy+277y^2$ or $p=17x^2+7xy+17y^2$.*

Proof. By [8, Corollary 7.4(i)], $N_p(x^3-3x-10)=3$ if and only if $p=x^2+162y^2$ or $2x^2+81y^2$. By Theorem 2.2, for $p\neq 5, 11, 97$, $N_p(x^3-3x-10)=3$ if and only if $\sum_{k=1}^{[p/3]}\binom{3k}{k}(-\frac{32}{9})^k\equiv 0 \pmod p$. Thus (i) holds for $p\neq 5, 11, 97$. For $p=5, 97$ using Maple we see that (i) is also true. In the same way, from Theorem 2.2 and [8, Corollary 7.4] we deduce (ii) and (iii).

Theorem 2.3. *Let $p>3$ be a prime, $n\in\mathbb{Z}_p$ and $3n+2\not\equiv 0 \pmod p$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}(n^2(n+1))^k\equiv\frac{3(n+1)}{2(3n+2)}\Big(\Big(\frac{(1+n)(1-3n)}{p}\Big)-1\Big) \pmod p.$$

Proof. Clearly the result is true for $n\equiv 0, -1 \pmod p$. Now assume $n(n+1)\not\equiv 0 \pmod p$. If $3n-1\equiv 0 \pmod p$, by Lemma 2.3 we have

$$\begin{aligned} \sum_{k=1}^{[p/3]}\binom{3k}{k}(n^2(n+1))^k &\equiv \sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{4}{27}\Big)^k\equiv(-1)^{[\frac{p}{3}]}U_{2[\frac{p}{3}]+1}(2,1)-1 \\ &=(-1)^{[\frac{p}{3}]}\Big(2\big[\frac{p}{3}\big]+1\Big)-1\equiv-\frac{2}{3}\equiv-\frac{3(n+1)}{2(3n+2)} \pmod p. \end{aligned}$$

Thus the result is true for $n\equiv\frac{1}{3} \pmod p$. From now on we assume $3n-1\not\equiv 0 \pmod p$. It is clear that $27n^2(n+1)-4=(3n+2)^2(3n-1)$. Set $a=n^2(n+1)$. Then $a(27a-4)\not\equiv 0 \pmod p$. By [8, (7.4)],

$$\begin{aligned} & U_{\frac{p-(\frac{p}{3})}{3}}(9a,3a)\equiv 0 \pmod p \\ \iff & x^3-9ax-27a^2\equiv 0 \pmod p \quad \text{has three solutions} \\ \iff & (3ax)^3-9a\cdot 3ax-27a^2\equiv 0 \pmod p \quad \text{has three solutions} \\ \iff & ax^3-x-1\equiv 0 \pmod p \quad \text{has three solutions} \\ \iff & (n+1)(nx)^3-nx-n\equiv 0 \pmod p \quad \text{has three solutions} \end{aligned}$$

$$\begin{aligned}
&\iff (n+1)x^3-x-n\equiv 0 \pmod p \quad \text{has three solutions}\\
&\iff (x-1)((n+1)(x^2+x)+n)\equiv 0 \pmod p \quad \text{has three solutions}\\
&\iff (x-1)\Big(\big(x+\frac12\big)^2+\frac{3n-1}{4(n+1)}\Big)\equiv 0 \pmod p \quad \text{has three solutions}\\
&\iff \Big(\frac{(1+n)(1-3n)}{p}\Big)=1.
\end{aligned}$$

Hence, if $(\frac{(1+n)(1-3n)}{p})=1$, then $U_{(p-(\frac{p}{3}))/3}(9a,3a)\equiv 0 \pmod p$ and so $U_{2[\frac{p}{3}]+1}(9a,3a)\equiv(-3a)^{[p/3]} \pmod p$ by Lemma 2.2. Applying Lemma 2.3 (with $P=9a$ and $Q=3a$) we find that $\sum_{k=1}^{[p/3]}\binom{3k}{k}a^k\equiv 0 \pmod p$.

Now we assume $(\frac{(1+n)(1-3n)}{p})=-1$. As $3n\not\equiv 0,-2 \pmod p$ we see that $(\frac{a(4-27a)}{p})=(\frac{n^2(n+1)(3n+2)^2(1-3n)}{p})=(\frac{(1+n)(1-3n)}{p})=-1$. By [9, Theorem 3.10], $x\equiv\sum_{k=0}^{[p/3]}\binom{3k}{k}(n^2(n+1))^k \pmod p$ is the unique solution of the congruence $(3n+2)^2(3n-1)x^3+3x+1\equiv 0 \pmod p$. As

$$\begin{aligned}
&(3n+2)^2(3n-1)x^3+3x+1\\
&=(3n-1)\Big(x+\frac{1}{3n+2}\Big)\Big\{\big((3n+2)x-\frac12\big)^2-\frac{9(1+n)}{4(1-3n)}\Big\},
\end{aligned}$$

we see that $x\equiv-\frac{1}{3n+2} \pmod p$ is the unique solution of the congruence $(3n+2)^2(3n-1)x^3+3x+1\equiv 0 \pmod p$. Hence $\sum_{k=0}^{[p/3]}\binom{3k}{k}(n^2(n+1))^k\equiv-\frac{1}{3n+2} \pmod p$. This completes the proof.

Example 2.1 Taking $n=1,-\frac12$ in Theorem 2.3 we see that for any prime $p>5$,

$$\begin{aligned}
&\sum_{k=1}^{[p/3]}\binom{3k}{k}2^k\equiv\frac35\big((-1)^{\frac{p-1}{2}}-1\big) \pmod p,\\
&\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{8^k}\equiv\frac32\Big(\Big(\frac{5}{p}\Big)-1\Big) \pmod p.
\end{aligned}$$

Corollary 2.2. *Let $p>3$ be a prime, $m\in\mathbb{Z}_p$ and $m\not\equiv -3,9 \pmod p$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{4(m-1)^2}{(m+3)^3}\Big)^k\equiv\frac{6}{m-9}\Big(1-\Big(\frac{m}{p}\Big)\Big) \pmod p.$$

Proof. Set $n=\frac{1-m}{m+3}$. Then $n\not\equiv -1,-\frac23 \pmod p$, $m=\frac{1-3n}{1+n}$ and $n^2(n+1)=\frac{4(m-1)^2}{(m+3)^3}$. Now applying Theorem 2.3 we deduce the result.

Lemma 2.6 ([9, Theorem 3.3]). *Let $p>3$ be a prime, $a,b\in\mathbb{Z}_p$ and $ab(81b^2-12a)\not\equiv 0 \pmod p$. Then*

$$\sum_{k=0}^{[p/3]}\binom{3k}{k}\frac{b^{2k}}{a^k}\equiv\begin{cases}
(-3a)^{[\frac{p}{3}]+1}U_{\frac{p-(\frac{p}{3})}{3}-1}(9b,3a) \pmod p & \text{if } (\dfrac{81b^2-12a}{p})=1,\\
-(-3a)^{[\frac{p}{3}]}U_{\frac{p-(\frac{p}{3})}{3}+1}(9b,3a) \pmod p & \text{if } (\dfrac{81b^2-12a}{p})=-1.
\end{cases}$$

Theorem 2.4. *Let $p>3$ be a prime, $m\in\mathbb{Z}_p$ and $m\not\equiv 1,-2,-\frac12 \pmod p$.*
(i) *If $p\equiv 1 \pmod 3$, then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}$$
$$\equiv\begin{cases}0 \pmod p & \text{if } \left(\frac{m-1}{m+2}\right)^{\frac{p-1}{3}}\equiv 1 \pmod p,\\ -\dfrac{3}{2m+1}\left(m+1+\left(\dfrac{m-1}{m+2}\right)^{\frac{p-1}{3}}\right) \pmod p & \text{if } \left(\frac{m-1}{m+2}\right)^{\frac{p-1}{3}}\not\equiv 1 \pmod p.\end{cases}$$

(ii) *If $p\equiv 2 \pmod 3$, then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}$$
$$\equiv\frac{1}{2m+1}\Big\{(m-1)\Big(\frac{m-1}{m+2}\Big)^{\frac{p-2}{3}}+(m+2)\Big(\frac{m+2}{m-1}\Big)^{\frac{p-2}{3}}\Big\}-1 \pmod p.$$

Proof. As $81-12(-3(m-1)(m+2))=3^2(2m+1)^2$ and $2[\frac{p}{3}]+\frac{p-(\frac{p}{3})}{3}=p-1$, putting $a=-3(m-1)(m+2)$ and $b=1$ in Lemma 2.6 and then applying (2.1) we see that

$$\begin{aligned}&1+\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}\\ &\equiv(9(m-1)(m+2))^{[\frac{p}{3}]+1}U_{\frac{p-(\frac{p}{3})}{3}-1}(9,-9(m-1)(m+2))\\ &=\frac{(9(m-1)(m+2))^{[\frac{p}{3}]+1}}{3(2m+1)}\Big\{\Big(\frac{9+3(2m+1)}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}-1}-\Big(\frac{9-3(2m+1)}{2}\Big)^{\frac{p-(\frac{p}{3})}{3}-1}\Big\}\\ &\equiv\frac{((m-1)(m+2))^{[\frac{p}{3}]+1}}{2m+1}\Big\{(m+2)^{\frac{p-(\frac{p}{3})}{3}-1}+(m-1)^{\frac{p-(\frac{p}{3})}{3}-1}\Big\}\\ &\equiv\frac{1}{2m+1}\Big\{(m-1)\Big(\frac{m-1}{m+2}\Big)^{[\frac{p}{3}]}+(m+2)\Big(\frac{m+2}{m-1}\Big)^{[\frac{p}{3}]}\Big\} \pmod p.\end{aligned}$$

If $p\equiv 1 \pmod 3$ and $(\frac{m-1}{m+2})^{\frac{p-1}{3}}\equiv 1 \pmod p$, from the above we deduce that

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}\equiv\frac{1}{2m+1}(m-1+m+2)-1=0 \pmod p.$$

If $p\equiv 1 \pmod 3$ and $(\frac{m-1}{m+2})^{\frac{p-1}{3}}\not\equiv 1 \pmod p$, then $1+(\frac{m-1}{m+2})^{\frac{p-1}{3}}+(\frac{m-1}{m+2})^{-\frac{p-1}{3}}\equiv 0 \pmod p$. Thus, from the above we deduce that

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}$$
$$\equiv\frac{1}{2m+1}\Big(-(m+2)-3\Big(\frac{m-1}{m+2}\Big)^{\frac{p-1}{3}}\Big)-1$$

$$= -\frac{3}{2m+1}\Big(m+1+\Big(\frac{m-1}{m+2}\Big)^{\frac{p-1}{3}}\Big) \pmod p.$$

This completes the proof.

Corollary 2.3. *Let $p>3$ be a prime, $m\in\mathbb{Z}_p$ and $(2m+1)^2\not\equiv 0,-3,9,-27 \pmod p$. Then the congruence $x^3+3(m-1)(m+2)x+3(m-1)(m+2)\equiv 0 \pmod p$ has three solutions if and only if $p\equiv 1 \pmod 3$ and $(\frac{m-1}{m+2})^{\frac{p-1}{3}}\equiv 1 \pmod p$.*

Proof. Set $a=-\frac{1}{3(m-1)(m+2)}=-\frac{4}{3((2m+1)^2-9)}$. Then $a\not\equiv 0,\frac{1}{9},\frac{1}{27},\frac{4}{27} \pmod p$. By Theorem 2.1,

$$\begin{aligned}&\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(-3(m-1)(m+2))^k}\equiv 0 \pmod p\\ &\iff \frac{1}{-3(m-1)(m+2)}x^3-x-1\equiv 0 \pmod p \quad \text{has three solutions}\\ &\iff x^3+3(m-1)(m+2)x+3(m-1)(m+2)\equiv 0 \pmod p \quad \text{has three solutions.}\end{aligned}$$

If $p\equiv 1 \pmod 3$, $t^2\equiv -3 \pmod p$ $(t\in\mathbb{Z})$ and $(\frac{m-1}{m+2})^{\frac{p-1}{3}}\not\equiv 1 \pmod p$, then $(\frac{m-1}{m+2})^{\frac{p-1}{3}}\equiv\frac{-1\pm t}{2} \pmod p$. As $(2m+1)^2\not\equiv -3 \pmod p$ we have $2m+1\not\equiv\pm t \pmod p$ and so $m+1\not\equiv\frac{1\pm t}{2} \pmod p$. Thus $m+1+(\frac{m-1}{m+2})^{\frac{p-1}{3}}\not\equiv 0 \pmod p$. Hence applying Theorem 2.4(i) we deduce the result.

Now we assume $p\equiv 2 \pmod 3$. Clearly $m\not\equiv 1,-2 \pmod p$ and $\frac{m-1}{m+2}\not\equiv\pm 1 \pmod p$. Thus $(\frac{m-1}{m+2})^{p-2}\not\equiv 1 \pmod p$ and so $(\frac{m-1}{m+2})^{\frac{p-2}{3}}\not\equiv 1 \pmod p$. We also have $(\frac{m-1}{m+2})^{p+1}\not\equiv 1 \pmod p$ and so $(\frac{m-1}{m+2})^{\frac{p+1}{3}}\not\equiv 1 \pmod p$. Hence $(\frac{m-1}{m+2})^{\frac{p-2}{3}}\not\equiv\frac{m+2}{m-1} \pmod p$. Therefore

$$\begin{aligned}&(m-1)\Big(\frac{m-1}{m+2}\Big)^{\frac{p-2}{3}}+(m+2)\Big(\frac{m+2}{m-1}\Big)^{\frac{p-2}{3}}-(2m+1)\\ &=(m-1)\Big(1-\Big(\frac{m-1}{m+2}\Big)^{-\frac{p-2}{3}}\Big)\Big(\Big(\frac{m-1}{m+2}\Big)^{\frac{p-2}{3}}-\frac{m+2}{m-1}\Big)\not\equiv 0 \pmod p.\end{aligned}$$

Now combining the above with Theorem 2.4(ii) yields the result in the case $p\equiv 2 \pmod 3$. The proof is now complete.

Corollary 2.4. *Let $p>3$ be a prime. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{6^k}\equiv\begin{cases}0 \pmod p & \text{if } 3\mid p-1 \text{ and } 2^{\frac{p-1}{3}}\equiv 1 \pmod p,\\ 3\cdot 2^{\frac{p-1}{3}} \pmod p & \text{if } 3\mid p-1 \text{ and } 2^{\frac{p-1}{3}}\not\equiv 1 \pmod p,\\ 2^{\frac{2p-1}{3}}-2^{\frac{p+1}{3}}-1 \pmod p & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

Proof. Taking $m=-1$ in Theorem 2.4 we deduce the result.

Corollary 2.5. *Let $p>3$ be a prime, $c\in\mathbb{Z}_p$ and $c\not\equiv 0,1,-1 \pmod p$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{(c+1)^2}{27c}\Big)^k$$

$$\equiv \begin{cases} 0 \pmod p & \text{if } 3 \mid p-1 \text{ and } c^{\frac{p-1}{3}} \equiv 1 \pmod p, \\ \dfrac{1}{c-1}\big((c+1)c^{\frac{p-1}{3}} - (c-2)\big) \pmod p & \text{if } 3 \mid p-1 \text{ and } c^{\frac{p-1}{3}} \not\equiv 1 \pmod p, \\ \dfrac{1}{1-c} \cdot c^{\frac{p+1}{3}}(1 - c^{\frac{p-2}{3}}) - 1 \pmod p & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Proof. Taking $m = \frac{1-2c}{1+c}$ in Theorem 2.4 we derive the result.
For two numbers P and Q let $\{V_n(P,Q)\}$ be defined by

$$V_0(P,Q) = 2,\ V_1(P,Q) = P, \quad V_{n+1}(P,Q) = PV_n(P,Q) - QV_{n-1}(P,Q)\ (n \geq 1).$$

It is well known that

$$V_n(P,Q) = \Big(\frac{P + \sqrt{P^2-4Q}}{2}\Big)^n + \Big(\frac{P - \sqrt{P^2-4Q}}{2}\Big)^n.$$

From [11, (4.2.19)] we know that

$$V_n(P,Q) = PU_n(P,Q) - 2QU_{n-1}(P,Q) = 2U_{n+1}(P,Q) - PU_n(P,Q). \tag{2.6}$$

Lemma 2.7 ([6, Corollary 6.1]). *Let $p > 3$ be a prime, $c \in \mathbb{Z}_p$ and $c(c^2+3) \not\equiv 0 \pmod p$. Then*

$$U_{\frac{p-(\frac{p}{3})}{3}}(6, 3(c^2+3)) \equiv \begin{cases} 0 \pmod p & \text{if } c \in C_0(p), \\ \dfrac{1}{2c}(-3(c^2+3))^{-[\frac{p}{3}]} \pmod p & \text{if } c \in C_1(p), \\ -\dfrac{1}{2c}(-3(c^2+3))^{-[\frac{p}{3}]} \pmod p & \text{if } c \in C_2(p) \end{cases}$$

and

$$V_{\frac{p-(\frac{p}{3})}{3}}(6, 3(c^2+3)) \equiv \begin{cases} 2(3(c^2+3))^{-[\frac{p}{3}]} \pmod p & \text{if } c \in C_0(p), \\ -(3(c^2+3))^{-[\frac{p}{3}]} \pmod p & \text{if } c \in C_1(p) \cup C_2(p). \end{cases}$$

Theorem 2.5. *Let $p > 3$ be a prime, $c \in \mathbb{Z}_p$ and $c(c^2+3) \not\equiv 0 \pmod p$. Then*

$$\sum_{k=1}^{[p/3]} \binom{3k}{k} \Big(\frac{4}{9(c^2+3)}\Big)^k \equiv \begin{cases} 0 \pmod p & \text{if } c \in C_0(p), \\ -\dfrac{3(c+1)}{2c} \pmod p & \text{if } c \in C_1(p), \\ -\dfrac{3(c-1)}{2c} \pmod p & \text{if } c \in C_2(p). \end{cases}$$

Proof. Let $a = c^2+3$ and $b = \frac{2}{3}$. Then $81b^2 - 12a = -3 \cdot 4c^2$. By Lemma 2.6,

$$\sum_{k=0}^{[p/3]} \binom{3k}{k} \Big(\frac{4}{9(c^2+3)}\Big)^k$$
$$\equiv \begin{cases} -(3(c^2+3))^{\frac{p-1}{3}+1} U_{\frac{p-1}{3}-1}(6, 3(c^2+3)) \pmod p & \text{if } 3 \mid p-1, \\ (3(c^2+3))^{\frac{p-2}{3}} U_{\frac{p+1}{3}+1}(6, 3(c^2+3)) \pmod p & \text{if } 3 \mid p-2. \end{cases}$$

If $p\equiv 1 \pmod 3$, by (2.6) and Lemma 2.7 we have

$$\begin{aligned}U_{\frac{p-1}{3}-1}(6,3(c^2+3)) &= \frac{1}{6(c^2+3)}\Big(6U_{\frac{p-1}{3}}(6,3(c^2+3))-V_{\frac{p-1}{3}}(6,3(c^2+3))\Big)\\ &\equiv\begin{cases}-(3(c^2+3))^{-\frac{p-1}{3}-1} \pmod p & \text{if } c\in C_0(p),\\ \dfrac{c+3}{2c}(3(c^2+3))^{-\frac{p-1}{3}-1} \pmod p & \text{if } c\in C_1(p),\\ \dfrac{c-3}{2c}(3(c^2+3))^{-\frac{p-1}{3}-1} \pmod p & \text{if } c\in C_2(p).\end{cases}\end{aligned}$$

If $p\equiv 2 \pmod 3$, by (2.6) and Lemma 2.7 we have

$$\begin{aligned}U_{\frac{p+1}{3}+1}(6,3(c^2+3)) &= 3U_{\frac{p+1}{3}}(6,3(c^2+3))+\frac{1}{2}V_{\frac{p+1}{3}}(6,3(c^2+3))\\ &\equiv\begin{cases}(3(c^2+3))^{-\frac{p-2}{3}} \pmod p & \text{if } c\in C_0(p),\\ -\dfrac{c+3}{2c}(3(c^2+3))^{-\frac{p-2}{3}} \pmod p & \text{if } c\in C_1(p),\\ -\dfrac{c-3}{2c}(3(c^2+3))^{-\frac{p-2}{3}} \pmod p & \text{if } c\in C_2(p).\end{cases}\end{aligned}$$

Hence

$$\sum_{k=0}^{[p/3]}\binom{3k}{k}\Big(\frac{4}{9(c^2+3)}\Big)^k\equiv\begin{cases}1 \pmod p & \text{if } c\in C_0(p),\\ -\dfrac{c+3}{2c} \pmod p & \text{if } c\in C_1(p),\\ -\dfrac{c-3}{2c} \pmod p & \text{if } c\in C_2(p).\end{cases}$$

This yields the result.

Corollary 2.6. *Let $p>3$ be a prime, $d\in\mathbb{Z}_p$ and $(2d+1)(d^2+d+7)\not\equiv 0 \pmod p$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(d^2+d+7)^k}\equiv\begin{cases}0 \pmod p & \text{if } \frac{2d+1}{3}\in C_0(p),\\ -\dfrac{3(d+2)}{2d+1} \pmod p & \text{if } \frac{2d+1}{3}\in C_1(p),\\ -\dfrac{3(d-1)}{2d+1} \pmod p & \text{if } \frac{2d+1}{3}\in C_2(p).\end{cases}$$

Proof. Set $c=\frac{2d+1}{3}$. Then $\frac{4}{9(c^2+3)}=\frac{1}{d^2+d+7}$. Now the result follows from Theorem 2.5.

Corollary 2.7. *Let $p>7$ be a prime. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{2}{9}\Big)^k\equiv 0 \pmod p \iff p=x^2+81y^2 \text{ or } 2x^2+2xy+41y^2,$$

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{4}{9}\Big)^k\equiv 0 \pmod p \iff p=x^2+162y^2 \text{ or } 2x^2+81y^2,$$

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(-\frac{4}{27}\Big)^k\equiv 0 \pmod p \iff p=x^2+54y^2 \text{ or } 2x^2+27y^2,$$

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(-\frac{1}{27}\Big)^k\equiv 0\pmod p\iff p=x^2+135y^2\ or\ 5x^2+27y^2.$$

Proof. If $\sum_{k=1}^{[p/3]}\binom{3k}{k}(\frac{2}{9})^k\equiv 0\pmod p$, by Remark 2.1 we have $(\frac{-1}{p})=(\frac{\frac{2}{9}(4-27\cdot\frac{2}{9})}{p})=1$. If $p=x^2+81y^2$ or $2x^2+2xy+41y^2$, we also have $(\frac{-1}{p})=1$. Suppose $(\frac{-1}{p})=1$ and $s^2\equiv -1\pmod p$ for $s\in\mathbb{Z}$. By Theorem 2.5 and [6, Theorem 5.2],

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{2}{9}\Big)^k\equiv 0\pmod p\Leftrightarrow s\in C_0(p)\Leftrightarrow p=x^2+81y^2\text{ or }2x^2+2xy+41y^2.$$

Similarly, using Theorem 2.5, [6, Theorem 5.2] and Remark 2.1 we deduce remaining results.

For two integers m and n let (m,n) be the greatest common divisor of m and n, and let $[m,n]$ be the least common multiple of m and n. Then we have:

Corollary 2.8. *Let p and q be distinct primes greater than 3, $m,n\in\mathbb{Z}$, $(mn(m^2-n^2)(m^2+3n^2),pq)=1$ and $(\frac{p}{3})p\equiv(\frac{q}{3})q\pmod{[9,m^2+3n^2]}$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{4n^2}{9(m^2+3n^2)}\Big)^k\equiv 0\pmod p\Leftrightarrow\sum_{k=1}^{[q/3]}\binom{3k}{k}\Big(\frac{4n^2}{9(m^2+3n^2)}\Big)^k\equiv 0\pmod q.$$

In particular, for $m=2d+1$ and $n=3$ we see that if $((d-1)(d+2)(2d+1)(d^2+d+7),pq)=1$ and $(\frac{p}{3})p\equiv(\frac{q}{3})q\pmod{[9,4(d^2+d+7)]}$, then

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{(d^2+d+7)^k}\equiv 0\pmod p\Leftrightarrow\sum_{k=1}^{[q/3]}\binom{3k}{k}\frac{1}{(d^2+d+7)^k}\equiv 0\pmod q.$$

Proof. Suppose $m+n(1+2\omega)=\pm\omega^r(1-\omega)^s(a+b\omega)$ with $a,b,r,s\in\mathbb{Z}$ and $a+b\omega\equiv 2\pmod 3$. Then $a^2-ab+b^2\mid m^2+3n^2$ and so $(\frac{p}{3})p\equiv(\frac{q}{3})q\pmod{|a^2-ab+b^2|}$. By [8, (1.1)-(1.2)],

$$\begin{aligned}\Big(\frac{\frac{m}{n}+1+2\omega}{p}\Big)_3&=\Big(\frac{m+n(1+2\omega)}{p}\Big)_3=\Big(\frac{\omega^r(1-\omega)^s(a+b\omega)}{p}\Big)_3\\&=\Big(\frac{\omega}{p}\Big)_3^r\Big(\frac{1-\omega}{p}\Big)_3^s\Big(\frac{a+b\omega}{p}\Big)_3=\omega^{\frac{1-(\frac{p}{3})p}{3}r}\cdot\omega^{\frac{2(1-(\frac{p}{3})p)}{3}s}\Big(\frac{-(\frac{p}{3})p}{a+b\omega}\Big)_3\\&=\omega^{\frac{1-(\frac{q}{3})q}{3}r}\cdot\omega^{\frac{2(1-(\frac{q}{3})q)}{3}s}\Big(\frac{-(\frac{q}{3})q}{a+b\omega}\Big)_3=\Big(\frac{\frac{m}{n}+1+2\omega}{q}\Big)_3.\end{aligned}$$

Thus, $\frac{m}{n}\in C_0(p)$ if and only if $\frac{m}{n}\in C_0(q)$. Now taking $c=\frac{m}{n}$ in Theorem 2.5 and applying the above we derive the result.

Theorem 2.6. *Let q be a prime of the form $3k+1$ and so $4q=L^2+27M^2$ with $L,M\in\mathbb{Z}$ and $L\equiv 1\pmod 3$. Let p be a prime with $p\neq 2,3,q$ and $p\nmid L$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{M^{2k}}{q^k}\equiv\begin{cases}0\pmod p & \text{if } p^{\frac{q-1}{3}}\equiv 1\pmod q,\\ \dfrac{-3\mp 9M/L}{2}\pmod p & \text{if } p^{\frac{q-1}{3}}\equiv\frac{-1\pm 9M/L}{2}\pmod q.\end{cases}$$

Proof. When $p \mid M$, by [6, Corollary 2.1] we have $p^{\frac{q-1}{3}} \equiv 1 \pmod q$. Thus the result is true. Now assume $p \nmid M$. Set $c = \frac{L}{3M}$. Then $c(c^2+3) \not\equiv 0 \pmod p$ and $\frac{4}{9(c^2+3)} = \frac{M^2}{q}$. By Theorem 2.5,

$$\sum_{k=1}^{[p/3]} \binom{3k}{k} \frac{M^{2k}}{q^k} \equiv \begin{cases} 0 \pmod p & \text{if } L/(3M) \in C_0(p), \\ -\frac{3}{2}(1+\frac{3M}{L}) \pmod p & \text{if } L/(3M) \in C_1(p), \\ -\frac{3}{2}(1-\frac{3M}{L}) \pmod p & \text{if } L/(3M) \in C_2(p). \end{cases}$$

From [6, Corollary 2.1] we know that for $r = 0, 1, 2$,

$$p^{\frac{q-1}{3}} \equiv \Big(\frac{-1-L/(3M)}{2}\Big)^r \pmod q \iff \frac{L}{3M} \in C_r(p). \tag{2.7}$$

As $\frac{L}{3M} \equiv -\frac{9M}{L} \pmod q$, from the above we deduce the result.

Corollary 2.9. *Let $p > 7$ be a prime. Then*

$$\sum_{k=1}^{[p/3]} \binom{3k}{k} \frac{1}{7^k} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm 1 \pmod 7, \\ -6 \pmod p & \text{if } p \equiv \pm 2 \pmod 7, \\ 3 \pmod p & \text{if } p \equiv \pm 4 \pmod 7. \end{cases}$$

Proof. As $4 \cdot 7 = 1^2 + 27 \cdot 1^2$, taking $q = 7$ and $L = M = 1$ in Theorem 2.6 we deduce the result.

Similarly, from Theorem 2.6 we deduce the following results.

Corollary 2.10. *Let p be a prime with $p \neq 2, 3, 5, 13$. Then*

$$\sum_{k=1}^{[p/3]} \binom{3k}{k} \frac{1}{13^k} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm 1, \pm 5 \pmod{13}, \\ -\frac{12}{5} \pmod p & \text{if } p \equiv \pm 2, \pm 3 \pmod{13}, \\ -\frac{3}{5} \pmod p & \text{if } p \equiv \pm 4, \pm 6 \pmod{13}. \end{cases}$$

Corollary 2.11. *Let p be a prime with $p \neq 2, 3, 7, 19$. Then*

$$\sum_{k=1}^{[p/3]} \binom{3k}{k} \frac{1}{19^k} \equiv \begin{cases} 0 \pmod p & \text{if } p \equiv \pm 1, \pm 7, \pm 8 \pmod{19}, \\ -\frac{6}{7} \pmod p & \text{if } p \equiv \pm 2, \pm 3, \pm 5 \pmod{19}, \\ -\frac{15}{7} \pmod p & \text{if } p \equiv \pm 4, \pm 6, \pm 9 \pmod{19}. \end{cases}$$

Theorem 2.7. *Let q be a prime of the form $3m+1$ and so $4q = L^2 + 27M^2$ with $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. Let p be a prime with $p \neq 2, 3, q$, $p \nmid L$ and $q \not\equiv 9M^2, 27M^2 \pmod p$. Then the congruence $x^3 - qx - qM \equiv 0 \pmod p$ has three solutions if and only if p is a cubic residue of q.*

Proof. When $p \mid M$, we have $L^2 \equiv 4q \pmod p$ and so $x^3 - qx - qM \equiv 0 \pmod p$ has three solutions. On the other hand, by [6, Corollary 2.1] and Euler's criterion, p is a cubic residue of q. Thus the result is true in the case $p \mid M$. Now we assume $p \nmid M$. By Theorems 2.1 and 2.6,

$$x^3 - qx - qM \equiv 0 \pmod p \text{ has three solutions}$$

$$\begin{aligned}
&\iff (Mx)^3 - qMx - qM \equiv 0 \pmod p \text{ has three solutions}\\
&\iff \tfrac{M^2}{q}x^3 - x - 1 \equiv 0 \pmod p \text{ has three solutions}\\
&\iff \sum_{k=1}^{[p/3]} \binom{3k}{k}\frac{M^{2k}}{q^k} \equiv 0 \pmod p\\
&\iff p^{\frac{q-1}{3}} \equiv 1 \pmod q \iff p \text{ is a cubic residues of } q.
\end{aligned}$$

As examples, if $p > 3$ is a prime, then

$$\begin{aligned}
&x^3 - 7x - 7 \equiv 0 \pmod p \text{ has three solutions} \Leftrightarrow p = 7 \text{ or } p \equiv \pm 1 \pmod 7,\\
&x^3 - 13x - 13 \equiv 0 \pmod p \text{ has three solutions} \Leftrightarrow p = 13 \text{ or } p \equiv \pm 1, \pm 5 \pmod{13},\\
&x^3 - 31x - 62 \equiv 0 \pmod p \text{ has three solutions}\\
&\qquad \Leftrightarrow p = 31 \text{ or } p \text{ is a cubic residue of } 31.
\end{aligned}$$

Theorem 2.8. *Let q be a prime of the form $3m+1$ and so $4q = L^2 + 27M^2$ with $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. Let p be a prime with $p \neq 2, 3, q$ and $p \nmid M$. Then*

$$\sum_{k=1}^{[p/3]} \binom{3k}{k}\Big(\frac{L^2}{27q}\Big)^k \equiv \begin{cases} 0 \pmod p & \text{if } p^{\frac{q-1}{3}} \equiv 1 \pmod q,\\ \dfrac{-3 \pm L/(3M)}{2} \pmod p & \text{if } p^{\frac{q-1}{3}} \equiv \frac{-1 \mp L/(3M)}{2} \pmod q. \end{cases}$$

Proof. By [6, Corollary 2.1 and Proposition 2.1], the result is true when $p \mid L$. Now we assume $p \nmid L$. Set $c = -\frac{9M}{L}$. Then $c(c^2+3) \not\equiv 0 \pmod p$ and $\frac{4}{9(c^2+3)} = \frac{L^2}{27q}$. By [6, Proposition 2.2], $-\frac{9M}{L} \in C_i(p)$ if and only if $\frac{L}{3M} \in C_i(p)$. Thus, from Theorem 2.5 we deduce that

$$\sum_{k=1}^{[p/3]} \binom{3k}{k}\Big(\frac{L^2}{27q}\Big)^k \equiv \begin{cases} 0 \pmod p & \text{if } L/(3M) \in C_0(p),\\ \dfrac{1}{2}(-3 + \dfrac{L}{3M}) \pmod p & \text{if } L/(3M) \in C_1(p),\\ \dfrac{1}{2}(-3 - \dfrac{L}{3M}) \pmod p & \text{if } L/(3M) \in C_2(p). \end{cases}$$

This together with (2.7) yields the result.

Corollary 2.12. *Let q be a prime of the form $3m+1$ and so $4q = L^2+27M^2$ with $L, M \in \mathbb{Z}$ and $L \equiv 1 \pmod 3$. Let p be a prime with $p \neq 2, 3, q$, $p \nmid M$ and $q \not\equiv 9M^2, 27M^2 \pmod p$. Then the congruence $x^3 - 3qx - qL \equiv 0 \pmod p$ has three solutions if and only if p is a cubic residue of q.*

Proof. When $p \mid L$, we have $x^3 - 3qx - qL \equiv x(x^2 - \frac{81}{4}M^2) \pmod p$ and so $N_p(x^3 - 3qx - qL) = 3$. On the other hand, from [6, Proposition 2.1 and Corollary 2.1] we know that $0 \in C_0(p)$ and so p is a cubic residue of q. Thus the result is true in this case. Now we assume that $p \nmid L$. By Theorems 2.1 and 2.8,

$$\begin{aligned}
&x^3 - 3qx - qL \equiv 0 \pmod p \text{ has three solutions}\\
&\iff (\tfrac{L}{3}x)^3 - 3q \cdot \tfrac{L}{3}x - qL \equiv 0 \pmod p \text{ has three solutions}\\
&\iff \tfrac{L^2}{27q}x^3 - x - 1 \equiv 0 \pmod p \text{ has three solutions}
\end{aligned}$$

$$\iff \sum_{k=1}^{[p/3]}\binom{3k}{k}\Big(\frac{L^2}{27q}\Big)^k\equiv 0\pmod p$$
$$\iff p^{\frac{q-1}{3}}\equiv 1\pmod q \iff p \text{ is a cubic residues of } q.$$

Remark 2.2 Assume that the conditions in Corollary 2.12 hold. From (1.2) we know that the discriminant of $x^3-3qx-qL$ is $(27qM)^2$. Thus, by (1.1), $N_p(x^3-3qx-qL)=0$ or 3. Hence, by Corollary 2.12, $x^3-3qx-qL\equiv 0 \pmod p$ is solvable if and only if p is a cubic residue (mod q). This is a well known result since Gauss and Kummer. See [1, Theorem 10.10.5] or [3, Corollaries 2.16 and 2.25]. In our proof, we do not need cyclotomic numbers.

Corollary 2.13. *Let p be a prime with $p\neq 2,3,7$. Then*

$$\sum_{k=1}^{[p/3]}\binom{3k}{k}\frac{1}{189^k}\equiv\begin{cases}0\pmod p & \text{if } p\equiv\pm1\pmod 7,\\ -\frac{4}{3}\pmod p & \text{if } p\equiv\pm2\pmod 7,\\ -\frac{5}{3}\pmod p & \text{if } p\equiv\pm4\pmod 7.\end{cases}$$

Proof. As $4\cdot 7=1^2+27\cdot 1^2$, taking $q=7$ and $L=M=1$ in Theorem 2.8 we obtain the result.

Conjecture 2.1. *Let $p>3$ be a prime, $c\in\mathbb{Z}_p$ and $c^2\not\equiv -3 \pmod p$. Then*

$$c\sum_{k=(p+1)/2}^{[2p/3]}\binom{3k}{k}\Big(\frac{4}{9(c^2+3)}\Big)^k\equiv\begin{cases}0\pmod p & \text{if } c\in C_0(p),\\ 1\pmod p & \text{if } c\in C_1(p),\\ -1\pmod p & \text{if } c\in C_2(p).\end{cases}$$

From Conjecture 2.1 and (2.7) we may deduce the following result.

Conjecture 2.2. *Let q be a prime of the form $3k+1$ and so $4q=L^2+27M^2$ with $L,M\in\mathbb{Z}$ and $L\equiv 1 \pmod 3$. Let p be a prime with $p\neq 2,3,q$ and $p\nmid LM$. Then*

$$\sum_{k=(p+1)/2}^{[2p/3]}\binom{3k}{k}\frac{M^{2k}}{q^k}\equiv\begin{cases}0\pmod p & \text{if } p^{\frac{q-1}{3}}\equiv 1\pmod q,\\ \pm\frac{3M}{L}\pmod p & \text{if } p^{\frac{q-1}{3}}\equiv\frac{-1\pm 9M/L}{2}\pmod q.\end{cases}$$

and

$$\sum_{k=(p+1)/2}^{[2p/3]}\binom{3k}{k}\frac{L^{2k}}{(27q)^k}\equiv\begin{cases}0\pmod p & \text{if } p^{\frac{q-1}{3}}\equiv 1\pmod q,\\ \pm\frac{L}{9M}\pmod p & \text{if } p^{\frac{q-1}{3}}\equiv\frac{-1\pm L/(3M)}{2}\pmod q.\end{cases}$$

Acknowledgment

The author is supported by the National Natural Science Foundation of China (grant No. 11371163).

References

[1] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[2] L.E. Dickson, *Criteria for the irreducibility of functions in a finite field*, Bull. Amer. Math. Soc. **13**(1906), 1-8.

[3] P. Pollack, *Not Always Buried Deep: A Second Course in Elementary Number Theory*, AMS, USA, 2009.

[4] T. Skolem, *On a certain connection between the discriminant of a polynomial and the number of its irreducible factors mod p*, Norsk Mat. Tidsskr. **34**(1952), 81-85.

[5] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress, Zürich, 1897, pp. 182-193.

[6] Z.H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84**(1998), 291-335.

[7] Z.H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory **102**(2003), 41-89.

[8] Z.H. Sun, *Cubic residues and binary quadratic forms*, J. Number Theory **124**(2007), 62-104.

[9] Z.H. Sun, *Congruences concerning Lucas sequences*, Int. J. Number Theory **10**(2014), 793-815.

[10] Z.W. Sun, *Various congruences involving binomial coefficients and higher-order Catalan numbers*, arXiv:0909.3808v2, 2009.

[11] H.C. Williams, *Édouard Lucas and Primality Testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol.22, Wiley, New York, 1998, pp. 74-92.

[12] L.L. Zhao, H. Pan and Z.W. Sun, *Some congruences for the second-order Catalan numbers*, Proc. Amer. Math. Soc. **138**(2010), 37-46.