

Quartic residues and sums involving $\binom{4k}{2k}$

Zhi-Hong Sun

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

Abstract

Let p be an odd prime and let $m \not\equiv 0 \pmod{p}$ be a rational p -adic integer. In this paper we reveal the connection between quartic residues and the sum $\sum_{k=0}^{[p/4]} \binom{4k}{2k} \frac{1}{m^k}$, where $[x]$ is the greatest integer not exceeding x . Let q be a prime of the form $4k+1$ and so $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$. When $p \nmid ab(a^2 - b^2)q$, we show that for $r = 0, 1, 2, 3$,

$$p^{\frac{q-1}{4}} \equiv \left(\frac{a}{b}\right)^r \pmod{q} \Leftrightarrow \sum_{k=0}^{[p/4]} \binom{4k}{2k} \left(\frac{a^2}{16q}\right)^k \equiv (-1)^{\frac{p^2-1}{8}a + \frac{p-1}{2} \cdot \frac{q-1}{4}} \left(\frac{p}{q}\right) \left(\frac{a}{b}\right)^r \pmod{p},$$

where $\left(\frac{p}{q}\right)$ is the Legendre symbol. We also establish congruences for $\sum_{k=0}^{[p/4]} \binom{4k}{2k} \frac{1}{m^k} \pmod{p}$ in the cases $m = 17, 18, 20, 32, 52, 80, 272$.

MSC: Primary 11A07; Secondary 11A15, 11B39, 11B65, 11E25.

Keywords: congruence; Lucas sequence; quartic residue; quartic reciprocity; binary quadratic form.

1. Introduction

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 $\left(\frac{m}{p}\right)$ be the Legendre symbol.

Suppose that p is an odd prime and $a \in \mathbb{Z}_p$. In [7] the author investigated congruences for $\sum_{k=0}^{[p/4]} \binom{4k}{2k} a^k$ modulo p , where $[x]$ is the greatest integer not exceeding x . For $k \in \{0, 1, \dots, p-1\}$ it is easily seen that $p \nmid \binom{4k}{2k}$ if and only if $0 \leq k < \frac{p}{4}$ or $\frac{p}{2} < k < \frac{3p}{4}$. In this paper we reveal the connection between quartic residues and the sum $\sum_{k=0}^{[p/4]} \binom{4k}{2k} a^k$. We also investigate congruences for $\sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} a^k$ modulo p .

¹The author is supported by the National Natural Science Foundation of China (grant no. 11371163).

Let $i = \sqrt{-1}$. For an odd prime p let $\left(\frac{a+bi}{p}\right)_4$ be the quartic Jacobi symbol defined in [1,2,3,4,6]. Following [4] we define

$$Q_r(p) = \left\{ c \in \mathbb{Z}_p : \left(\frac{c+i}{p}\right)_4 = i^r \right\} \quad \text{for } r = 0, 1, 2, 3.$$

According to [4,6], $Q_r(p)$ ($r \in \{0, 1, 2, 3\}$) plays a central role in the theory of quartic residues and nonresidues. In this paper, for an odd prime p and $c \in \mathbb{Z}_p$ with $c(c^2 + 1) \not\equiv 0 \pmod{p}$ we give simple criteria for $c \in Q_r(p)$ by proving that

$$(1.1) \quad \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv \begin{cases} 1 \pmod{p} & \text{if } c \in Q_0(p), \\ -\frac{1}{c} \pmod{p} & \text{if } c \in Q_1(p), \\ -1 \pmod{p} & \text{if } c \in Q_2(p), \\ \frac{1}{c} \pmod{p} & \text{if } c \in Q_3(p) \end{cases}$$

and

$$(1.2) \quad 2c \sum_{k=(p+1)/2}^{\lfloor 3p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ 1 \pmod{p} & \text{if } c \in Q_1(p), \\ -1 \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

Let q be a prime of the form $4m + 1$ and so $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$. Let p be an odd prime with $p \nmid ab(a^2 - b^2)q$. In this paper, using (1.1) and the theory of quartic residues we show that for $r = 0, 1, 2, 3$,

$$(1.3) \quad \begin{aligned} p^{\frac{q-1}{4}} &\equiv \left(\frac{a}{b}\right)^r \pmod{q} \\ \Leftrightarrow \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a^2}{16q}\right)^k &\equiv (-1)^{\frac{p^2-1}{8}a + \frac{p-1}{2} \cdot \frac{q-1}{4}} \left(\frac{p}{q}\right) \left(\frac{a}{b}\right)^r \pmod{p}. \end{aligned}$$

As consequences we establish congruences for $\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{m^k} \pmod{p}$ in the cases $m = 17, 18, 20, 32, 52, 80, 272$.

In addition to the above notation, throughout this paper we use (m, n) to denote the greatest common divisor of integers m and n . If $a, b, c \in \mathbb{Z}$ and $p = ax^2 + bxy + cy^2$ for some integers x and y , we briefly write that $p = ax^2 + bxy + cy^2$. We also use $[a, b, c]$ to denote the equivalence class containing the form $ax^2 + bxy + cy^2$, and use $H(d)$ to denote the form class group consisting of classes of primitive binary quadratic forms of discriminant d .

2. Congruences for $\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} a^k \pmod{p}$

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

$$\begin{aligned} U_0(P, Q) &= 0, \quad U_1(P, Q) = 1, \quad U_{n+1}(P, Q) = PU_n(P, Q) - QU_{n-1}(P, Q) \quad (n \geq 1), \\ V_0(P, Q) &= 2, \quad V_1(P, Q) = P, \quad V_{n+1}(P, Q) = PV_n(P, Q) - QV_{n-1}(P, Q) \quad (n \geq 1). \end{aligned}$$

It is well known (see [8]) that

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

and

$$(2.2) \quad V_n(P, Q) = \left(\frac{P + \sqrt{P^2 - 4Q}}{2} \right)^n + \left(\frac{P - \sqrt{P^2 - 4Q}}{2} \right)^n.$$

Lemma 2.1 ([7, Theorem 2.1]). *Let p be an odd prime, $P, Q \in \mathbb{Z}_p$ and $PQ \not\equiv 0 \pmod{p}$. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{Q}{4P^2} \right)^k \equiv \left(\frac{P}{p} \right) U_{\frac{p+1}{2}}(P, Q) \pmod{p}$$

and

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{P^2}{64Q} \right)^k \equiv (-Q)^{-\lfloor \frac{p}{4} \rfloor} U_{\frac{p+(-1)}{2}}(P, Q) \pmod{p}.$$

Lemma 2.2 ([7, Theorem 2.2]). *Let p be an odd prime and $x \in \mathbb{Z}_p$ with $x \not\equiv 0, 1 \pmod{p}$. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16x)^k} \equiv \begin{cases} \frac{1}{x^{\frac{p-1}{4}}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{x}{16} \right)^k \pmod{p} & \text{if } 4 \mid p-1, \\ \left(1 - \frac{1}{x} \right)^{\frac{p-3}{4}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(1-x))^k} \pmod{p} & \text{if } 4 \mid p-3. \end{cases}$$

Lemma 2.3 ([4, Lemma 2.1]). *Let p be an odd prime, $m, n \in \mathbb{Z}_p$ and $m^2 + n^2 \not\equiv 0 \pmod{p}$. Then $\left(\frac{m+ni}{p} \right)_4^2 = \left(\frac{m^2+n^2}{p} \right)$.*

Theorem 2.1. *Suppose that p is an odd prime, $c \in \mathbb{Z}_p$ and $c(c^2 + 1) \not\equiv 0 \pmod{p}$. Then*

$$(2.3) \quad \left(\frac{2}{p} \right) \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{c^2}{16(c^2 + 1)} \right)^k \equiv \begin{cases} 1 \pmod{p} & \text{if } c \in Q_0(p), \\ c \pmod{p} & \text{if } c \in Q_1(p), \\ -1 \pmod{p} & \text{if } c \in Q_2(p), \\ -c \pmod{p} & \text{if } c \in Q_3(p) \end{cases}$$

and

$$(2.4) \quad \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv \begin{cases} 1 \pmod{p} & \text{if } c \in Q_0(p), \\ -\frac{1}{c} \pmod{p} & \text{if } c \in Q_1(p), \\ -1 \pmod{p} & \text{if } c \in Q_2(p), \\ \frac{1}{c} \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

Proof. Clearly

$$\left(\frac{c+i}{p}\right)_4 = \left(\frac{i}{p}\right)_4 \left(\frac{1-ci}{p}\right)_4 = \left(\frac{2}{p}\right) \left(\frac{-\frac{1}{c}+i}{p}\right)_4.$$

Thus, if $\left(\frac{2}{p}\right) = 1$, then $-\frac{1}{c} \in Q_r(p)$ if and only if $c \in Q_r(p)$; if $\left(\frac{2}{p}\right) = -1$, then $-\frac{1}{c} \in Q_r(p)$ if and only if $c \in Q_{r'}(p)$, where $r' \in \{0, 1, 2, 3\}$ is given by $r' \equiv r + 2 \pmod{4}$. Thus, replacing c with $-\frac{1}{c}$ in (2.3) we get (2.4). Hence (2.3) is equivalent to (2.4).

By [7, proof of Theorem 2.1], for $P, Q \in \mathbb{Z}_p$ with $PQ \not\equiv 0 \pmod{p}$,

$$(2.5) \quad V_{\frac{p-1}{2}}(P, (P^2 - 4Q)/4) \equiv 2 \left(\frac{2P}{p}\right) \sum_{k=0}^{[p/4]} \binom{4k}{2k} \left(\frac{Q}{4P^2}\right)^k \pmod{p}.$$

Taking $P = 2c$ and $Q = c^2 + 1$ we see that

$$V_{\frac{p-1}{2}}(2c, -1) \equiv 2 \left(\frac{c}{p}\right) \sum_{k=0}^{[p/4]} \binom{4k}{2k} \left(\frac{c^2 + 1}{16c^2}\right)^k \pmod{p}.$$

From Lemma 2.3 we have $\left(\frac{n+i}{p}\right)_4^2 = \left(\frac{n^2+1}{p}\right)$ for $n^2 + 1 \not\equiv 0 \pmod{p}$. We first assume $p \equiv 1 \pmod{4}$. Taking $a = -1$ and $b = 2c$ in [5, Corollary 3.1(i)] we get

$$V_{\frac{p-1}{2}}(2c, -1) \equiv \begin{cases} 2(4c^2 + 4)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_0(p), \\ 2c(4c^2 + 4)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_1(p), \\ -2(4c^2 + 4)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_2(p), \\ -2c(4c^2 + 4)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

Combining the above with the fact $4^{\frac{p-1}{4}} = 2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$ we obtain

$$(2.6) \quad \left(\frac{2c}{p}\right) \sum_{k=0}^{[p/4]} \binom{4k}{2k} \left(\frac{c^2 + 1}{16c^2}\right)^k \equiv \begin{cases} (c^2 + 1)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_0(p), \\ c(c^2 + 1)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_1(p), \\ -(c^2 + 1)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_2(p), \\ -c(c^2 + 1)^{\frac{p-1}{4}} \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

Putting $x = \frac{c^2+1}{c^2}$ in Lemma 2.2 we see that

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

This together with (2.6) yields (2.3). Hence (2.4) is also true.

Now we assume $p \equiv 3 \pmod{4}$. Taking $P = 2c$ and $Q = -1$ in Lemma 2.1 we see that

$$\sum_{k=0}^{[p/4]} \binom{4k}{2k} \frac{1}{(-16c^2)^k} \equiv \left(\frac{2c}{p}\right) U_{\frac{p+1}{2}}(2c, -1) \pmod{p}.$$

By [5, Theorem 3.1(ii)] and Lemma 2.3,

$$U_{\frac{p+1}{2}}(2c, -1) \equiv \begin{cases} 2c(4c^2 + 4)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_0(p), \\ -2(4c^2 + 4)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_1(p), \\ -2c(4c^2 + 4)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_2(p), \\ 2(4c^2 + 4)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

Thus,

$$\left(\frac{c}{p}\right) \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(-16c^2)^k} \equiv \begin{cases} c(c^2 + 1)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_0(p), \\ -(c^2 + 1)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_1(p), \\ -c(c^2 + 1)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_2(p), \\ (c^2 + 1)^{\frac{p-3}{4}} \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

By Lemma 2.2,

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv \frac{1}{c} \left(\frac{c}{p}\right) (c^2 + 1)^{-\frac{p-3}{4}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(-16c^2)^k} \pmod{p}.$$

Now combining the above we obtain (2.4). Since (2.3) is equivalent to (2.4), the proof is complete.

Remark 2.1 Let p be an odd prime, $a \in \mathbb{Z}_p$, $\left(\frac{a}{p}\right) = -1$ and $\left(\frac{a+1}{p}\right) = 1$. Taking $P = 2$ and $Q = a + 1$ in [7, Theorem 2.3(i)] we see that

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(a+1))^k} \equiv 0 \pmod{p}.$$

Replacing a with $\frac{1}{a}$ we see that for $a \in \mathbb{Z}_p$ with $\left(\frac{a}{p}\right) = \left(\frac{a+1}{p}\right) = -1$,

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a}{16(a+1)}\right)^k \equiv 0 \pmod{p}.$$

Corollary 2.1. *Suppose that p is an odd prime, $c \in \mathbb{Z}_p$ and $c(c^2 + 1) \not\equiv 0 \pmod{p}$. Then*

$$\left(\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{c^2}{16(c^2 + 1)}\right)^k\right) \left(\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k}\right) \equiv \left(\frac{2(c^2 + 1)}{p}\right) \pmod{p}.$$

Proof. By Lemma 2.3, $c \in Q_0(p) \cup Q_2(p)$ if and only if $\left(\frac{c^2+1}{p}\right) = 1$. Thus the result follows from Theorem 2.1.

Corollary 2.2. *Suppose that p and q are distinct primes, $m, n \in \mathbb{Z}$, $(mn(m^2 + n^2)(m^2 - n^2), pq) = 1$ and $p \equiv \pm q \pmod{8(m^2 + n^2)}$. Assume $a \in \{1, -1, \frac{n}{m}, -\frac{n}{m}\}$. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{n^2}{16(m^2 + n^2)}\right)^k \equiv a \pmod{p}$$

$$\Leftrightarrow \sum_{k=0}^{\lfloor q/4 \rfloor} \binom{4k}{2k} \left(\frac{n^2}{16(m^2 + n^2)} \right)^k \equiv a \pmod{q}.$$

Proof. By [4, Theorem 2.1], $\frac{m}{n} \in Q_r(p) \Leftrightarrow \frac{m}{n} \in Q_r(q)$. Now taking $c = \frac{m}{n}$ in (2.4) we obtain the result.

Corollary 2.3. *Let p be an odd prime. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{32^k} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv \pm 1, \pm 3 \pmod{16}, \\ -1 \pmod{p} & \text{if } p \equiv \pm 5, \pm 7 \pmod{16}. \end{cases}$$

Proof. It is well known (see [1-3]) that

$$(2.7) \quad \left(\frac{1+i}{p} \right)_4 = i^{\frac{(-1)^{\frac{p-1}{2}} - 1}{4} p - 1} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{16}, \\ i & \text{if } p \equiv \pm 5 \pmod{16}, \\ -1 & \text{if } p \equiv \pm 7 \pmod{16}, \\ -i & \text{if } p \equiv \pm 3 \pmod{16}. \end{cases}$$

Now taking $c = 1$ in (2.4) we deduce the result.

Corollary 2.4. *Suppose that p is an odd prime, $c \in \mathbb{Z}_p$, $c \not\equiv 0, \pm 1 \pmod{p}$ and $c^2 + 1 \not\equiv 0 \pmod{p}$. Then the congruence $x^4 - 2(c^2 + 1)x^2 + c^2(c^2 + 1) \equiv 0 \pmod{p}$ is solvable if and only if*

$$\sum_{k=1}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv 0 \pmod{p}.$$

Proof. By [6, Theorem 4.2], $c \in C_0(p)$ if and only if $x^4 - 2(c^2 + 1)x^2 + c^2(c^2 + 1) \equiv 0 \pmod{p}$ is solvable. By Theorem 2.1, $c \in C_0(p)$ if and only if $\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv 1 \pmod{p}$. Thus the result follows.

Corollary 2.5. *Let p be an odd prime, $d \in \mathbb{Z}$, $d \not\equiv 0, \pm 1 \pmod{p}$, $\left(\frac{-d}{p}\right) = 1$ and $1 - d = (-1)^r 2^s W$ ($W \equiv 1 \pmod{4}$). Let d_0 be the product of all distinct odd prime divisors of $1 - d$, and let $m = 8d_0$ or $\frac{4d_0}{(2, r+s/2)}$ according as $2 \nmid s$ or $2 \mid s$. Then p is represented by some primitive form $ax^2 + 2bxy + cy^2$ of discriminant $-4m^2d$ with the condition that $(a, 2(1-d)) = 1$ and $\left(\frac{b-mi}{a}\right)_4 = 1$ if and only if*

$$\sum_{k=1}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(1-d))^k} \equiv 0 \pmod{p}.$$

Proof. This is immediate from [6, Theorem 4.2] and (2.4).

It is known that

$$\begin{aligned} H(-128) &= \{[1, 0, 32], [4, 4, 9], [3, 2, 11], [3, -2, 11]\}, \\ H(-768) &= \{[1, 0, 192], [12, 12, 19], [3, 0, 64], [4, 4, 49], \\ &\quad [7, 4, 28], [7, -4, 28], [13, 8, 16], [13, -8, 16]\}, \\ H(-80) &= \{[1, 0, 20], [4, 0, 5], [3, 2, 7], [3, -2, 7]\}. \end{aligned}$$

Thus taking $d = 2, 3, 5$ in Corollary 2.5 and doing some calculations for certain quartic Jacobi symbols we see that for any prime $p > 3$,

$$(2.8) \quad p = x^2 + 32y^2 \Leftrightarrow \sum_{k=1}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(-16)^k} \equiv 0 \pmod{p},$$

$$(2.9) \quad p = x^2 + 192y^2 \text{ or } 12x^2 + 12xy + 19y^2 \Leftrightarrow \sum_{k=1}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(-32)^k} \equiv 0 \pmod{p},$$

$$(2.10) \quad p = x^2 + 20y^2 \Leftrightarrow \sum_{k=1}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{(-64)^k} \equiv 0 \pmod{p}.$$

Lemma 2.4 ([4, Theorem 2.2]). *Let q be a prime of the form $4m+1$ and $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$, $2 \mid b$ and $a + b \equiv 1 \pmod{4}$. Suppose that p is an odd prime and $p \nmid bq$. For $r = 0, 1, 2, 3$ we have*

$$\left((-1)^{\frac{p-1}{2}} p \right)^{\frac{q-1}{4}} \equiv \left(-\frac{a}{b} \right)^r \pmod{q} \iff \frac{a}{b} \in Q_r(p).$$

Theorem 2.2. *Let q be a prime of the form $4m+1$ and $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod{2}$. Suppose that p is an odd prime and $p \nmid bq$. Then*

$$(-1)^{\frac{p^2-1}{8} + \frac{p-1}{2} \cdot \frac{q-1}{4}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a^2}{16q} \right)^k \equiv \begin{cases} \pm 1 \pmod{p} & \text{if } p^{\frac{q-1}{4}} \equiv \pm 1 \pmod{q}, \\ \mp \frac{a}{b} \pmod{p} & \text{if } p^{\frac{q-1}{4}} \equiv \pm \frac{a}{b} \pmod{q}. \end{cases}$$

Proof. Clearly the result does not depend on the sign of a . We may assume $a + b \equiv 1 \pmod{4}$. Taking $c = \frac{a}{b}$ in (2.3) we see that

$$\left(\frac{2}{p} \right) \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a^2}{16q} \right)^k \equiv \begin{cases} 1 \pmod{p} & \text{if } \frac{a}{b} \in Q_0(p), \\ \frac{a}{b} \pmod{p} & \text{if } \frac{a}{b} \in Q_1(p), \\ -1 \pmod{p} & \text{if } \frac{a}{b} \in Q_2(p), \\ -\frac{a}{b} \pmod{p} & \text{if } \frac{a}{b} \in Q_3(p). \end{cases}$$

This is also true when $p \mid a$ since $\left(\frac{0+i}{p} \right)_4 = \left(\frac{2}{p} \right)$. Now applying Lemma 2.4 we deduce the result.

Corollary 2.6. *Let $p \neq 5$ be an odd prime. Then*

$$(-1)^{\lfloor \frac{p}{4} \rfloor} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{80^k} \equiv \begin{cases} \pm 1 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{5}, \\ \pm \frac{1}{2} \pmod{p} & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

Proof. Taking $q = 5$, $a = 1$ and $b = 2$ in Theorem 2.2 we deduce the result.

Corollary 2.7. *Let $p \neq 13$ be an odd prime. Then*

$$(-1)^{\lfloor \frac{p}{4} \rfloor} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{9}{208} \right)^k \equiv \begin{cases} \pm 1 \pmod{p} & \text{if } p \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \mp \frac{3}{2} \pmod{p} & \text{if } p \equiv \pm 2, \pm 5, \pm 6 \pmod{13}. \end{cases}$$

Proof. Taking $q = 13$, $a = -3$ and $b = 2$ in Theorem 2.2 we deduce the result.

Corollary 2.8. *Let $p \neq 17$ be an odd prime. Then*

$$\binom{2}{p} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{272^k} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv \pm 1, \pm 4 \pmod{17}, \\ -1 \pmod{p} & \text{if } p \equiv \pm 2, \pm 8 \pmod{17}, \\ \frac{1}{4} \pmod{p} & \text{if } p \equiv \pm 6, \pm 7 \pmod{17}, \\ -\frac{1}{4} \pmod{p} & \text{if } p \equiv \pm 3, \pm 5 \pmod{17}. \end{cases}$$

Proof. Taking $q = 17$, $a = 1$ and $b = 4$ in Theorem 2.2 we deduce the result.

Theorem 2.3. *Let q be a prime of the form $4m + 1$ and $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod{2}$. Suppose that p is an odd prime and $p \nmid aq$. Then*

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{4}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{b^2}{16q} \right)^k \equiv \begin{cases} \pm 1 \pmod{p} & \text{if } p^{\frac{q-1}{4}} \equiv \pm 1 \pmod{q}, \\ \mp \frac{b}{a} \pmod{p} & \text{if } p^{\frac{q-1}{4}} \equiv \pm \frac{b}{a} \pmod{q}. \end{cases}$$

Proof. Clearly the result does not depend on the sign of a . We may assume $a + b \equiv 1 \pmod{4}$. When $p \mid b$, by [4, Theorem 2.2] we have $((-1)^{\frac{p-1}{2}} p)^{\frac{q-1}{4}} \equiv 1 \pmod{q}$. Thus the result is true in this case. Now we assume $p \nmid b$. Taking $c = \frac{a}{b}$ in (2.4) and then applying Lemma 2.4 we obtain the result.

Combining Theorem 2.2 with Theorem 2.3 we obtain (1.3).

Corollary 2.9. *Let $p > 3$ be a prime. Then*

$$\begin{aligned} (-1)^{\frac{p-1}{2}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{20^k} &\equiv \begin{cases} \pm 1 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{5}, \\ \pm 2 \pmod{p} & \text{if } p \equiv \pm 3 \pmod{5}, \end{cases} \\ (-1)^{\frac{p-1}{2}} \sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{52^k} &\equiv \begin{cases} \pm 1 \pmod{p} & \text{if } p \equiv \pm 1, \pm 3, \pm 9 \pmod{13}, \\ \pm \frac{2}{3} \pmod{p} & \text{if } p \equiv \pm 2, \pm 5, \pm 6 \pmod{13} \end{cases} \end{aligned}$$

and

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{17^k} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv \pm 1, \pm 4 \pmod{17}, \\ -1 \pmod{p} & \text{if } p \equiv \pm 2, \pm 8 \pmod{17}, \\ 4 \pmod{p} & \text{if } p \equiv \pm 3, \pm 5 \pmod{17}, \\ -4 \pmod{p} & \text{if } p \equiv \pm 6, \pm 7 \pmod{17}. \end{cases}$$

Proof. Taking $q = 5, 13, 17$ in Theorem 2.3 we deduce the result.

Theorem 2.4. *Let p be an odd prime, $a, b \in \mathbb{Z}_p$ and $ab(a^2 - b^2) \not\equiv 0 \pmod{p}$. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a^2 - b^2}{16a^2} \right)^k \equiv \frac{1}{2b} \binom{2a}{p} \left\{ (a+b) \left(\frac{a+b}{p} \right) - (a-b) \left(\frac{a-b}{p} \right) \right\} \pmod{p}$$

and

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a^2}{16(a^2 - b^2)} \right)^k$$

$$\equiv \begin{cases} \frac{1}{2b} \left\{ (a+b) \left(\frac{a-b}{p} \right) - (a-b) \left(\frac{a+b}{p} \right) \right\} (b^2 - a^2)^{\frac{p-1}{4}} \pmod{p} & \text{if } 4 \mid p-1, \\ \frac{1}{2b} \left\{ \left(\frac{a+b}{p} \right) - \left(\frac{a-b}{p} \right) \right\} (b^2 - a^2)^{\frac{p+1}{4}} \pmod{p} & \text{if } 4 \nmid p-1. \end{cases}$$

Proof. By (2.1) we have

$$\begin{aligned} U_{\frac{p+1}{2}} \left(a, \frac{a^2 - b^2}{4} \right) &= \frac{1}{b} \left\{ \left(\frac{a+b}{2} \right)^{\frac{p+1}{2}} - \left(\frac{a-b}{2} \right)^{\frac{p+1}{2}} \right\} \\ &\equiv \frac{1}{2b} \binom{2}{p} \left\{ (a+b) \left(\frac{a+b}{p} \right) - (a-b) \left(\frac{a-b}{p} \right) \right\} \pmod{p}. \end{aligned}$$

Now taking $P = a$ and $Q = \frac{a^2 - b^2}{4}$ in Lemma 2.1 and then applying the above we obtain the first part.

Taking $P = 2a$ and $Q = a^2 - b^2$ in Lemma 2.1 and then applying (2.1) we see that

$$\begin{aligned} &\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(\frac{a^2}{16(a^2 - b^2)} \right)^k \\ &\equiv (b^2 - a^2)^{-\lfloor \frac{p}{4} \rfloor} U_{\frac{p+(-1)}{2}}(2a, a^2 - b^2) \\ &= (b^2 - a^2)^{\frac{p-(-1)}{4} - \frac{p-1}{2}} \frac{1}{2b} \left\{ (a+b)^{\frac{p+(-1)}{2}} - (a-b)^{\frac{p+(-1)}{2}} \right\} \\ &\equiv \begin{cases} \left(\frac{b^2 - a^2}{p} \right) (b^2 - a^2)^{\frac{p-1}{4}} \frac{1}{2b} \left\{ (a+b) \left(\frac{a+b}{p} \right) - (a-b) \left(\frac{a-b}{p} \right) \right\} \pmod{p} & \text{if } 4 \mid p-1, \\ \left(\frac{b^2 - a^2}{p} \right) (b^2 - a^2)^{\frac{p+1}{4}} \frac{1}{2b} \left\{ \left(\frac{a+b}{p} \right) - \left(\frac{a-b}{p} \right) \right\} \pmod{p} & \text{if } 4 \nmid p-1. \end{cases} \end{aligned}$$

This yields the remaining part.

Corollary 2.10. *Let p be an odd prime, $m \in \mathbb{Z}_p$ and $m \not\equiv 0, \pm 1 \pmod{p}$. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(-\frac{m}{4(m-1)^2} \right)^k \equiv \frac{1}{m+1} \left(\frac{m-1}{p} \right) \left\{ m \binom{m}{p} + \binom{-1}{p} \right\} \pmod{p}$$

and

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \left(-\frac{(m-1)^2}{64m} \right)^k \equiv \begin{cases} \frac{1}{m+1} \left(m + \left(\frac{m}{p} \right) \right) m^{\frac{p-1}{4}} \pmod{p} & \text{if } 4 \mid p-1, \\ \frac{1}{m+1} \left(\left(\frac{m}{p} \right) + 1 \right) m^{\frac{p+1}{4}} \pmod{p} & \text{if } 4 \nmid p-1. \end{cases}$$

Proof. Taking $a = \frac{m-1}{2}$ and $b = \frac{m+1}{2}$ in Theorem 2.4 we deduce the result.

Corollary 2.11. *Let $p > 3$ be a prime. Then*

$$\sum_{k=0}^{\lfloor p/4 \rfloor} \binom{4k}{2k} \frac{1}{18^k} \equiv 2 \binom{6}{p} - \binom{3}{p} \pmod{p}.$$

Proof. Taking $a = 3$ and $b = 1$ in Theorem 2.4 we obtain the result.

3. Congruences for $\sum_{k=(p+1)/2}^{\lfloor 3p/4 \rfloor} \binom{4k}{2k} a^k \pmod{p}$

Lemma 3.1. *Let p be an odd prime and $k \in \{1, 2, \dots, \frac{p-1}{2}\}$. Then*

$$\binom{4(\frac{p-1}{2} + k)}{2(\frac{p-1}{2} + k)} \equiv 2 \binom{4k-2}{2k-1} \pmod{p}.$$

Proof. Clearly

$$\begin{aligned} \binom{4(\frac{p-1}{2} + k)}{2(\frac{p-1}{2} + k)} &= \frac{(p+2k)(p+2k+1) \cdots (2p-1) \cdot 2p(2p+1) \cdots (2p+4k-2)}{(p-1)! \cdot p(p+1) \cdots (p+2k-1)} \\ &\equiv \frac{2k(2k+1) \cdots (p-1) \cdot 2 \cdot 1 \cdot 2 \cdots (4k-2)}{(p-1)! \cdot 1 \cdot 2 \cdots (2k-1)} \\ &= \frac{2 \cdot (4k-2)!}{(2k-1)!^2} = 2 \binom{4k-2}{2k-1} \pmod{p}. \end{aligned}$$

Lemma 3.2. *Let p be an odd prime, $P, Q \in \mathbb{Z}_p$ and $PQ \not\equiv 0 \pmod{p}$. Then*

$$U_{\frac{p-1}{2}}(P, Q) \equiv \frac{2P}{Q} \left(\frac{P}{p}\right) \sum_{k=1}^{\lfloor (p+1)/4 \rfloor} \binom{4k-2}{2k-1} \left(\frac{Q}{4P^2}\right)^k \pmod{p}.$$

Proof. By (2.1) and the fact $\binom{\frac{p-1}{2}}{k} \equiv \binom{-\frac{1}{2}}{k} = \frac{1}{(-4)^k} \binom{2k}{k} \pmod{p}$ for $k \in \{0, 1, \dots, \frac{p-1}{2}\}$,

$$\begin{aligned} U_{\frac{p-1}{2}}(P, (P^2 - 4Q)/4) &= \frac{1}{2\sqrt{Q}} \left\{ \left(\frac{P+2\sqrt{Q}}{2}\right)^{\frac{p-1}{2}} - \left(\frac{P-2\sqrt{Q}}{2}\right)^{\frac{p-1}{2}} \right\} \\ &= \frac{1}{2^{\frac{p-1}{2}} \cdot 2\sqrt{Q}} \sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} P^{\frac{p-1}{2}-r} ((2\sqrt{Q})^r - (-2\sqrt{Q})^r) \\ &= \frac{1}{2^{\frac{p-1}{2}} \cdot 2\sqrt{Q}} \sum_{k=1}^{\lfloor \frac{p+1}{4} \rfloor} \binom{\frac{p-1}{2}}{2k-1} P^{\frac{p-1}{2}-(2k-1)} \cdot 2(2\sqrt{Q})^{2k-1} \\ &\equiv \left(\frac{2}{p}\right) \sum_{k=1}^{\lfloor \frac{p+1}{4} \rfloor} \binom{4k-2}{2k-1} \frac{1}{(-4P)^{2k-1}} \left(\frac{P}{p}\right) \cdot 2(4Q)^{k-1} \\ &= -\frac{2P}{Q} \left(\frac{2P}{p}\right) \sum_{k=1}^{\lfloor \frac{p+1}{4} \rfloor} \binom{4k-2}{2k-1} \left(\frac{Q}{4P^2}\right)^k \pmod{p}. \end{aligned}$$

By [5, Lemma 3.1(i)], $U_{\frac{p-1}{2}}(P, Q) \equiv -\left(\frac{2}{p}\right) U_{\frac{p-1}{2}}(P, \frac{P^2-4Q}{4}) \pmod{p}$. Thus the result follows.

Theorem 3.1. *Let p be an odd prime, $c \in \mathbb{Z}_p$ and $c(c^2 + 1) \not\equiv 0 \pmod{p}$. Then*

$$2c \sum_{k=(p+1)/2}^{\lfloor 3p/4 \rfloor} \binom{4k}{2k} \frac{1}{(16(c^2 + 1))^k} \equiv -4c \sum_{k=1}^{\lfloor (p+1)/4 \rfloor} \binom{4k-2}{2k-1} \frac{1}{(16(c^2 + 1))^k}$$

$$\equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ 1 \pmod{p} & \text{if } c \in Q_1(p), \\ -1 \pmod{p} & \text{if } c \in Q_3(p). \end{cases}$$

Proof. By Lemmas 3.1 and 3.2,

$$\begin{aligned} \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \frac{1}{(16(c^2+1))^k} &= \sum_{k=1}^{[(p+1)/4]} \binom{4(\frac{p-1}{2}+k)}{2(\frac{p-1}{2}+k)} \frac{1}{(16(c^2+1))^{\frac{p-1}{2}+k}} \\ &\equiv 2 \left(\frac{c^2+1}{p}\right) \sum_{k=1}^{[\frac{p+1}{4}]} \binom{4k-2}{2k-1} \frac{1}{(16(c^2+1))^k} \\ &\equiv U_{\frac{p-1}{2}}(4(c^2+1), 4(c^2+1)) \pmod{p}. \end{aligned}$$

From (2.1) we see that

$$\begin{aligned} &U_{\frac{p-1}{2}}(4(c^2+1), 4(c^2+1)) \\ &= \frac{1}{4c\sqrt{c^2+1}} (2\sqrt{c^2+1})^{\frac{p-1}{2}} \{(\sqrt{c^2+1}+c)^{\frac{p-1}{2}} - (\sqrt{c^2+1}-c)^{\frac{p-1}{2}}\} \\ &= \begin{cases} \frac{1}{2c} (4c^2+4)^{\frac{p-1}{4}} U_{\frac{p-1}{2}}(2c, -1) & \text{if } 4 \mid p-1, \\ \frac{1}{2c} (4c^2+4)^{\frac{p-3}{4}} V_{\frac{p-1}{2}}(2c, -1) & \text{if } 4 \mid p-3. \end{cases} \end{aligned}$$

If $p \equiv 1 \pmod{4}$, by [5, Theorem 3.1(i)] we have

$$U_{\frac{p-1}{2}}(2c, -1) \equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ (4c^2+4)^{\frac{p-1}{4}} \left(\frac{c+i}{p}\right)_4 i \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = -1. \end{cases}$$

Thus,

$$\begin{aligned} 2c \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \frac{1}{(16(c^2+1))^k} &\equiv (4c^2+4)^{\frac{p-1}{4}} U_{\frac{p-1}{2}}(2c, -1) \\ &\equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ -\left(\frac{c+i}{p}\right)_4 i \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = -1. \end{cases} \end{aligned}$$

If $p \equiv 3 \pmod{4}$, from [5, Corollary 3.1(ii)] we have

$$V_{\frac{p-1}{2}}(2c, -1) \equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ (4c^2+4)^{\frac{p+1}{4}} \left(\frac{c+i}{p}\right)_4 i \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = -1. \end{cases}$$

Thus,

$$2c \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \frac{1}{(16(c^2+1))^k} \equiv (4c^2+4)^{\frac{p-3}{4}} V_{\frac{p-1}{2}}(2c, -1)$$

$$\equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ -\left(\frac{c+i}{p}\right)_4 i \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = -1. \end{cases}$$

Note that $\left(\frac{c+i}{p}\right)_4^2 = \left(\frac{c^2+1}{p}\right)$ by Lemma 2.3. Combining all the above we deduce the result.

Corollary 3.1. *Let p be an odd prime, $c \in \mathbb{Z}_p$ and $c(c^2+1) \not\equiv 0 \pmod{p}$. Then*

$$\begin{aligned} -\frac{2}{c} \left(\frac{2}{p}\right) \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \left(\frac{c^2}{16(c^2+1)}\right)^k &\equiv \frac{4}{c} \left(\frac{2}{p}\right) \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \left(\frac{c^2}{16(c^2+1)}\right)^k \\ &\equiv \begin{cases} 0 \pmod{p} & \text{if } \left(\frac{c^2+1}{p}\right) = 1, \\ 1 \pmod{p} & \text{if } c \in Q_1(p), \\ -1 \pmod{p} & \text{if } c \in Q_3(p). \end{cases} \end{aligned}$$

Proof. Clearly $\left(\frac{c+i}{p}\right)_4 = \left(\frac{i}{p}\right)_4 \left(\frac{1-ci}{p}\right)_4 = \left(\frac{2}{p}\right) \left(\frac{-\frac{1}{c}+i}{p}\right)_4$. If $\left(\frac{2}{p}\right) = 1$, then $-\frac{1}{c} \in Q_r(p)$ if and only if $c \in Q_r(p)$. If $\left(\frac{2}{p}\right) = -1$, then $-\frac{1}{c} \in Q_1(p)$ if and only if $c \in Q_3(p)$, and $-\frac{1}{c} \in Q_3(p)$ if and only if $c \in Q_1(p)$. Thus, replacing c with $-1/c$ in Theorem 3.1 we deduce the result.

Corollary 3.2. *Let p be an odd prime, $c \in \mathbb{Z}_p$ and $\left(\frac{c^2+1}{p}\right) = -1$. Then*

$$\begin{aligned} 4 \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \frac{1}{(16(c^2+1))^k} &\equiv -2 \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \frac{1}{(16(c^2+1))^k} \\ &\equiv \sum_{k=0}^{[p/4]} \binom{4k}{2k} \frac{1}{(16(c^2+1))^k} \pmod{p}. \end{aligned}$$

Proof. This is immediate from Theorem 3.1 and (2.4).

Corollary 3.3. *Let p be an odd prime, $c \in \mathbb{Z}_p$ and $c(c^2+1) \not\equiv 0 \pmod{p}$. Then*

$$\sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \left(\frac{c^2}{16(c^2+1)}\right)^k \equiv -c^2 \left(\frac{2}{p}\right) \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \frac{1}{(16(c^2+1))^k} \pmod{p}$$

and

$$\sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \left(\frac{c^2}{16(c^2+1)}\right)^k \equiv -c^2 \left(\frac{2}{p}\right) \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \frac{1}{(16(c^2+1))^k} \pmod{p}.$$

Proof. This is immediate from Theorem 3.1 and Corollary 3.1.

Corollary 3.4. *Let p be an odd prime. Then*

$$\begin{aligned} 2 \sum_{k=(p+1)/2}^{[3p/4]} \binom{4k}{2k} \frac{1}{32^k} &\equiv -4 \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \frac{1}{32^k} \\ &\equiv \begin{cases} 0 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{8}, \\ 1 \pmod{p} & \text{if } p \equiv \pm 5 \pmod{16}, \\ -1 \pmod{p} & \text{if } p \equiv \pm 3 \pmod{16}. \end{cases} \end{aligned}$$

Proof. Taking $c = 1$ in Theorem 3.1 and then applying (2.7) we obtain the result.

Corollary 3.5. *Let q be a prime of the form $4m + 1$ and $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod{2}$. Suppose that p is an odd prime and $\left(\frac{p}{q}\right) = -1$. Then*

$$(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{4}} \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \left(\frac{b^2}{16q}\right)^k \equiv \mp \frac{b}{4a} \pmod{p} \iff p^{\frac{q-1}{4}} \equiv \pm \frac{b}{a} \pmod{q}.$$

Proof. As $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = -1$ we see that $p \nmid ab$. Taking $c = \frac{a}{b}$ in Corollary 3.2 we see that

$$(3.1) \quad 4 \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \left(\frac{b^2}{16q}\right)^k \equiv \sum_{k=0}^{[p/4]} \binom{4k}{2k} \left(\frac{b^2}{16q}\right)^k \pmod{p}.$$

Now applying Theorem 2.3 we obtain the result.

Corollary 3.6. *Let q be a prime of the form $4m + 1$ and $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod{2}$. Suppose that p is an odd prime and $\left(\frac{p}{q}\right) = -1$. Then*

$$(-1)^{\frac{p^2-1}{8} + \frac{p-1}{2} \cdot \frac{q-1}{4}} \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \left(\frac{a^2}{16q}\right)^k \equiv \mp \frac{a}{4b} \pmod{p} \iff p^{\frac{q-1}{4}} \equiv \pm \frac{a}{b} \pmod{q}.$$

Proof. As $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = -1$ we see that $p \nmid ab$. Taking $c = \frac{a}{b}$ in Corollary 3.2 we see that

$$(3.2) \quad 4 \sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \left(\frac{a^2}{16q}\right)^k \equiv \sum_{k=0}^{[p/4]} \binom{4k}{2k} \left(\frac{a^2}{16q}\right)^k \pmod{p}.$$

Now applying Theorem 2.2 we obtain the result.

Corollary 3.7. *Let p be an odd prime with $p \neq 5$. Then*

$$\sum_{k=1}^{[(p+1)/4]} \binom{4k-2}{2k-1} \frac{1}{20^k} \equiv \begin{cases} 0 \pmod{p} & \text{if } p \equiv \pm 1 \pmod{5}, \\ \pm (-1)^{\frac{p-1}{2}} \frac{p-1}{2} \pmod{p} & \text{if } p \equiv \pm 2 \pmod{5}. \end{cases}$$

Proof. When $p \equiv \pm 1 \pmod{5}$, taking $c = \frac{1}{2}$ in Theorem 3.1 we obtain the result. When $p \equiv \pm 2 \pmod{5}$, taking $q = 5$, $a = 1$ and $b = 2$ in Corollary 3.5 we obtain the result.

References

- [1] B.C. Berndt, R.J. Evans and K.S. Williams, Gauss and Jacobi Sums, Wiley, New York, 1998.
- [2] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed., Springer, New York, 1990.
- [3] F. Lemmermeyer, Reciprocity Laws: From Euler to Eisenstein, Springer, Berlin, 2000.

- [4] Z.H. Sun, Supplements to the theory of quartic residues, *Acta Arith.* **97**(2001), 361-377.
- [5] Z.H. Sun, Values of Lucas sequences modulo primes, *Rocky Mountain J. Math.* **33**(2003), 1123-1145.
- [6] Z.H. Sun, Quartic residues and binary quadratic forms, *J. Number Theory* **113**(2005), 10-52.
- [7] Z.H. Sun, Congruences concerning Lucas sequences, *Int. J. Number Theory* **10**(2014), 793-815.
- [8] 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.