ACTA ARITHMETICA
159.1 (2013)

Congruences for $q^{[p/8]}$ (mod p)

by

Zhi-Hong Sun (Huaian)

1. Introduction. Let $\mathbb{Z}$ be the set of integers, $i = \sqrt{-1}$ and $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. For any positive odd number m and $a \in \mathbb{Z}$ let $\left(\frac{a}{m}\right)$ be the (quadratic) Jacobi symbol. (We also assume $\left(\frac{a}{1}\right) = 1$.) For convenience we also define $\left(\frac{a}{-m}\right) = \left(\frac{a}{m}\right)$. Then for any two odd numbers m and n with $m > 0$ or $n > 0$ we have the following general quadratic reciprocity law: $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right)$.

For $a, b, c, d \in \mathbb{Z}$ with $2 \nmid c$ and $2 \mid d$, one can define the quartic Jacobi symbol $\left(\frac{a+bi}{c+di}\right)_4$ as in [S4]. From [IR] we know that $\overline{\left(\frac{a+bi}{c+di}\right)_4} = \left(\frac{a-bi}{c-di}\right)_4 = \left(\frac{a+bi}{c+di}\right)_4^{-1}$, where $\bar{x}$ means the complex conjugate of x. In Section 2 we list the main properties of the quartic Jacobi symbol. See also [IR], [BEW] and [S2].

For a prime $p = 24k + 1 = c^2 + d^2 = x^2 + 3y^2$ with $k, c, d, x, y \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$, in [HW] and [H], by using cyclotomic numbers and Jacobi sums Hudson and Williams proved that

$$3^{\frac{p-1}{8}} \equiv \begin{cases} \pm 1 \pmod p & \text{if } c \equiv \pm(-1)^{\frac{y}{4}} \pmod 3, \\ \pm\frac{d}{c} \pmod p & \text{if } d \equiv \pm(-1)^{\frac{y}{4}} \pmod 3. \end{cases}$$

Let p be a prime of the form $4k + 1$, $q \in \mathbb{Z}$, $2 \nmid q$ and $p \nmid q$. Suppose that $p = c^2 + d^2 = x^2 + qy^2$ with $c, d, x, y \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. In [S4] and [S5] the author posed many conjectures on $q^{[p/8]} \pmod p$ in terms of c, d, x and y, where $[\cdot]$ is the greatest integer function. For $m, n \in \mathbb{Z}$ let (m, n) be the greatest common divisor of m and n. For $m \in \mathbb{Z}$ with $m = 2^\alpha m_0$ $(2 \nmid m_0)$ we say that $2^\alpha \,\|\, m$. In this paper, by developing the calculation technique of quartic Jacobi symbols, we partially solve many conjectures from [S4] and [S5], and establish new reciprocity laws for quartic and octic residues on the condition that $(c, x + d) = 1$ or $(d, x + c) = 2^\alpha$. For the history of classical reciprocity laws, see [Lem]. Suppose $d = 2^r d_0$, $y = 2^t y_0$

2010 *Mathematics Subject Classification*: Primary 11A15; Secondary 11A07, 11E25.
Key words and phrases: reciprocity law, octic residue, congruence, quartic Jacobi symbol.

DOI: 10.4064/aa159-1-1

© Instytut Matematyczny PAN, 2013

and $d_0\equiv y_0\equiv 1\pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$. We then have the following typical results.

(1.1) If $p\equiv q\equiv 1\pmod 8$, q is a prime and $q=a^2+b^2$ with $a,b\in\mathbb{Z}$, then

$$q^{\frac{p-1}{8}}\equiv(-1)^{\frac d4+\frac{xy}4}\Big(\frac dc\Big)^m\pmod p\iff\Big(\frac{ac+bd}{ac-bd}\Big)^{\frac{q-1}8}\equiv\Big(\frac ba\Big)^m\pmod q.$$

(1.2) If $q\equiv 7\pmod 8$ is a prime, then

$$q^{[p/8]}\equiv\begin{cases}(-1)^{\frac y4}\big(\frac dc\big)^m\pmod p&\text{if }p\equiv 1\pmod 8,\\(-1)^{\frac{x-1}2}\big(\frac dc\big)^m\frac yx\pmod p&\text{if }p\equiv 5\pmod 8\end{cases}$$
$$\iff\Big(\frac{c-di}{c+di}\Big)^{\frac{q+1}8}\equiv i^m\pmod q.$$

(1.3) If $p\equiv 1\pmod 8$, $q=a^2+b^2$, $a,b\in\mathbb{Z}$, $2\mid a$ and $(a,b)=1$, then

$$q^{\frac{p-1}8}\equiv\begin{cases}(-1)^{\frac d4+\frac x4}\big(\frac cd\big)^m\pmod p&\text{if }4\mid a\text{ and }2\mid x,\\(-1)^{\frac d4+\frac y4}\big(\frac cd\big)^m\pmod p&\text{if }4\mid a\text{ and }2\nmid x,\\(-1)^{\frac{b-1}2+\frac d4+\frac{x+2}4}\big(\frac cd\big)^{m-1}\pmod p&\text{if }2\parallel a\text{ and }2\mid x,\\(-1)^{\frac{b-1}2+\frac d4+\frac y4+\frac{x-1}2}\big(\frac cd\big)^{m-1}\pmod p&\text{if }2\parallel a\text{ and }2\nmid x\end{cases}$$
$$\iff\Big(\frac{(ac+bd)/x}{b+ai}\Big)_4=i^m.$$

2. Basic lemmas

Lemma 2.1 ([S4, Proposition 2.1]). *Let $a,b\in\mathbb{Z}$ with $2\nmid a$ and $2\mid b$. Then*

$$\Big(\frac{i}{a+bi}\Big)_4=i^{\frac{a^2+b^2-1}4}=(-1)^{\frac{a^2-1}8}i^{(1-(-1)^{b/2})/2},$$
$$\Big(\frac{1+i}{a+bi}\Big)_4=\begin{cases}i^{((-1)^{(a-1)/2}(a-b)-1)/4}&\textit{if }4\mid b,\\i^{\frac{(-1)^{(a-1)/2}(b-a)-1}4-1}&\textit{if }2\parallel b.\end{cases}$$

Lemma 2.2 ([S4, Proposition 2.2]). *Let $a,b\in\mathbb{Z}$ with $2\nmid a$ and $2\mid b$. Then*

$$\Big(\frac{-1}{a+bi}\Big)_4=(-1)^{\frac b2}\quad\textit{and}\quad\Big(\frac{2}{a+bi}\Big)_4=i^{(-1)^{\frac{a-1}2}\frac b2}.$$

Lemma 2.3 ([S4, Proposition 2.3]). *Let $a,b,c,d\in\mathbb{Z}$ with $2\nmid ac$, $2\mid b$ and $2\mid d$. If $a+bi$ and $c+di$ are relatively prime elements of $\mathbb{Z}[i]$, we have the following general law of quartic reciprocity:*

$$\Big(\frac{a+bi}{c+di}\Big)_4=(-1)^{\frac b2\cdot\frac{c-1}2+\frac d2\cdot\frac{a+b-1}2}\Big(\frac{c+di}{a+bi}\Big)_4.$$

In particular, if $4\mid b$, *then*

$$\Big(\frac{a+bi}{c+di}\Big)_4=(-1)^{\frac{a-1}{2}\cdot\frac{d}{2}}\Big(\frac{c+di}{a+bi}\Big)_4.$$

Lemma 2.4 ([E], [S1, Lemma 2.1]). *Let* $a,b,m\in\mathbb{Z}$ *with* $2\nmid m$ *and suppose* $(m,a^2+b^2)=1$. *Then*

$$\Big(\frac{a+bi}{m}\Big)_4^2=\Big(\frac{a^2+b^2}{m}\Big).$$

Lemma 2.5 ([S3, Lemma 4.3]). *Let* $a,b\in\mathbb{Z}$ *with* $2\nmid a$ *and* $2\mid b$. *For any integer* x *with* $(x,a^2+b^2)=1$ *we have*

$$\Big(\frac{x^2}{a+bi}\Big)_4=\Big(\frac{x}{a^2+b^2}\Big).$$

Lemma 2.6. *Let* $a,b\in\mathbb{Z}$ *with* $2\mid b$ *and* $(a,b)=1$. *Then*

$$\Big(\frac{b}{a+bi}\Big)_4=\begin{cases}1 & \text{if } 4\mid b,\\ (-1)^{\frac{a-1}{2}}i & \text{if } 2\parallel b.\end{cases}$$

Proof. By Lemmas 2.1 and 2.3,

$$\begin{aligned}\Big(\frac{b}{a+bi}\Big)_4&=\Big(\frac{i}{a+bi}\Big)_4\Big(\frac{-bi}{a+bi}\Big)_4=\Big(\frac{i}{a+bi}\Big)_4\Big(\frac{a}{a+bi}\Big)_4\\&=\Big(\frac{i}{a+bi}\Big)_4\cdot(-1)^{\frac{a-1}{2}\cdot\frac{b}{2}}\Big(\frac{a+bi}{a}\Big)_4=(-1)^{\frac{a-1}{2}\cdot\frac{b}{2}}\Big(\frac{i}{a+bi}\Big)_4\Big(\frac{i}{a}\Big)_4\\&=(-1)^{\frac{a-1}{2}\cdot\frac{b}{2}}\cdot(-1)^{\frac{a^2-1}{8}}i^{\frac{1-(-1)^{b/2}}{2}}\cdot(-1)^{\frac{a^2-1}{8}}\\&=\begin{cases}1 & \text{if } 4\mid b,\\ (-1)^{\frac{a-1}{2}}i & \text{if } 2\parallel b.\end{cases}\end{aligned}$$

Thus the lemma is proved.

For a given odd prime p let $\mathbb{Z}_p$ denote the set of those rational numbers whose denominator is not divisible by p. Following [S1, S2] we define

$$Q_r(p)=\Big\{k\;\Big|\;k\in\mathbb{Z}_p,\ \Big(\frac{k+i}{p}\Big)_4=i^r\Big\}\quad\text{for } r=0,1,2,3.$$

Lemma 2.7 ([S1, Theorem 2.3]). *Let* p *be an odd prime,* $r\in\{0,1,2,3\}$, $k\in\mathbb{Z}_p$ *and* $k^2+1\not\equiv 0\pmod p$.

(i) *If* $p\equiv 1\pmod 4$ *and* $t^2\equiv -1\pmod p$ *with* $t\in\mathbb{Z}_p$, *then* $k\in Q_r(p)$ *if and only if* $\big(\frac{k+t}{k-t}\big)^{(p-1)/4}\equiv t^r\pmod p$.

(ii) *If* $p\equiv 3\pmod 4$, *then* $k\in Q_r(p)$ *if and only if* $\big(\frac{k-i}{k+i}\big)^{(p+1)/4}\equiv i^r\pmod p$.

Lemma 2.8. *Let* p *be an odd prime,* $k\in\mathbb{Z}_p$ *and* $n^2\equiv k^2+1\pmod p$ *with* $n\in\mathbb{Z}_p$ *and* $n(n+1)\not\equiv 0\pmod p$. *Then* $\big(\frac{k+i}{p}\big)_4=\big(\frac{n(n+1)}{p}\big)$.

Proof. For $k \equiv 0 \pmod p$ we have $\big(\frac{k+i}{p}\big)_4 = \big(\frac{i}{p}\big)_4 = (-1)^{\frac{p^2-1}{8}} = \big(\frac{1\cdot 2}{p}\big)$. So the result is true. Now assume $k \not\equiv 0 \pmod p$. Then $\big(\frac{n-1}{p}\big)\big(\frac{n+1}{p}\big) = \big(\frac{n^2-1}{p}\big) = \big(\frac{k^2}{p}\big) = 1$ and so $\big(\frac{n-1}{p}\big) = \big(\frac{n+1}{p}\big)$. By Lemma 2.4, $\big(\frac{k+i}{p}\big)_4^2 = \big(\frac{k^2+1}{p}\big) = 1$ and so $\big(\frac{k+i}{p}\big)_4 = \pm 1$. By [S1, Theorem 2.4], $\big(\frac{k+i}{p}\big)_4 = 1 \iff k \in Q_0(p) \iff \big(\frac{n(n+1)}{p}\big) = 1$. Hence $\big(\frac{k+i}{p}\big)_4 = \big(\frac{n(n+1)}{p}\big)$.

Lemma 2.9. *Suppose $c, d, m, x \in \mathbb{Z}$, $2 \nmid m$, $x^2 \equiv c^2 + d^2 \pmod m$ and $(m, x(x+d)) = 1$. Then*

$$\Big(\frac{c+di}{m}\Big)_4 = \Big(\frac{x(x+d)}{m}\Big).$$

Proof. Suppose that p is a prime divisor of m. Then $p \nmid x(x+d)$. If $p \nmid d$, then $\big(\frac{x}{d}\big)^2 \equiv \big(\frac{c}{d}\big)^2 + 1 \pmod p$. Thus, applying Lemma 2.8 we obtain

$$\Big(\frac{c+di}{p}\Big)_4 = \Big(\frac{\frac{c}{d}+i}{p}\Big)_4 = \Big(\frac{\frac{x}{d}(1+\frac{x}{d})}{p}\Big) = \Big(\frac{x(x+d)}{p}\Big).$$

When $p \mid d$, we have $p \nmid c$ and so

$$\Big(\frac{c+di}{p}\Big)_4 = \Big(\frac{c}{p}\Big)_4 = 1 = \Big(\frac{x^2}{p}\Big) = \Big(\frac{x(x+d)}{p}\Big).$$

Hence,

$$\Big(\frac{c+di}{m}\Big)_4 = \prod_{p\mid m}\Big(\frac{c+di}{p}\Big)_4 = \prod_{p\mid m}\Big(\frac{x(x+d)}{p}\Big) = \Big(\frac{x(x+d)}{m}\Big),$$

where in the products p runs over all prime divisors of m. The proof is now complete.

Lemma 2.10. *Suppose $c, d, x, y, q \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $2 \mid d$, $c^2 + d^2 = x^2 + qy^2$, $y = 2^t y_0$, $y_0 \equiv 1 \pmod 4$ and $(y_0, x(x+d)) = 1$.*

(i) *If $2 \mid x$, then $\big(\frac{y}{c^2+(x+d)^2}\big) = (-1)^{\frac{y-1}{4}}\big(\frac{y^{-1}}{c+di}\big)_4$.*

(ii) *If $2 \nmid x$, then $\big(\frac{y}{(c^2+(x+d)^2)/2}\big) = (-1)^{\frac{c^2-(x+d)^2}{8}t} i^{\frac{d}{2}t}\big(\frac{y^{-1}}{c+di}\big)_4$.*

Proof. Since $c^2 + (x+d)^2 = 2x(x+d) + qy^2$ we see that $(c^2 + (x+d)^2, y_0) = 1$. For even x we have $2 \nmid qy$, $c^2 + (x+d)^2 \equiv 1 \pmod 4$ and so

$$\Big(\frac{y}{c^2+(x+d)^2}\Big) = \Big(\frac{c^2+(x+d)^2}{y}\Big) = \Big(\frac{2x(x+d)}{y}\Big)$$
$$= (-1)^{\frac{y-1}{4}}\Big(\frac{x(x+d)}{y}\Big).$$

For odd x we have $c^2+(x+d)^2\equiv 2 \pmod 8$ and so

$$\begin{aligned}&\Big(\frac{y}{(c^2+(x+d)^2)/2}\Big)\\ &\quad=\Big(\frac{2^ty_0}{(c^2+(x+d)^2)/2}\Big)=(-1)^{\frac{(c^2+(x+d)^2)/2-1}{4}t}\Big(\frac{(c^2+(x+d)^2)/2}{y_0}\Big)\\ &\quad=(-1)^{\frac{c^2-(x+d)^2}{8}t}\Big(\frac{2}{y_0}\Big)\Big(\frac{2x(x+d)+qy^2}{y_0}\Big)=(-1)^{\frac{c^2-(x+d)^2}{8}t}\Big(\frac{x(x+d)}{y_0}\Big).\end{aligned}$$

Since $x^2\equiv c^2+d^2 \pmod{|y_0|}$, using Lemmas 2.9, 2.3 and 2.2 we find that

$$\begin{aligned}\Big(\frac{x(x+d)}{y_0}\Big)&=\Big(\frac{c+di}{y_0}\Big)_4=\Big(\frac{y_0}{c+di}\Big)_4=\Big(\frac{y_0^{-1}}{c+di}\Big)_4=\Big(\frac{2^ty^{-1}}{c+di}\Big)_4\\ &=i^{\frac d2 t}\Big(\frac{y^{-1}}{c+di}\Big)_4.\end{aligned}$$

Now combining all the above we obtain the result.

Lemma 2.11. *Let p be a prime of the form $4k+1$ and $p=c^2+d^2$ with $c,d\in\mathbb{Z}$. Suppose $q\in\mathbb{Z}$, $p\nmid q$ and $p=x^2+qy^2$ with $x,y\in\mathbb{Z}$. Then $(x+d,c^2)=(x+d,qy^2)$ and*

$$(qy^2,c^2+(x+d)^2)=(x+d,c^2)\Big(2,x+d+\frac{c^2}{(x+d,c^2)}\Big).$$

Proof. Since $(x,y)^2\mid p$ we see that $(x,y)=1$. If $p\mid x$, then $p\mid qy^2$ and so $p\mid y$. This contradicts the fact $(x,y)=1$. Hence $p\nmid x$. Since $(x,c^2+(x+d)^2)=(x,c^2+d^2)=(x,p)=1$ and $qy^2=d^2-x^2+c^2=c^2+(x+d)^2-2x(x+d)$, we observe that $(x+d,c^2)=(x+d,x^2-d^2+qy^2)=(x+d,qy^2)$ and

$$\begin{aligned}(qy^2,c^2+(x+d)^2)&=(2x(x+d),c^2+(x+d)^2)=(2(x+d),c^2+(x+d)^2)\\ &=(x+d,c^2)\Big(2\frac{x+d}{(x+d,c^2)},\frac{c^2}{(x+d,c^2)}+(x+d)\frac{x+d}{(x+d,c^2)}\Big)\\ &=(x+d,c^2)\Big(2,\frac{c^2}{(x+d,c^2)}+(x+d)\frac{x+d}{(x+d,c^2)}\Big)\\ &=(x+d,c^2)\Big(2,\frac{c^2}{(x+d,c^2)}+(x+d)\Big).\end{aligned}$$

Thus the lemma is proved.

Lemma 2.12. *Let p be a prime of the form $4k+1$ and $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $2\nmid c$. Suppose $q\in\mathbb{Z}$, $p\nmid q$, $p=x^2+qy^2$, $x,y\in\mathbb{Z}$ and $\big(\frac{x/y}{c+di}\big)_4=(-1)^{[\frac p8]+n}i^k$. Then*

$$q^{[p/8]}\equiv\begin{cases}(-1)^n\big(\frac dc\big)^k \pmod p & \text{if } p\equiv 1\pmod 8,\\ (-1)^n\big(\frac dc\big)^k\frac yx \pmod p & \text{if } p\equiv 5\pmod 8.\end{cases}$$

Proof. It is clear that $(c,d)=1$, $p\nmid y$ and so

$$\Big(\frac xy\Big)^{\frac{p-1}4}\equiv\Big(\frac{x/y}{c+di}\Big)_4=(-1)^{[\frac p8]+n}i^k\equiv(-1)^{[\frac p8]+n}\Big(\frac dc\Big)^k\pmod{c+di}.$$

Thus $\big(\frac xy\big)^{\frac{p-1}4}\equiv(-1)^{[\frac p8]+n}\big(\frac dc\big)^k\pmod p$ and so

$$\begin{aligned}q^{[\frac p8]}&=(-1)^{[\frac p8]}(-q)^{[\frac p8]}\equiv(-1)^{[\frac p8]}\Big(\frac xy\Big)^{2[\frac p8]}\\&\equiv\begin{cases}(-1)^n\big(\frac dc\big)^k\pmod p&\text{if }8\mid p-1,\\(-1)^n\big(\frac dc\big)^k\frac yx\pmod p&\text{if }8\mid p-5.\end{cases}\end{aligned}$$

This proves the lemma.

3. Determination of $q^{[p/8]}\pmod p$ using $\big(\frac{c+(x+d)i}{q}\big)_4$ or $\big(\frac{d-(x+c)i}{q}\big)_4$

THEOREM 3.1. *Let p be a prime of the form $4k+1$, $q\in\mathbb Z$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+qy^2$ with $c,d,x,y\in\mathbb Z$, $c\equiv1\pmod 4$, $d=2^rd_0$, $d_0\equiv1\pmod 4$, $(c,x+d)=1$, $2\mid x$, $y\equiv1\pmod 4$ and $\big(\frac{c/(x+d)+i}{q}\big)_4=i^k$.*

(i) *If $p\equiv1\pmod 8$, then*

$$q^{\frac{p-1}8}\equiv\begin{cases}(-1)^{\frac{q-1}8+\frac d4+\frac x4}\big(\frac dc\big)^k\pmod p&\text{if }q\equiv1\pmod 8,\\(-1)^{\frac{q-5}8+\frac d4+\frac{x-2}4}\big(\frac dc\big)^{k+1}\pmod p&\text{if }q\equiv5\pmod 8.\end{cases}$$

(ii) *If $p\equiv5\pmod 8$, then*

$$q^{\frac{p-5}8}\equiv\begin{cases}(-1)^{\frac{q-1}8+\frac{x-2}4}\big(\frac dc\big)^{k+1}\frac yx\pmod p&\text{if }q\equiv1\pmod 8,\\(-1)^{\frac{q-5}8+\frac x4}\big(\frac dc\big)^k\frac yx\pmod p&\text{if }q\equiv5\pmod 8.\end{cases}$$

Proof. Suppose $2^m\parallel(x+d)$ and $x=2^sx_0(2\nmid x_0)$. Since $2\mid x$ we have $q\equiv1\pmod 4$. As $(c,x+d)=1$, by Lemma 2.11 we have $(qy,x+d)=1$ and $(qy^2,c^2+(x+d)^2)=1$. Note that $(x,y)^2\mid p$. We also have $(x,y)=1$. Using Lemmas 2.1–2.5, 2.10 and the fact that $\big(\frac an\big)_4=1$ for $a,n\in\mathbb Z$ with $2\nmid n$ and $(a,n)=1$, we see that

$$\begin{aligned}i^k&=\Big(\frac{c+(x+d)i}{q}\Big)_4=\Big(\frac{qy^2}{c+(x+d)i}\Big)_4\Big(\frac{y^2}{c+(x+d)i}\Big)_4\\&=\Big(\frac{-2x(x+d)+c^2+(x+d)^2}{c+(x+d)i}\Big)_4\Big(\frac{y}{c^2+(x+d)^2}\Big)\\&=\Big(\frac{-2x(x+d)}{c+(x+d)i}\Big)_4(-1)^{\frac{y-1}4}\Big(\frac{y^{-1}}{c+di}\Big)_4\end{aligned}$$

and

$$\begin{aligned}\Big(\frac{-2x(x+d)}{c+(x+d)i}\Big)_4 &= \Big(\frac{2}{c+(x+d)i}\Big)_4^{m+s+1}\Big(\frac{-x_0(x+d)/2^m}{c+(x+d)i}\Big)_4\\ &= i^{\frac{x+d}{2}(m+s+1)}(-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}}\Big(\frac{c+(x+d)i}{x_0(x+d)/2^m}\Big)_4\\ &= (-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}}i^{\frac{x+d}{2}(m+s+1)}\Big(\frac{c+di}{x_0}\Big)_4\Big(\frac{c}{(x+d)/2^m}\Big)_4\\ &= (-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}}i^{\frac{x+d}{2}(m+s+1)}(-1)^{\frac{x_0-1}{2}\cdot\frac{d}{2}}\Big(\frac{x_0}{c+di}\Big)_4\\ &= (-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}}i^{\frac{x+d}{2}(m+s+1)}(-1)^{\frac{x_0-1}{2}\cdot\frac{d}{2}}\Big(\frac{2}{c+di}\Big)_4^{-s}\Big(\frac{x}{c+di}\Big)_4\\ &= (-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}}i^{\frac{x+d}{2}(m+s+1)}(-1)^{\frac{x_0-1}{2}\cdot\frac{d}{2}}i^{-\frac{d}{2}s}\Big(\frac{x}{c+di}\Big)_4.\end{aligned}$$

Therefore,

$$i^k = (-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}+\frac{x_0-1}{2}\cdot\frac{d}{2}+\frac{y-1}{4}}i^{\frac{x+d}{2}(m+s+1)-\frac{d}{2}s}\Big(\frac{x/y}{c+di}\Big)_4.$$

Observe that

$$(-1)^{\frac{y-1}{4}} = (-1)^{\frac{q(y^2-1)}{8}} = (-1)^{\frac{p-q-x^2}{8}} = \begin{cases}(-1)^{\frac{p-q-4}{8}} & \text{if } 2\,\|\, x,\\ (-1)^{\frac{p-q}{8}} & \text{if } 4\mid x\end{cases}$$

and

$$\begin{aligned}i^{\frac{d}{2}s-\frac{x+d}{2}(m+s+1)} &= i^{-\frac{x+d}{2}(m+1)-\frac{x}{2}s} = (-1)^{\frac{(m+1)(x+d)}{4}}i^{-\frac{x}{2}s}\\ &= \begin{cases}(-1)^{\frac{(m+1)(x+d)}{4}}\cdot(-1)^{\frac{x+2}{4}}i & \text{if } 2\,\|\, x,\\ (-1)^{\frac{(m+1)(x+d)}{4}} & \text{if } 4\mid x.\end{cases}\end{aligned}$$

From the above we obtain

$$\begin{aligned}(3.1)\qquad &\Big(\frac{x/y}{c+di}\Big)_4\\ &= \begin{cases}(-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}+\frac{x-2}{4}\cdot\frac{d}{2}+\frac{p-q-4}{8}}\cdot(-1)^{\frac{(m+1)(x+d)}{4}+\frac{x+2}{4}}i^{k+1} & \text{if } 2\,\|\, x,\\ (-1)^{\frac{x_0(x+d)/2^m+1}{2}\cdot\frac{x+d}{2}+\frac{x_0-1}{2}\cdot\frac{d}{2}+\frac{p-q}{8}}\cdot(-1)^{\frac{(m+1)(x+d)}{4}}i^{k} & \text{if } 4\mid x.\end{cases}\end{aligned}$$

When $4\mid(x+d)$, we have $(-1)^{\frac{(m+1)(x+d)}{4}} = (-1)^{\frac{x+d}{4}}$. For $p\equiv q\equiv 1\ (\mathrm{mod}\ 8)$ we have $4\mid d$, $4\mid x$ and $4\mid(x+d)$. For $p\equiv 1\ (\mathrm{mod}\ 8)$ and $q\equiv 5\ (\mathrm{mod}\ 8)$, we have $2\,\|\, x$, $4\mid d$, $2\,\|\,(x+d)$, $m=1$ and $(-1)^{\frac{x_0(x+d)/2+1}{2}} = (-1)^{\frac{d}{4}x_0+\frac{x_0^2+1}{2}} = (-1)^{\frac{d}{4}+1}$. For $p\equiv 5\ (\mathrm{mod}\ 8)$ and $q\equiv 1\ (\mathrm{mod}\ 8)$, we have $2\,\|\, d$, $2\,\|\, x$, $4\mid(x+d)$ and $m\ge 2$. For $p\equiv q\equiv 5\ (\mathrm{mod}\ 8)$, we have $2\,\|\, d$, $4\mid x$,

$2\,\|\,(x+d)$, $m=1$ and $(-1)^{\frac{x_0(x+d)/2+1}{2}}=(-1)^{\frac{x}{4}x_0+\frac{d_0x_0+1}{2}}=(-1)^{\frac{x}{4}+\frac{x_0+1}{2}}$. Now, from the above and (3.1) we deduce that

$$\Big(\frac{x/y}{c+di}\Big)_4 = \begin{cases} (-1)^{\frac{p-1}{8}+\frac{q-1}{8}+\frac d4+\frac x4}i^k & \text{if } p\equiv q\equiv 1 \pmod 8,\\ (-1)^{\frac{p-1}{8}+\frac{q-5}{8}+\frac d4+\frac{x-2}{4}}i^{k+1} & \text{if } p\equiv 1 \pmod 8 \text{ and } q\equiv 5 \pmod 8,\\ (-1)^{\frac{p-5}{8}+\frac{q-1}{8}+\frac{x-2}{4}}i^{k+1} & \text{if } p\equiv 5 \pmod 8 \text{ and } q\equiv 1 \pmod 8,\\ (-1)^{\frac{p-5}{8}+\frac{q-5}{8}+\frac x4}i^k & \text{if } p\equiv q\equiv 5 \pmod 8. \end{cases}$$

This together with Lemma 2.12 yields the result.

LEMMA 3.1. *Let p be a prime of the form $4k+1$, $q\in\mathbb Z$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+qy^2$ with $c,d,x,y\in\mathbb Z$, $c\equiv 1 \pmod 4$, $d=2^rd_0$, $y=2^ty_0$, $d_0\equiv y_0\equiv 1 \pmod 4$, $(c,x+d)=1$ and $2\nmid x$. Assume that $\big(\frac{c/(x+d)+i}{q}\big)_4=i^k$. Then*

$$\Big(\frac{x/y}{c+di}\Big)_4 = \begin{cases} (-1)^{[\frac p8]+\frac{q-(\frac{-1}{q})}{4}\cdot\frac{x-1}{2}+\frac{q-1}{2}\cdot\frac d4}\, i^{\frac{1-(\frac{-1}{q})q}{4}+\frac{(-1)^{\frac{x-1}{2}}x-c}{4}+k} & \textit{if } 8\,|\,(p-1),\\ (-1)^{[\frac p8]+\frac{q+1}{2}+\frac{x+1}{2}(1+\frac{q-(\frac{-1}{q})}{4})}\, i^{\frac{1-(\frac{-1}{q})q}{4}+\frac{(-1)^{\frac{x-1}{2}}x-c}{4}+k-1} & \textit{if } 8\,|\,(p-5). \end{cases}$$

Proof. As $(c,x+d)=1$, by Lemma 2.11 we have $(qy_0,x+d)=1$ and $(qy_0^2,c^2+(x+d)^2)=1$. Note that $(x,y)^2\,|\,p$. We also have $(x,y)=1$. It is easily seen that

$$c+(x+d)i=i^{\frac{1\mp1}{2}}(1+i)\Big(\frac{x+d\pm c}{2}+\frac{\pm(x+d)-c}{2}i\Big)$$

and so

$$\Big(\frac{x+d\pm c}{2}\Big)^2+\Big(\frac{\pm(x+d)-c}{2}\Big)^2=\frac{c^2+(x+d)^2}{2}.$$

Set $\varepsilon=(-1)^{\frac{p-1}{4}+\frac{x-1}{2}}$. Since $4\,|\,d \iff 8\,|\,(p-1)$ we see that $x+d\equiv\varepsilon \pmod 4$ and $4\,|\,(\varepsilon(x+d)-c)$. Using Lemmas 2.1–2.5, 2.10 and the above we see that

$$\begin{aligned} i^k &= \Big(\frac{c+(x+d)i}{q}\Big)_4=\Big(\frac iq\Big)_4^{\frac{1-\varepsilon}{2}}\Big(\frac{1+i}{q}\Big)_4\Big(\frac{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}{q}\Big)_4\\ &=(-1)^{\frac{q-(\frac{-1}{q})}{4}\cdot\frac{1-\varepsilon}{2}}\, i^{\frac{(\frac{-1}{q})q-1}{4}}(-1)^{\frac{q-1}{2}\cdot\frac{\varepsilon(x+d)-c}{4}}\Big(\frac{q}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4 \end{aligned}$$

and

$$\begin{aligned}
&\Big(\frac{q}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4=\Big(\frac{qy^2}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{y^2}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\\
&\quad=\Big(\frac{c^2+(x+d)^2-2x(x+d)}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{y}{(\frac{x+d+\varepsilon c}{2})^2+(\frac{\varepsilon(x+d)-c}{2})^2}\Big)\\
&\quad=\Big(\frac{2}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{-x(x+d)}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{y}{(c^2+(x+d)^2)/2}\Big)\\
&\quad=i^{(-1)^{((x+d+\varepsilon c)/2-1)/2}\frac{\varepsilon(x+d)-c}{4}}(-1)^{\frac{x(x+d)+1}{2}\cdot\frac{\varepsilon(x+d)-c}{4}}\Big(\frac{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}{x(x+d)}\Big)_4\\
&\qquad\times(-1)^{\frac{c^2-(x+d)^2}{8}t}i^{\frac{d}{2}t}\Big(\frac{y^{-1}}{c+di}\Big)_4.
\end{aligned}$$

Obviously we have $i^{(-1)^ab}=(-1)^{ab}i^b$ and $(-1)^{\frac{x+d+\varepsilon c-2}{4}}=(-1)^{\frac{\varepsilon(x+d)+c-2\varepsilon}{4}}=(-1)^{\frac{\varepsilon(x+d)-c}{4}+\frac{1-\varepsilon}{2}}$ and so

$$\begin{aligned}
i^{(-1)^{\frac{x+d+\varepsilon c-2}{4}}\frac{\varepsilon(x+d)-c}{4}}&=(-1)^{(\frac{\varepsilon(x+d)-c}{4}+\frac{1-\varepsilon}{2})\frac{\varepsilon(x+d)-c}{4}}i^{\frac{\varepsilon(x+d)-c}{4}}\\
&=(-1)^{\frac{1+\varepsilon}{2}\cdot\frac{\varepsilon(x+d)-c}{4}}i^{\frac{\varepsilon(x+d)-c}{4}}.
\end{aligned}$$

Also, we have $(-1)^{\frac{x(x+d)+1}{2}}=(-1)^{\frac{x^2-1}{2}+\frac{d}{2}x+1}=(-1)^{\frac{d}{2}+1}$ and $(-1)^{\frac{c^2-(x+d)^2}{8}}=(-1)^{\frac{\varepsilon(x+d)-c}{4}}$. Thus,

$$\begin{aligned}
&i^{(-1)^{\frac{(x+d+\varepsilon c)/2-1}{2}}\frac{\varepsilon(x+d)-c}{4}}(-1)^{\frac{x(x+d)+1}{2}\cdot\frac{\varepsilon(x+d)-c}{4}}\cdot(-1)^{\frac{c^2-(x+d)^2}{8}t}i^{\frac{d}{2}t}\\
&\quad=(-1)^{\frac{1+\varepsilon}{2}\cdot\frac{\varepsilon(x+d)-c}{4}}i^{\frac{\varepsilon(x+d)-c}{4}}(-1)^{(\frac{d}{2}+1)\frac{\varepsilon(x+d)-c}{4}}\cdot(-1)^{\frac{\varepsilon(x+d)-c}{4}t}i^{\frac{d}{2}t}\\
&\quad=(-1)^{(\frac{1-\varepsilon}{2}+\frac{d}{2}+t)\frac{\varepsilon(x+d)-c}{4}}i^{\frac{\varepsilon(x+d)-c}{4}+\frac{d}{2}t}.
\end{aligned}$$

It is easily seen that

$$\begin{aligned}
&\Big(\frac{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}{x(x+d)}\Big)_4\\
&\quad=\Big(\frac{x+d+\varepsilon c+(\varepsilon(x+d)-c)i}{x}\Big)_4\Big(\frac{x+d+\varepsilon c+(\varepsilon(x+d)-c)i}{x+d}\Big)_4\\
&\quad=\Big(\frac{d+\varepsilon c+(\varepsilon d-c)i}{x}\Big)_4\Big(\frac{\varepsilon c-ci}{x+d}\Big)_4=\Big(\frac{(\varepsilon-i)(c+di)}{x}\Big)_4\Big(\frac{\varepsilon-i}{x+d}\Big)_4\\
&\quad=\Big(\frac{\varepsilon-i}{x(x+d)}\Big)_4\Big(\frac{c+di}{x}\Big)_4=\Big(\frac{i^{\frac{5+\varepsilon}{2}}(1+i)}{x(x+d)}\Big)_4\Big(\frac{c+di}{x}\Big)_4
\end{aligned}$$

$$= \Big(\frac{i}{x(x+d)}\Big)_4^{\frac{5+\varepsilon}{2}}\Big(\frac{1+i}{x(x+d)}\Big)_4(-1)^{\frac{x-1}{2}\cdot\frac d2}\Big(\frac{x}{c+di}\Big)_4$$
$$= (-1)^{\frac{(x(d+x))^2-1}{8}\cdot\frac{5+\varepsilon}{2}} i^{\frac{(-1)^{d/2}x(x+d)-1}{4}}(-1)^{\frac{x-1}{2}\cdot\frac d2}\Big(\frac{x}{c+di}\Big)_4.$$

Now combining all the above we deduce that

$$\begin{aligned} i^k &= (-1)^{\frac{q-(\frac{-1}{q})}{4}\cdot\frac{1-\varepsilon}{2}+\frac{q-1}{2}\cdot\frac{\varepsilon(x+d)-c}{4}} i^{\frac{(\frac{-1}{q})q-1}{4}} \\ &\quad\times(-1)^{(\frac{1-\varepsilon}{2}+\frac d2+t)\frac{\varepsilon(x+d)-c}{4}} i^{\frac{\varepsilon(x+d)-c}{4}+\frac d2 t} \\ &\quad\times(-1)^{\frac{(x(d+x))^2-1}{8}\cdot\frac{5+\varepsilon}{2}+\frac{x-1}{2}\cdot\frac d2} i^{\frac{(-1)^{d/2}x(x+d)-1}{4}}\Big(\frac{x/y}{c+di}\Big)_4. \end{aligned} \tag{3.2}$$

It is clear that

$$(-1)^{\frac{\varepsilon(x+d)-c}{4}} = (-1)^{\frac{\varepsilon(x+d)-c}{4}\cdot\frac{\varepsilon(x+d)+c}{2}} = (-1)^{\frac{(x+d)^2-c^2}{8}} = (-1)^{\frac{2d^2+2dx-qy^2}{8}}$$
$$= \begin{cases} (-1)^{\frac d4} & \text{if } 8\mid(p-1) \text{ and so } d\equiv y\equiv 0 \pmod 4,\\ (-1)^{\frac{2+x-q}{2}} = (-1)^{\frac{q-1}{2}+\frac{1-\varepsilon}{2}} & \text{if } 8\mid(p-5) \text{ and so } d\equiv y\equiv 2 \pmod 4)\end{cases}$$

and

$$(-1)^{\frac{x^2(x+d)^2-1}{8}} = (-1)^{\frac{(-1)^{d/2}x(x+d)-1}{4}} = (-1)^{\frac{(-1)^{d/2}(dx+1)-1}{4}}$$
$$= \begin{cases} (-1)^{\frac d4} & \text{if } 8\mid(p-1) \text{ and so } 4\mid d,\\ (-1)^{\frac{d_0x+1}{2}} = \varepsilon & \text{if } 8\mid(p-5) \text{ and so } d\equiv y\equiv 2 \pmod 4).\end{cases}$$

Since $x+d\equiv\varepsilon \pmod 4$ and $(-1)^{\frac d2}=(-1)^{\frac{p-1}{4}}$ we also have

$$i^{\frac{\varepsilon(x+d)-c}{4}+\frac{(-1)^{d/2}x(x+d)-1}{4}+\frac d2 t}$$
$$\begin{aligned} &= (-1)^{\frac{(-1)^{d/2}x(x+d)-1}{4}} i^{\frac{\varepsilon(x+d)-c}{4}-\frac{(-1)^{(p-1)/4}x(x+d)-1}{4}+\frac d2 t} \\ &= (-1)^{\frac{(-1)^{d/2}x(x+d)-1}{4}} i^{\varepsilon(x+d)\frac{1-(-1)^{(x-1)/2}x}{4}-\frac{c-1}{4}+\frac d2 t} \\ &= (-1)^{\frac{(-1)^{d/2}x(x+d)-1}{4}+\frac{c-1}{4}} i^{\frac{1-(-1)^{(x-1)/2}x}{4}+\frac{c-1}{4}+\frac d2 t} \\ &= \begin{cases} (-1)^{\frac d4+\frac{c-1}{4}+\frac d4 t} i^{\frac{c-(-1)^{(x-1)/2}x}{4}} & \text{if } 8\mid(p-1),\\ \varepsilon(-1)^{\frac{c-1}{4}} i^{\frac{c-(-1)^{(x-1)/2}x}{4}+d_0} & \\ \quad = (-1)^{\frac{1-\varepsilon}{2}+\frac{c-1}{4}} i^{\frac{c-(-1)^{(x-1)/2}x}{4}+1} & \text{if } 8\mid(p-5).\end{cases} \end{aligned}$$

Note that $(-1)^{\frac{c-1}{4}} = (-1)^{\frac{c^2-1}{8}} = (-1)^{\frac{p-1-d^2}{8}} = (-1)^{[\frac p8]}$. From the above and (3.2) we deduce the result.

THEOREM 3.2. *Let p be a prime of the form $4k+1$, $q\in\mathbb{Z}$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+qy^2$ with $c,d,x,y\in\mathbb{Z}$, $c\equiv 1 \pmod 4$, $d=2^rd_0$, $y=2^ty_0$, $d_0\equiv y_0\equiv 1 \pmod 4$, $(c,x+d)=1$, $2\nmid x$ and $\left(\frac{c/(x+d)+i}{q}\right)_4=i^k$.*

(i) *If $p\equiv 1 \pmod 8$, then*

$$q^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac{q-1}{8}+\frac d4+\frac y4}\left(\frac dc\right)^k \pmod p & \text{if } q\equiv 1 \pmod 8,\\ (-1)^{\frac{q+5}{8}+\frac{x-1}{2}+\frac y4}\left(\frac dc\right)^{k-1} \pmod p & \text{if } q\equiv 3 \pmod 8,\\ (-1)^{\frac{q-5}{8}+\frac d4+\frac{x-1}{2}+\frac y4}\left(\frac dc\right)^{k-1} \pmod p & \text{if } q\equiv 5 \pmod 8,\\ (-1)^{\frac{q+1}{8}+\frac y4}\left(\frac dc\right)^k \pmod p & \text{if } q\equiv 7 \pmod 8.\end{cases}$$

(ii) *If $p\equiv 5 \pmod 8$, then*

$$q^{\frac{p-5}{8}}\equiv\begin{cases}(-1)^{\frac{q-1}{8}+\frac{x-1}{2}}\left(\frac dc\right)^{k-1}\frac yx \pmod p & \text{if } q\equiv 1 \pmod 8,\\ (-1)^{\frac{q+5}{8}}\left(\frac dc\right)^{k-1}\frac yx \pmod p & \text{if } q\equiv 3 \pmod 8,\\ (-1)^{\frac{q+3}{8}}\left(\frac dc\right)^{k}\frac yx \pmod p & \text{if } q\equiv 5 \pmod 8,\\ (-1)^{\frac{q+1}{8}+\frac{x-1}{2}}\left(\frac dc\right)^k\frac yx \pmod p & \text{if } q\equiv 7 \pmod 8.\end{cases}$$

Proof. Suppose $c\neq(-1)^{(x-1)/2}x$ and $2^m\parallel(c-(-1)^{(x-1)/2}x)$. Then $m\geq 2$ and $2^{m+1}\parallel(c-x)(c+x)$. As $d^2-qy^2=-(c-x)(c+x)$ we see that $2^{m+1}\parallel(d^2-qy^2)$. We first assume $p\equiv 1 \pmod 8$. Since $4\mid d$ and $4\mid y$ we have $m\geq 3$ and $2^{m-3}\parallel\left(\left(\frac d4\right)^2-q\left(\frac y4\right)^2\right)$. Thus,

$$i^{\frac{(-1)^{(x-1)/2}x-c}{4}}=(-1)^{\frac{(-1)^{(x-1)/2}x-c}{8}}=(-1)^{2^{m-3}}=(-1)^{(\frac d4)^2-q(\frac y4)^2}=(-1)^{\frac d4+\frac y4}.$$

This is also true when $c=(-1)^{(x-1)/2}x$. From the above and Lemma 3.1 we deduce that

$$\left(\frac{x/y}{c+di}\right)_4=\begin{cases}(-1)^{\frac{p-1}{8}+\frac{q-(\frac{-1}{q})}{8}+\frac{q+1}{2}\cdot\frac d4+\frac y4}i^k & \text{if } q\equiv\pm 1 \pmod 8,\\ (-1)^{\frac{p-1}{8}+\frac{q-5(\frac{-1}{q})}{8}+\frac{q+1}{2}\cdot\frac d4+\frac{x-1}{2}+\frac y4}i^{k-1} & \text{if } q\equiv\pm 3 \pmod 8.\end{cases}$$

Now applying Lemma 2.12 we deduce (i).

Suppose $p\equiv 5 \pmod 8$. As $qy^2-d^2=4(qy_0^2-d_0^2)$ we get $2^{m-1}\parallel(qy_0^2-d_0^2)$. Clearly $qy_0^2-d_0^2\equiv q-1 \pmod 8$. Thus

$$q\equiv\begin{cases}3 \pmod 4 & \text{if } m=2,\\ 5 \pmod 8 & \text{if } m=3,\\ 1 \pmod 8 & \text{if } m>3.\end{cases}$$

For $q\equiv 1 \pmod 4$ we have $8\mid(c-(-1)^{\frac{x-1}{2}}x)$ and

$$i^{\frac{(-1)^{(x-1)/2}x-c}{4}}=(-1)^{\frac{(-1)^{(x-1)/2}x-c}{8}}=(-1)^{2^{m-3}}=(-1)^{\frac{q-1}{4}}.$$

This is also true when $c=(-1)^{(x-1)/2}x$. Thus, using Lemma 3.1 we deduce that

$$\Big(\frac{x/y}{c+di}\Big)_4=\begin{cases}(-1)^{\frac{p-5}{8}+\frac{q-1}{8}+\frac{x-1}{2}}i^{k-1}&\text{if } q\equiv 1 \pmod 8,\\ (-1)^{\frac{p-5}{8}+\frac{q+3}{8}}i^k&\text{if } q\equiv 5 \pmod 8).\end{cases}$$

Now applying Lemma 2.12 we deduce the result in the case $p\equiv 5 \pmod 8$ and $q\equiv 1 \pmod 4$. For $q\equiv 3 \pmod 4$ we have $2^2\parallel (c-(-1)^{(x-1)/2}x)$ and so

$$\begin{aligned}q\equiv qy_0^2&=2c\cdot\frac{c-(-1)^{\frac{x-1}{2}}x}{4}-4\Big(\frac{c-(-1)^{\frac{x-1}{2}}x}{4}\Big)^2+d_0^2\\ &\equiv 2\cdot\frac{c-(-1)^{\frac{x-1}{2}}x}{4}-4+1 \pmod 8).\end{aligned}$$

Thus, $\frac{(-1)^{(x-1)/2}x-c}{4}\equiv -\frac{q+3}{2} \pmod 4$ and so $i^{\frac{(-1)^{(x-1)/2}x-c}{4}}=i^{-\frac{q+3}{2}}$. Using Lemma 3.1 we see that

$$\Big(\frac{x/y}{c+di}\Big)_4=\begin{cases}(-1)^{\frac{p-5}{8}+\frac{q+5}{8}}i^{k-1}&\text{if } q\equiv 3 \pmod 8,\\ (-1)^{\frac{p-5}{8}+\frac{q+1}{8}+\frac{x-1}{2}}i^k&\text{if } q\equiv 7 \pmod 8).\end{cases}$$

Now applying Lemma 2.12 we obtain the result in the case $p\equiv 5 \pmod 8$ and $q\equiv 3 \pmod 4$.

Summarizing all the above we prove the theorem.

REMARK 3.1. We note that the k in Theorems 3.1–3.2 depends only on $\frac{c}{x+d} \pmod q$.

COROLLARY 3.1. *Let $p\equiv 1,49 \pmod{60}$ be a prime and so $p=c^2+d^2=x^2+15y^2$ with $c,d,x,y\in\mathbb{Z}$. Suppose $c\equiv 1 \pmod 4$, $d=2^rd_0$, $y=2^ty_0$, $d_0\equiv y_0\equiv 1 \pmod 4$ and $(c,x+d)=1$.*

(i) *If $p\equiv 1 \pmod 8$, then*

$$15^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac{y}{4}} \pmod p & \textit{if } \frac{c}{x+d}\equiv 0,\pm1 \pmod{15},\\ -(-1)^{\frac{y}{4}} \pmod p & \textit{if } \frac{c}{x+d}\equiv \pm4 \pmod{15},\\ \pm(-1)^{\frac{y}{4}}\frac{c}{d} \pmod p & \textit{if } \frac{c}{x+d}\equiv \pm5,\pm6 \pmod{15}.\end{cases}$$

(ii) *If $p\equiv 5 \pmod 8$, then*

$$15^{\frac{p-5}{8}}\equiv\begin{cases}(-1)^{\frac{x-1}{2}}\frac{y}{x} \pmod p & \textit{if } \frac{c}{x+d}\equiv 0,\pm1 \pmod{15},\\ -(-1)^{\frac{x-1}{2}}\frac{y}{x} \pmod p & \textit{if } \frac{c}{x+d}\equiv \pm4 \pmod{15},\\ \mp(-1)^{\frac{x-1}{2}}\frac{dy}{cx} \pmod p & \textit{if } \frac{c}{x+d}\equiv \pm5,\pm6 \pmod{15}.\end{cases}$$

Proof. Clearly x is odd. Thus, putting $q=15$ in Theorem 3.2 and noting that (see [S1, Example 2.1])

$$\Big(\frac{n+i}{15}\Big)_4=\Big(\frac{n+i}{3}\Big)_4\Big(\frac{n+i}{5}\Big)_4=\begin{cases}1 & \text{if } n\equiv 0,\pm 1\ (\mathrm{mod}\ 15),\\ -1 & \text{if } n\equiv \pm 4\ (\mathrm{mod}\ 15),\\ \mp i & \text{if } n\equiv \pm 5,\pm 6\ (\mathrm{mod}\ 15),\end{cases}$$

we deduce the result.

For example, since $61=5^2+(-6)^2=(-1)^2+15\cdot 2^2$, $(5,-1-6)=1$ and $\frac{5}{-1-6}\equiv -5\ (\mathrm{mod}\ 15)$ we have

$$15^{\frac{61-5}{8}}=15^7\equiv(-1)^{\frac{-1-1}{2}}\frac{-6\cdot 2}{5\cdot(-1)}\equiv-\frac{12}{5}\equiv 22\ (\mathrm{mod}\ 61).$$

THEOREM 3.3. *Let p be a prime of the form $4k+1$, $q\in\mathbb{Z}$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+qy^2$ with $c,d,x,y\in\mathbb{Z}$, $c\equiv 1\ (\mathrm{mod}\ 4)$, $d=2^rd_0$, $y=2^ty_0$, $d_0\equiv y_0\equiv 1\ (\mathrm{mod}\ 4)$, $(d_0,x+c)=1$ and $\big(\frac{d/(x+c)-i}{q}\big)_4=i^k$.*

(i) *If $p\equiv 1\ (\mathrm{mod}\ 8)$, then*

$$q^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac d4+[\frac x4]}\big(\frac dc\big)^k\ (\mathrm{mod}\ p) & \text{if } 2\mid x,\\ (-1)^{\frac{q^2-1}{8}\cdot\frac{x+1}{2}+\frac{q+1}{2}\cdot\frac d4+\frac y4}\big(\frac dc\big)^k\ (\mathrm{mod}\ p) & \text{if } 2\nmid x.\end{cases}$$

(ii) *If $p\equiv 5\ (\mathrm{mod}\ 8)$, then*

$$q^{\frac{p-5}{8}}\equiv\begin{cases}(-1)^{[\frac{x+2}{4}]}\big(\frac dc\big)^{k-1}\frac yx\ (\mathrm{mod}\ p) & \text{if } 2\mid x \text{ and so } q\equiv 1\ (\mathrm{mod}\ 4),\\ -(-1)^{\frac{q+3}{4}\cdot\frac{x+1}{2}}\big(\frac dc\big)^{k-1}\frac yx\ (\mathrm{mod}\ p) & \text{if } 2\nmid x \text{ and } q\equiv 1\ (\mathrm{mod}\ 4),\\ -(-1)^{\frac{q-3}{4}\cdot\frac{x+1}{2}}\big(\frac dc\big)^{k}\frac yx\ (\mathrm{mod}\ p) & \text{if } q\equiv 3\ (\mathrm{mod}\ 4).\end{cases}$$

Proof. Suppose $x=2^sx_0(2\nmid x_0)$ and $2^m\parallel(x+c)$. As $(x+c,d_0)=1$, by Lemma 2.11 we have $(qy_0,x+c)=1$ and $(qy_0^2,(x+c)^2+d^2)=1$. Note that $(x,y)^2\mid p$. We also have $(x,y)=1$. If $m<r$, using Lemmas 2.1–2.5 and the fact $\big(\frac aq\big)_4=1$ for $a\in\mathbb{Z}$ with $(a,q)=1$ we see that

$$\begin{aligned}(3.3)\quad \Big(\frac{d-(x+c)i}{q}\Big)_4&=\Big(\frac{-2^m}{q}\Big)_4\Big(\frac iq\Big)_4\Big(\frac{\frac{x+c}{2^m}+\frac{d}{2^m}i}{q}\Big)_4\\ &=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}\Big(\frac{q}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\\ &=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}\Big(\frac{qy^2}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\Big(\frac{y^2}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\\ &=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}\Big(\frac{c^2+d^2-x^2}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\Big(\frac{y}{\frac{(x+c)^2+d^2}{2^{2m}}}\Big).\end{aligned}$$

If $m=r$, then clearly

$$\text{(3.4)}\qquad \Big(\frac{d-(x+c)i}{q}\Big)_4=\Big(\frac{-2^r}{q}\Big)_4\Big(\frac{i}{q}\Big)_4\Big(\frac{\frac{x+c}{2^r}+\frac{d}{2^r}i}{q}\Big)_4 =\Big(\frac{2}{q}\Big)\Big(\frac{1+i}{q}\Big)_4\Big(\frac{\frac{x+c+d}{2^{r+1}}-\frac{x+c-d}{2^{r+1}}i}{q}\Big)_4.$$

If $m>r$, using Lemmas 2.1–2.5 we see that

$$\begin{aligned}\text{(3.5)}\qquad \Big(\frac{d-(x+c)i}{q}\Big)_4&=\Big(\frac{\frac{d}{2^r}-\frac{x+c}{2^r}i}{q}\Big)_4=(-1)^{\frac{q-1}{2}\cdot\frac{x+c}{2^{r+1}}}\Big(\frac{q}{\frac{d}{2^r}-\frac{x+c}{2^r}i}\Big)_4\\ &=(-1)^{\frac{q-1}{2}\cdot\frac{x+c}{2^{r+1}}}\Big(\frac{qy^2}{\frac{d}{2^r}-\frac{x+c}{2^r}i}\Big)_4\Big(\frac{y^2}{\frac{d}{2^r}-\frac{x+c}{2^r}i}\Big)_4\\ &=(-1)^{\frac{q-1}{2}\cdot\frac{x+c}{2^{r+1}}}\Big(\frac{(x+c)^2+d^2-2x(x+c)}{\frac{d}{2^r}-\frac{x+c}{2^r}i}\Big)_4\Big(\frac{y}{(\frac{d}{2^r})^2+(\frac{x+c}{2^r})^2}\Big)\\ &=(-1)^{\frac{q-1}{2}\cdot 2^{m-r-1}}\Big(\frac{-2x(x+c)}{\frac{d}{2^r}-\frac{x+c}{2^r}i}\Big)_4\Big(\frac{y}{((x+c)^2+d^2)/2^{2r}}\Big).\end{aligned}$$

By considering the three cases $m<r$, $m=r$ and $m>r$ and applying lemmas from Section 2, one may deduce the result after doing horrible long calculations. We only prove the result in the case $m<r$ (including $2\mid x$ and $4\mid(x-1)$). The remaining two cases can be proved similarly. For the details in the cases $m=r$ and $m>r$, see the fourth version of the author's "Quartic, octic residues and binary quadratic forms" at arXiv:1108.3027.

Now suppose $m<r$. Then

$$\begin{aligned}&\Big(\frac{c^2+d^2-x^2}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\\ &\quad=\Big(\frac{-2x(x+c)+d^2+(x+c)^2}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4=\Big(\frac{-2x(x+c)}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\\ &\quad=\Big(\frac{2^{m+s+1}}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\Big(\frac{-x_0}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\Big(\frac{(x+c)/2^m}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4\\ &\quad=i^{(-1)^{(\frac{x+c}{2^m}-1)/2}\frac{d}{2^{m+1}}(m+s+1)}(-1)^{(\frac{x_0+1}{2}+\frac{\frac{x+c}{2^m}-1}{2})\frac{d}{2^{m+1}}}\\ &\qquad\times\Big(\frac{\frac{x+c}{2^m}+\frac{d}{2^m}i}{x_0}\Big)_4\Big(\frac{\frac{x+c}{2^m}+\frac{d}{2^m}i}{\frac{x+c}{2^m}}\Big)_4\\ &\quad=i^{(-1)^{(\frac{x+c}{2^m}-1)/2}\frac{d}{2^{m+1}}(m+s+1)}\cdot(-1)^{\frac{\frac{x+c}{2^m}+x_0}{2}\cdot\frac{d}{2^{m+1}}}\Big(\frac{x+c+di}{x_0}\Big)_4\Big(\frac{i}{\frac{x+c}{2^m}}\Big)_4.\end{aligned}$$

Clearly $\big(\frac{i}{\frac{x+c}{2^m}}\big)_4=\big(\frac{2}{\frac{x+c}{2^m}}\big)$ and

$$\Big(\frac{x+c+di}{x_0}\Big)_4=\Big(\frac{c+di}{x_0}\Big)_4=(-1)^{\frac d2\cdot\frac{x_0-1}{2}}\Big(\frac{x_0}{c+di}\Big)_4$$
$$=(-1)^{\frac d2\cdot\frac{x_0-1}{2}}\Big(\frac{2}{c+di}\Big)_4^{-s}\Big(\frac{x}{c+di}\Big)_4$$
$$=(-1)^{\frac d2\cdot\frac{x_0-1}{2}}i^{-\frac d2 s}\Big(\frac{x}{c+di}\Big)_4.$$

Thus,

$$\Big(\frac{c^2+d^2-x^2}{\frac{x+c}{2^m}+\frac{d}{2^m}i}\Big)_4=(-1)^{\frac{(x+c)/2^m+x_0}{2}\cdot\frac{d}{2^{m+1}}+\frac{x_0-1}{2}\cdot\frac d2}$$
$$\times\, i^{(-1)^{((x+c)/2^m-1)/2}\frac{d}{2^{m+1}}(m+s+1)-\frac d2 s}\Big(\frac{2}{\frac{x+c}{2^m}}\Big)\Big(\frac{x}{c+di}\Big)_4.$$

As $((x+c)^2+d^2)/2^{2m}\equiv 1+4d/2^{m+1}\pmod 8$ and $x^2\equiv c^2+d^2\pmod{|y_0|}$, using Lemma 2.9 we see that

$$\Big(\frac{y}{((x+c)^2+d^2)/2^{2m}}\Big)=\Big(\frac{2^ty_0}{((x+c)^2+d^2)/2^{2m}}\Big)$$
$$=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{(x+c)^2+d^2}{y_0}\Big)=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{2x(x+c)}{y_0}\Big)$$
$$=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{2}{y_0}\Big)\Big(\frac{-d+ci}{y_0}\Big)_4=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{-i}{y_0}\Big)_4\Big(\frac{-d+ci}{y_0}\Big)_4$$
$$=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{c+di}{y_0}\Big)_4=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{y_0}{c+di}\Big)_4=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{y_0^{-1}}{c+di}\Big)_4$$
$$=(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{2^ty^{-1}}{c+di}\Big)_4=(-1)^{\frac{d}{2^{m+1}}t}i^{\frac d2 t}\Big(\frac{y^{-1}}{c+di}\Big)_4.$$

From the above and (3.3) we deduce that

$$\Big(\frac{d-(x+c)i}{q}\Big)_4 \tag{3.6}$$
$$=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}\cdot(-1)^{\frac{(x+c)/2^m+x_0}{2}\cdot\frac{d}{2^{m+1}}+\frac{x_0-1}{2}\cdot\frac d2}\Big(\frac{2}{\frac{x+c}{2^m}}\Big)$$
$$\times\, i^{(-1)^{((x+c)/2^m-1)/2}\frac{d}{2^{m+1}}(m+s+1)-\frac d2 s}(-1)^{\frac{d}{2^{m+1}}t}i^{\frac d2 t}\Big(\frac{x/y}{c+di}\Big)_4.$$

If $m=0$, then $2\nmid(x+c)$, $2\mid x$, $2\nmid y$ and so $q\equiv p\equiv 1\pmod 4$. Thus, from (3.6) we infer that

$$\Big(\frac{d-(x+c)i}{q}\Big)_4=(-1)^{\frac{q-1}{4}+(\frac x2+1)\frac d2}i^{\frac d2}\Big(\frac{2}{x+c}\Big)\Big(\frac{x/y}{c+di}\Big)_4.$$

Since $\big(\frac{d-(x+c)i}{q}\big)_4=i^k$, $(-1)^{\frac{q-1}{4}}=(-1)^{\frac{qy^2-1}{4}}=(-1)^{\frac{c^2-1+d^2-x^2}{4}}=(-1)^{\frac{d^2-x^2}{4}}$ $=(-1)^{\frac x2-\frac d2}$ and

$$\Big(\frac{2}{x+c}\Big)=(-1)^{\frac{(x+c)^2-1}{8}}=(-1)^{\frac{c^2-1}{8}+\frac{(x/2)(x/2+c)}{2}}=(-1)^{\frac{p-1-d^2}{8}+\frac{(x/2)(x/2+1)}{2}}$$
$$=(-1)^{[\frac p8]+[\frac{x+2}{4}]},$$

from the above and the fact $d_0\equiv 1\pmod 4$ we derive that

$$\begin{aligned}\Big(\frac{x/y}{c+di}\Big)_4&=(-1)^{\frac x2-\frac d2+(\frac x2+1)\frac d2}\cdot(-1)^{[\frac p8]+[\frac{x+2}{4}]}i^{k-\frac d2}\\&=\begin{cases}(-1)^{[\frac p8]+\frac x2-[\frac{x+2}{4}]+\frac d4}i^k=(-1)^{[\frac p8]+\frac d4+[\frac x4]}i^k&\text{if } p\equiv 1\pmod 8,\\(-1)^{[\frac p8]+[\frac{x+2}{4}]}i^{k-1}&\text{if } p\equiv 5\pmod 8).\end{cases}\end{aligned}$$

Now applying Lemma 2.12 we obtain the result in the case $m=0$.

If $m=1<r$, then $x\equiv 1\pmod 4$, $s=0$, $4\mid d$ and $p\equiv 1\pmod 8$. Since $p\equiv x^2\equiv 1\pmod 8$ we have $8\mid qy^2$ and so $4\mid y$. Thus,

$$\begin{aligned}1-c\cdot\frac{x+c}{2}&\equiv\Big(\frac{x+c}{2}\Big)^2-c\cdot\frac{x+c}{2}=4\Big(\Big(\frac d4\Big)^2-q\Big(\frac y4\Big)^2\Big)\\&\equiv 4\Big(\frac d4+\frac y4\Big)=d+y\pmod 8\end{aligned}$$

and so $\frac{x+c}{2}\equiv c-d-y\pmod 8$. Therefore $\frac{x+c}{2}\equiv 1\pmod 4$ and

$$\Big(\frac{2}{\frac{x+c}{2}}\Big)=\Big(\frac{2}{c-d-y}\Big)=(-1)^{\frac{c-1}{4}+\frac d4+\frac y4}=(-1)^{\frac{c^2-1}{8}+\frac d4+\frac y4}=(-1)^{\frac{p-1}{8}+\frac d4+\frac y4}.$$

Hence, from (3.6) we deduce that

$$\begin{aligned}&\Big(\frac{d-(x+c)i}{q}\Big)_4\\&\quad=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac d4}\cdot(-1)^{\frac{\frac{x+c}{2}+x}{2}\cdot\frac d4}\cdot(-1)^{\frac d4}\cdot(-1)^{\frac{p-1}{8}+\frac d4+\frac y4}\cdot\Big(\frac{x/y}{c+di}\Big)_4\\&\quad=(-1)^{\frac{p-1}{8}+\frac{q^2-1}{8}+\frac{q+1}{2}\cdot\frac d4+\frac y4}\Big(\frac{x/y}{c+di}\Big)_4.\end{aligned}$$

Since $\big(\frac{d-(x+c)i}{q}\big)_4=i^k$, we get $\big(\frac{x/y}{c+di}\big)_4=(-1)^{\frac{p-1}{8}+\frac{q^2-1}{8}+\frac{q+1}{2}\cdot\frac d4+\frac y4}i^k$. Now applying Lemma 2.12 we obtain $q^{\frac{p-1}{8}}\equiv(-1)^{\frac{q^2-1}{8}+\frac{q+1}{2}\cdot\frac d4+\frac y4}\big(\frac dc\big)^k\pmod p$ as asserted.

Now we assume $2\le m<r$. Then $x\equiv 3\pmod 4$, $s=0$, $8\mid d$ and so $p\equiv 1\pmod 8$. Since $qy^2=d^2-(x+c)^2+2c(x+c)$ we see that

$$q\frac{y^2}{2^{m+1}}=2^{2r-m-1}d_0^2-2^{m-1}\Big(\frac{x+c}{2^m}\Big)^2+c\frac{x+c}{2^m}.$$

As $m\ge 2$ and $2r\ge 2(m+1)\ge m+4$, we must have $2^{m+1}\,\|\,y^2$, $2\mid (m+1)$, $t=\frac{m+1}{2}$ and $q\equiv -2^{m-1}+c\frac{x+c}{2^m}\pmod 8$. Thus $m\ge 3$, $\frac{x+c}{2^m}\equiv c(2^{m-1}+q)\equiv c-1+2^{m-1}+q\pmod 8$ and so $\frac{x+c}{2^m}\equiv q\pmod 4$. Therefore, by (3.6) we have

$$\begin{aligned}\Big(\frac{d-(x+c)i}{q}\Big)_4 \\ &=(-1)^{\frac{q^2-1}{8}+\frac{d}{2^{m+1}}\cdot\frac{m+1}{2}}\Big(\frac{2}{c-1+2^{m-1}+q}\Big)(-1)^{\frac{d}{2^{m+1}}t}\Big(\frac{x/y}{c+di}\Big)_4\\ &=(-1)^{\frac{c-1}{4}+2^{m-3}}\Big(\frac{x/y}{c+di}\Big)_4.\end{aligned}$$

Note that $(-1)^{\frac{c-1}{4}}=(-1)^{\frac{c^2-1}{8}}=(-1)^{\frac{p-1}{8}}$, $\big(\frac{d-(x+c)i}{q}\big)_4=i^k$ and

$$(-1)^{2^{m-3}}=\begin{cases}1 & \text{if } m>3\\ -1 & \text{if } m=3\end{cases}=\begin{cases}1 & \text{if } t>2\\ -1 & \text{if } t=2\end{cases}=(-1)^{\frac{y}{4}}.$$

We then get $\big(\frac{x/y}{c+di}\big)_4=(-1)^{\frac{p-1}{8}+\frac{y}{4}}i^k$. Recall that $8\mid d$. Applying Lemma 2.12 we obtain $q^{\frac{p-1}{8}}\equiv(-1)^{\frac{y}{4}}\big(\frac{d}{c}\big)^k=(-1)^{\frac{q+1}{2}\cdot\frac{d}{4}+\frac{y}{4}}\big(\frac{d}{c}\big)^k\pmod p$. This proves the result in the case $2\le m<r$.

Summarizing all the above we obtain the theorem.

4. New reciprocity laws for quartic and octic residues

THEOREM 4.1. *Let p and q be primes such that $p\equiv 1\pmod 4$ and $q\equiv 3\pmod 4$. Suppose $p=c^2+d^2=x^2+qy^2$, $c,d,x,y\in\mathbb{Z}$, $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$, $d_0\equiv y_0\equiv 1\pmod 4$ and $\big(\frac{c-di}{x}\big)^{\frac{q+1}{4}}\equiv i^m\pmod q$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$. Then*

$$q^{[p/8]}\equiv\begin{cases}(-1)^{\frac{y}{4}+\frac{q+1}{4}\cdot\frac{x-1}{2}}\big(\frac{d}{c}\big)^m \pmod p & \text{if } p\equiv 1\pmod 8,\\ (-1)^{\frac{q-3}{4}\cdot\frac{x-1}{2}}\big(\frac{d}{c}\big)^m\frac{y}{x}\pmod p & \text{if } p\equiv 5\pmod 8.\end{cases}$$

Proof. Since $p\equiv 1\pmod 4$ and $q\equiv 3\pmod 4$ we see that $q\nmid x$ and x is odd. We first assume $(c,x+d)=1$. By Lemma 2.11 we have $(q,(x+d)(c^2+(x+d)^2))=1$. It is easily seen that $\frac{c/(x+d)-i}{c/(x+d)+i}=\frac{c-(x+d)i}{c+(x+d)i}\equiv\frac{c-di}{ix}\pmod q$. Thus, for $k=0,1,2,3$, using Lemma 2.7 we get

$$\begin{aligned}\Big(\frac{c+(x+d)i}{q}\Big)_4=i^k \\ &\Leftrightarrow\ \frac{c}{x+d}\in Q_k(q)\Leftrightarrow\Big(\frac{\frac{c}{x+d}-i}{\frac{c}{x+d}+i}\Big)^{\frac{q+1}{4}}\equiv i^k\pmod q\\ &\Leftrightarrow\ \Big(\frac{c-di}{ix}\Big)^{\frac{q+1}{4}}\equiv i^k\pmod q\Leftrightarrow\Big(\frac{c-di}{x}\Big)^{\frac{q+1}{4}}\equiv i^{\frac{q+1}{4}+k}\pmod q.\end{aligned}$$

Since $\left(\frac{c-di}{x}\right)^{\frac{q+1}{4}}\equiv i^m \pmod q$, from the above we deduce that

$$\left(\frac{c+(x+d)i}{q}\right)_4=i^{m-\frac{q+1}{4}}=\begin{cases}(-1)^{\frac{q+5}{8}}i^{m+1} & \text{if } q\equiv 3 \pmod 8,\\ (-1)^{\frac{q+1}{8}}i^m & \text{if } q\equiv 7 \pmod 8).\end{cases}$$

Now, applying Theorem 3.2 we derive the result.

Now we assume $(d_0,x+c)=1$. By Lemma 2.11, $(q,x+c)=(q,d^2+(x+c)^2)=1$. It is easily seen that $\frac{d+(x+c)i}{d-(x+c)i}\equiv\frac{c-di}{-x} \pmod q$. Thus, for $k=0,1,2,3$, using Lemma 2.7 we get

$$\begin{aligned}&\left(\frac{d-(x+c)i}{q}\right)_4=i^k\\ &\quad\Leftrightarrow\ -\frac{d}{x+c}\in Q_k(q)\ \Leftrightarrow\ \left(\frac{-\frac{d}{x+c}-i}{-\frac{d}{x+c}+i}\right)^{\frac{q+1}{4}}\equiv i^k \pmod q\\ &\quad\Leftrightarrow\ \left(\frac{d+(x+c)i}{d-(x+c)i}\right)^{\frac{q+1}{4}}\equiv i^k \pmod q\Leftrightarrow\left(\frac{c-di}{-x}\right)^{\frac{q+1}{4}}\equiv i^k \pmod q\\ &\quad\Leftrightarrow\ \left(\frac{c-di}{x}\right)^{\frac{q+1}{4}}\equiv i^{\frac{q+1}{2}+k} \pmod q.\end{aligned}$$

Since $\left(\frac{c-di}{x}\right)^{\frac{q+1}{4}}\equiv i^m \pmod q$, from the above we deduce that $\left(\frac{d-(x+c)i}{q}\right)_4=i^{m-\frac{q+1}{2}}=(-1)^{\frac{q+1}{4}}i^m$. Now applying Theorem 3.3 we obtain the result. The proof is now complete.

Corollary 4.1. *Let $p\equiv 1 \pmod 4$ and $q\equiv 3 \pmod 8$ be primes such that $p=c^2+d^2=x^2+qy^2$ with $c,d,x,y\in\mathbb{Z}$ and $q\mid cd$. Suppose $c\equiv 1 \pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1 \pmod 4$. Assume $(c,d+x)=1$ or $(d_0,x+c)=1$.*

(i) *If $p\equiv 1 \pmod 8$, then*

$$q^{\frac{p-1}{8}}\equiv\begin{cases}\pm(-1)^{\frac{x-1}{2}+\frac{y}{4}} \pmod p & \text{if } x\equiv\pm c \pmod q,\\ \mp(-1)^{\frac{q-3}{8}+\frac{x-1}{2}+\frac{y}{4}}\frac{d}{c} \pmod p & \text{if } x\equiv\pm d \pmod q.\end{cases}$$

(ii) *If $p\equiv 5 \pmod 8$, then*

$$q^{\frac{p-5}{8}}\equiv\begin{cases}\pm\frac{y}{x} \pmod p & \text{if } x\equiv\pm c \pmod q,\\ \mp(-1)^{\frac{q-3}{8}}\frac{dy}{cx} \pmod p & \text{if } x\equiv\pm d \pmod q.\end{cases}$$

Proof. If $x\equiv\pm c \pmod q$, then $q\mid d$ and so $\left(\frac{c-di}{x}\right)^{\frac{q+1}{4}}\equiv(\pm1)^{\frac{q+1}{4}}=\pm1 \pmod q$. If $x\equiv\pm d \pmod q$, then $q\mid c$ and so $\left(\frac{c-di}{x}\right)^{\frac{q+1}{4}}\equiv(\mp i)^{\frac{q+1}{4}}=\mp(-1)^{\frac{q-3}{8}}i \pmod q$. Now applying Theorem 4.1 we deduce the result.

We note that Corollary 4.1 partially settles [S5, Conjecture 4.3].

For example, let p be a prime such that $p\equiv 13\pmod{24}$ and hence $p=c^2+d^2=x^2+3y^2$ with $c,d,x,y\in\mathbb{Z}$. Suppose $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1\pmod 4$. If $(c,x+d)=1$ or $(d_0,x+c)=1$, then

$$3^{\frac{p-5}{8}}\equiv\begin{cases}\pm\frac{y}{x}\pmod p & \text{if } x\equiv\pm c\pmod 3,\\ \mp\frac{dy}{cx}\pmod p & \text{if } x\equiv\pm d\pmod 3.\end{cases}$$

This partially solves [S4, Conjecture 9.1].

Theorem 4.2. *Let p and q be primes such that $p\equiv 1\pmod 4$, $q\equiv 7\pmod 8$, $p=c^2+d^2=x^2+qy^2$, $c,d,x,y\in\mathbb{Z}$, $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1\pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$. Suppose $\left(\frac{c-di}{c+di}\right)^{\frac{q+1}{8}}\equiv i^m\pmod q$. Then*

$$q^{[p/8]}\equiv\begin{cases}(-1)^{\frac{y}{4}}\left(\frac{d}{c}\right)^m\pmod p & \text{if } p\equiv 1\pmod 8,\\ (-1)^{\frac{x-1}{2}}\left(\frac{d}{c}\right)^m\frac{y}{x}\pmod p & \text{if } p\equiv 5\pmod 8.\end{cases}$$

Proof. Observe that

$$\left(\frac{c-di}{c+di}\right)^{\frac{q+1}{8}}=\frac{(c-di)^{\frac{q+1}{4}}}{(c^2+d^2)^{\frac{q+1}{8}}}=\frac{(c-di)^{\frac{q+1}{4}}}{(x^2+qy^2)^{\frac{q+1}{8}}}\equiv\left(\frac{c-di}{x}\right)^{\frac{q+1}{4}}\pmod q.$$

The result follows from Theorem 4.1.

We note that if $q\nmid d$, then the m in Theorem 4.2 depends only on $\frac{c}{d}\pmod q$.

Corollary 4.2. *Let $p\equiv 1\pmod 4$ and $q\equiv 7\pmod 8$ be primes such that $p=c^2+d^2=x^2+qy^2$ with $c,d,x,y\in\mathbb{Z}$ and $q\mid cd(c^2-d^2)$. Suppose $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1\pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$.*

(i) *If $p\equiv 1\pmod 8$, then*

$$q^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac{q+1}{8}+\frac{y}{4}}\pmod p & \text{if } q\mid c,\\ (-1)^{\frac{y}{4}}\pmod p & \text{if } q\mid d,\\ \pm(-1)^{\frac{q+9}{16}+\frac{y}{4}}\frac{d}{c}\pmod p & \text{if } 16\mid(q-7) \text{ and } c\equiv\pm d\pmod q,\\ (-1)^{\frac{q+1}{16}+\frac{y}{4}}\pmod p & \text{if } 16\mid(q-15) \text{ and } c\equiv\pm d\pmod q.\end{cases}$$

(ii) *If $p\equiv 5\pmod 8$, then*

$$q^{\frac{p-5}{8}}\equiv\begin{cases}(-1)^{\frac{q+1}{8}+\frac{x-1}{2}}\frac{y}{x}\pmod p & \text{if } q\mid c,\\ (-1)^{\frac{x-1}{2}}\frac{y}{x}\pmod p & \text{if } q\mid d,\\ \pm(-1)^{\frac{q+9}{16}+\frac{x-1}{2}}\frac{dy}{cx}\pmod p & \text{if } 16\mid(q-7) \text{ and } c\equiv\pm d\pmod q,\\ (-1)^{\frac{q+1}{16}+\frac{x-1}{2}}\frac{y}{x}\pmod p & \text{if } 16\mid(q-15) \text{ and } c\equiv\pm d\pmod q.\end{cases}$$

Proof. Clearly

$$\frac{c-di}{c+di}\equiv\begin{cases}-1 \pmod q & \text{if } q\mid c,\\ 1 \pmod q & \text{if } q\mid d,\\ -i \pmod q & \text{if } c\equiv d \pmod q,\\ i \pmod q & \text{if } c\equiv -d \pmod q.\end{cases}$$

Thus the result follows from Theorem 4.2.

THEOREM 4.3. *Let p and q be distinct primes of the form $4k+1$, $p=c^2+d^2=x^2+qy^2$, $q=a^2+b^2$, $a,b,c,d,x,y\in\mathbb{Z}$, $c\equiv 1 \pmod 4$, $d=2^r d_0$, $y=2^t y_0$ and $d_0\equiv y_0\equiv 1 \pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$. Suppose $\left(\frac{ac+bd}{ax}\right)^{\frac{q-1}{4}}\equiv\left(\frac{b}{a}\right)^m \pmod q$.*

(i) *If $p\equiv 1 \pmod 8$, then*

$$q^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac d4+[\frac{x+2}{4}]}\left(\frac dc\right)^m \pmod p & \text{if } 2\mid x,\\ (-1)^{\frac{q-1}{4}\cdot\frac{x-1}{2}+\frac d4+\frac y4}\left(\frac dc\right)^m \pmod p & \text{if } 2\nmid x.\end{cases}$$

(ii) *If $p\equiv 5 \pmod 8$, then*

$$q^{\frac{p-5}{8}}\equiv\begin{cases}(-1)^{[\frac x4]}\left(\frac dc\right)^{m+1}\frac yx \pmod p & \text{if } 2\mid x,\\ -(-1)^{\frac{q+3}{4}\cdot\frac{x-1}{2}}\left(\frac dc\right)^{m+1}\frac yx \pmod p & \text{if } 2\nmid x.\end{cases}$$

Proof. Clearly $q\nmid x$. We first assume $(c,x+d)=1$. By Lemma 2.11, $(q,(x+d)(c^2+(x+d)^2))=1$. It is easily seen that $\frac{ac+b(x+d)}{ac-b(x+d)}\equiv\frac{ac+bd}{ax}\cdot\frac ba \pmod q$. Thus, for $k=0,1,2,3$, using Lemma 2.7 we get

$$\begin{aligned}\left(\frac{c+(x+d)i}{q}\right)_4=i^k \Leftrightarrow \frac{c}{x+d}\in Q_k(q) &\Leftrightarrow \left(\frac{\frac{c}{x+d}+\frac ba}{\frac{c}{x+d}-\frac ba}\right)^{\frac{q-1}{4}}\equiv\left(\frac ba\right)^k \pmod q\\ &\Leftrightarrow \left(\frac{ac+b(x+d)}{ac-b(x+d)}\right)^{\frac{q-1}{4}}\equiv\left(\frac ba\right)^k \pmod q\\ &\Leftrightarrow \left(\frac{ac+bd}{ax}\cdot\frac ba\right)^{\frac{q-1}{4}}\equiv\left(\frac ba\right)^k \pmod q\\ &\Leftrightarrow \left(\frac{ac+bd}{ax}\right)^{\frac{q-1}{4}}\equiv\left(\frac ba\right)^{k-\frac{q-1}{4}} \pmod q.\end{aligned}$$

Since $\left(\frac{ac+bd}{ax}\right)^{\frac{q-1}{4}}\equiv\left(\frac ba\right)^m \pmod q$, from the above we get $\left(\frac{c+(x+d)i}{q}\right)_4=i^{m+\frac{q-1}{4}}$. Now the result follows from Theorems 3.1 and 3.2 immediately.

Suppose $(d_0,x+c)=1$. By Lemma 2.11, $(q,(x+c)(d^2+(x+c)^2))=1$. It is easily seen that $\frac{ad-b(x+c)}{ad+b(x+c)}\equiv\frac{ac+bd}{-ax} \pmod q$. Thus, for $k=0,1,2,3$, using Lemma 2.7 we get

$$\begin{aligned}\Big(\frac{d-(x+c)i}{q}\Big)_4 = i^k &\Leftrightarrow -\frac{d}{x+c} \in Q_k(q)\\ &\Leftrightarrow \left(\frac{-\frac{d}{x+c}+\frac{b}{a}}{-\frac{d}{x+c}-\frac{b}{a}}\right)^{\frac{q-1}{4}} \equiv \Big(\frac{b}{a}\Big)^k \pmod q\\ &\Leftrightarrow \Big(\frac{ad-b(x+c)}{ad+b(x+c)}\Big)^{\frac{q-1}{4}} \equiv \Big(\frac{b}{a}\Big)^k \pmod q\\ &\Leftrightarrow \Big(\frac{ac+bd}{-ax}\Big)^{\frac{q-1}{4}} \equiv \Big(\frac{b}{a}\Big)^k \pmod q\\ &\Leftrightarrow \Big(\frac{ac+bd}{ax}\Big)^{\frac{q-1}{4}} \equiv \Big(\frac{b}{a}\Big)^{\frac{q-1}{2}+k} \pmod q.\end{aligned}$$

Since $\big(\frac{ac+bd}{ax}\big)^{\frac{q-1}{4}} \equiv \big(\frac{b}{a}\big)^m \pmod q$, by the above we get $\big(\frac{d-(x+c)i}{q}\big)_4 = i^{m-\frac{q-1}{2}}$. Thus, applying Theorem 3.3 and the fact $\frac{x}{2} \equiv \frac{x^2}{4} = \frac{c^2-qy^2+d^2}{4} \equiv \frac{1-q}{4}+\frac{d}{2} \pmod 2$ for even x we derive the result. The proof is now complete.

Corollary 4.3. *Let $p \equiv 1 \pmod 4$ and $q \equiv 5 \pmod 8$ be primes such that $p = c^2+d^2 = x^2+qy^2$ with $c,d,x,y \in \mathbb{Z}$ and $q \mid cd$. Suppose $c \equiv 1 \pmod 4$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$.*

(i) *If $p \equiv 1 \pmod 8$, then*

$$q^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{d}{4}+\frac{x+2}{4}} \pmod p & \text{if } 2 \mid x \text{ and } x \equiv \pm c \pmod q,\\ \pm(-1)^{\frac{d}{4}+\frac{x-1}{2}+\frac{y}{4}} \pmod p & \text{if } 2 \nmid x \text{ and } x \equiv \pm c \pmod q,\\ \pm(-1)^{\frac{q-5}{8}+\frac{d}{4}+\frac{x+2}{4}}\frac{d}{c} \pmod p & \text{if } 2 \mid x \text{ and } x \equiv \pm d \pmod q,\\ \pm(-1)^{\frac{q-5}{8}+\frac{d}{4}+\frac{x-1}{2}+\frac{y}{4}}\frac{d}{c} \pmod p & \text{if } 2 \nmid x \text{ and } x \equiv \pm d \pmod q.\end{cases}$$

(ii) *If $p \equiv 5 \pmod 8$, then*

$$q^{\frac{p-5}{8}} \equiv \begin{cases} \pm\delta(x)\frac{dy}{cx} \pmod p & \text{if } x \equiv \pm c \pmod q,\\ \mp(-1)^{\frac{q-5}{8}}\delta(x)\frac{y}{x} \pmod p & \text{if } x \equiv \pm d \pmod q,\end{cases}$$

where $\delta(x) = 1$ or -1 according as $8 \mid x$ or not.

Proof. If $x \equiv \pm c \pmod q$, then $q \mid d$ and so $\big(\frac{ac+bd}{ax}\big)^{\frac{q-1}{4}} \equiv \big(\frac{c}{x}\big)^{\frac{q-1}{4}} \equiv (\pm 1)^{\frac{q-1}{4}} = \pm 1 \pmod q$. If $x \equiv \pm d \pmod q$, then $q \mid c$ and so $\big(\frac{ac+bd}{ax}\big)^{\frac{q-1}{4}} \equiv \big(\frac{bd}{ax}\big)^{\frac{q-1}{4}} \equiv (\pm\frac{b}{a})^{\frac{q-1}{4}} \equiv \pm(-1)^{\frac{q-5}{8}}\frac{b}{a} \pmod q$. Now combining the above with Theorem 4.3 we deduce the result.

Theorem 4.4. *Let p and q be distinct primes such that $p \equiv 1 \pmod 4$, $q \equiv 1 \pmod 8$, $p = c^2+d^2 = x^2+qy^2$, $q = a^2+b^2$, $a,b,c,d,x,y \in \mathbb{Z}$,*

$c \equiv 1 \pmod 4$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Suppose $(\frac{ac+bd}{ac-bd})^{\frac{q-1}{8}} \equiv (\frac{b}{a})^m \pmod q$.

(i) *If $p \equiv 1 \pmod 8$, then*

$$q^{\frac{p-1}{8}} \equiv (-1)^{\frac{d}{4}+\frac{xy}{4}} \left(\frac{d}{c}\right)^m \pmod p.$$

(ii) *If $p \equiv 5 \pmod 8$, then*

$$q^{\frac{p-5}{8}} \equiv \begin{cases} (-1)^{\frac{x-2}{4}} \left(\frac{d}{c}\right)^{m+1} \frac{y}{x} \pmod p & \text{if } 2 \mid x, \\ (-1)^{\frac{x+1}{2}} \left(\frac{d}{c}\right)^{m+1} \frac{y}{x} \pmod p & \text{if } 2 \nmid x. \end{cases}$$

Proof. Observe that $b^2 \equiv -a^2 \pmod q$, $p \equiv x^2 \pmod q$ and so

$$\left(\frac{ac+bd}{ac-bd}\right)^{\frac{q-1}{8}} = \frac{(ac+bd)^{\frac{q-1}{4}}}{(a^2c^2-b^2d^2)^{\frac{q-1}{8}}} \equiv \frac{(ac+bd)^{\frac{q-1}{4}}}{(a^2p)^{\frac{q-1}{8}}}$$
$$\equiv \left(\frac{ac+bd}{ax}\right)^{\frac{q-1}{4}} \pmod q.$$

The result follows from Theorem 4.3.

We note that if $q \nmid d$, then the m in Theorem 4.4 depends only on $\frac{c}{d} \pmod q$.

Corollary 4.4. *Let $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 8$ be distinct primes such that $p = c^2 + d^2 = x^2 + qy^2$ with $c, d, x, y \in \mathbb{Z}$ and $q \mid cd(c^2 - d^2)$. Suppose $c \equiv 1 \pmod 4$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$.*

(i) *If $p \equiv 1 \pmod 8$, then*

$$q^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^{\frac{q-1}{8}+\frac{d}{4}+\frac{xy}{4}} \pmod p & \text{if } q \mid c, \\ (-1)^{\frac{d}{4}+\frac{xy}{4}} \pmod p & \text{if } q \mid d, \\ (-1)^{\frac{q-1}{16}+\frac{d}{4}+\frac{xy}{4}} \pmod p & \text{if } 16 \mid (q-1) \text{ and } c \equiv \pm d \pmod q, \\ \pm(-1)^{\frac{q-9}{16}+\frac{d}{4}+\frac{xy}{4}} \frac{d}{c} \pmod p & \text{if } 16 \mid (q-9) \text{ and } c \equiv \pm d \pmod q. \end{cases}$$

(ii) *If $p \equiv 5 \pmod 8$ and $\varepsilon(x) = (-1)^{\frac{x-2}{4}}$ or $(-1)^{\frac{x+1}{2}}$ according as $2 \mid x$ or $2 \nmid x$, then*

$$q^{\frac{p-5}{8}} \equiv \begin{cases} (-1)^{\frac{q-1}{8}} \varepsilon(x) \frac{dy}{cx} \pmod p & \text{if } q \mid c, \\ \varepsilon(x) \frac{dy}{cx} \pmod p & \text{if } q \mid d, \\ (-1)^{\frac{q-1}{16}} \varepsilon(x) \frac{dy}{cx} \pmod p & \text{if } 16 \mid (q-1) \text{ and } c \equiv \pm d \pmod q, \\ \mp(-1)^{\frac{q-9}{16}} \varepsilon(x) \frac{y}{x} \pmod p & \text{if } 16 \mid (q-9) \text{ and } c \equiv \pm d \pmod q. \end{cases}$$

Proof. Suppose that $q=a^2+b^2$ with $a,b\in\mathbb{Z}$. Then clearly

$$\Big(\frac{ac+bd}{ac-bd}\Big)^{\frac{q-1}{8}}\equiv\begin{cases}(-1)^{\frac{q-1}{8}}\pmod q & \text{if } q\mid c,\\ 1\pmod q & \text{if } q\mid d,\\ (-1)^{\frac{q-1}{16}}\pmod q & \text{if } 16\mid(q-1) \text{ and } c\equiv\pm d\pmod q,\\ \pm(-1)^{\frac{q-9}{16}}\frac ba\pmod q & \text{if } 16\mid(q-9) \text{ and } c\equiv\pm d\pmod q.\end{cases}$$

Thus the result follows from Theorem 4.4.

Corollary 4.5. *Let $p\equiv 1\pmod 4$ be a prime such that $p\ne 17$ and $p=c^2+d^2=x^2+17y^2$ with $c,d,x,y\in\mathbb{Z}$. Suppose $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1\pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$.*

(i) *If $p\equiv 1\pmod 8$, then*

$$17^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac d4+\frac{xy}4}\pmod p & \text{if } 17\mid cd,\\ -(-1)^{\frac d4+\frac{xy}4}\pmod p & \text{if } c\equiv\pm d\pmod{17},\\ \pm(-1)^{\frac d4+\frac{xy}4}\frac cd\pmod p & \text{if } c\equiv\pm 5d,\pm 10d\pmod{17}.\end{cases}$$

(ii) *If $p\equiv 5\pmod 8$ and $\varepsilon(x)=(-1)^{\frac{x-2}{4}}$ or $(-1)^{\frac{x+1}{2}}$ according as $2\mid x$ or $2\nmid x$, then*

$$17^{\frac{p-5}{8}}\equiv\begin{cases}\varepsilon(x)\frac{dy}{cx}\pmod p & \text{if } 17\mid cd,\\ -\varepsilon(x)\frac{dy}{cx}\pmod p & \text{if } c\equiv\pm d\pmod{17},\\ \pm\varepsilon(x)\frac yx\pmod p & \text{if } c\equiv\pm 5d,\pm 10d\pmod{17}.\end{cases}$$

Proof. Since $17=1^2+4^2$ and $\big(\frac{\pm5+4}{\pm5-4}\big)^{\frac{17-1}{8}}\equiv\big(\frac{\pm10+4}{\pm10-4}\big)^{\frac{17-1}{8}}\equiv\mp4\pmod{17}$, from Theorem 4.4 and Corollary 4.4 we deduce the result.

Theorem 4.5. *Let $p\equiv 1\pmod 4$ be a prime, $p=c^2+d^2=x^2+(a^2+b^2)y^2\ne a^2+b^2$, $a,b,c,d,x,y\in\mathbb{Z}$, $a\ne 0$, $2\mid a$, $(a,b)=1$, $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1\pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$. Suppose $\big(\frac{(ac+bd)/x}{b+ai}\big)_4=i^m$.*

(i) *If $p\equiv 1\pmod 8$, then*

$$(a^2+b^2)^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac d4+\frac x4}\big(\frac cd\big)^m\pmod p & \text{if } 4\mid a \text{ and } 2\mid x,\\ (-1)^{\frac d4+\frac y4}\big(\frac cd\big)^m\pmod p & \text{if } 4\mid a \text{ and } 2\nmid x,\\ (-1)^{\frac{b+1}{2}+\frac d4+\frac{x-2}{4}}\big(\frac cd\big)^{m-1}\pmod p & \text{if } 2\parallel a \text{ and } 2\mid x,\\ (-1)^{\frac{b-1}{2}+\frac d4+\frac y4+\frac{x-1}{2}}\big(\frac cd\big)^{m-1}\pmod p & \text{if } 2\parallel a \text{ and } 2\nmid x.\end{cases}$$

(ii) *If* $p\equiv 5\pmod 8$, *then*

$$(a^2+b^2)^{\frac{p-5}{8}}\equiv\begin{cases}(-1)^{\frac{x-2}{4}}\left(\frac cd\right)^{m-1}\frac yx\pmod p&\text{if } 4\mid a \text{ and } 2\mid x,\\(-1)^{\frac{x+1}{2}}\left(\frac cd\right)^{m-1}\frac yx\pmod p&\text{if } 4\mid a \text{ and } 2\nmid x,\\(-1)^{\frac x4+\frac{b+1}{2}}\left(\frac cd\right)^{m}\frac yx\pmod p&\text{if } 2\parallel a \text{ and } 2\mid x,\\(-1)^{\frac{b-1}{2}}\left(\frac cd\right)^{m}\frac yx\pmod p&\text{if } 2\parallel a \text{ and } 2\nmid x.\end{cases}$$

Proof. Set $q=a^2+b^2$. Then clearly $2\nmid q$ and $p\nmid q$. We first assume $(c,x+d)=1$. By Lemma 2.11, $(q,x+d)=(q,c^2+(x+d)^2)=1$. Since $\frac{c-(x+d)i}{c+(x+d)i}\equiv\frac{c-di}{ix}\pmod q$, we see that

$$\begin{aligned}\left(\frac{c/(x+d)+i}{q}\right)_4&=\left(\frac{c+(x+d)i}{q}\right)_4=\left(\frac{c+(x+d)i}{b+ai}\right)_4\left(\frac{c+(x+d)i}{b-ai}\right)_4\\&=\left(\frac{c+(x+d)i}{b+ai}\right)_4\overline{\left(\frac{c-(x+d)i}{b+ai}\right)_4}=\left(\frac{c+(x+d)i}{b+ai}\right)_4\left(\frac{c-(x+d)i}{b+ai}\right)_4^{-1}\\&=\left(\frac{\frac{c-(x+d)i}{c+(x+d)i}}{b+ai}\right)_4^{-1}=\left(\frac{\frac{c-di}{ix}}{b+ai}\right)_4^{-1}=\left(\frac{ai}{b+ai}\right)_4\left(\frac{(ac-adi)/x}{b+ai}\right)_4^{-1}\\&=\left(\frac{-b}{b+ai}\right)_4\left(\frac{(ac+bd)/x}{b+ai}\right)_4^{-1}=(-1)^{\frac{b+1}{2}\cdot\frac a2}\left(\frac{b+ai}{b}\right)_4 i^{-m}\\&=(-1)^{\frac{b+1}{2}\cdot\frac a2}\left(\frac ib\right)_4 i^{-m}=(-1)^{\frac{b+1}{2}\cdot\frac a2+\frac{b^2-1}{8}}i^{-m}\\&=(-1)^{\frac{b+1}{2}\cdot\frac a2+\frac{q-1-a^2}{8}}i^{-m}=(-1)^{\frac{b+1}{2}\cdot\frac a2+[\frac q8]}i^{-m}.\end{aligned}$$

This together with Theorems 3.1 and 3.2 yields the result in this case.

Now we assume $(d_0,x+c)=1$. By Lemma 2.11, $(q,x+c)=(q,(x+c)^2+d^2)=1$. Since $\frac{d+(x+c)i}{d-(x+c)i}\equiv\frac{c-di}{-x}\pmod q$, using Lemma 2.6 we see that

$$\begin{aligned}\left(\frac{d/(x+c)-i}{q}\right)_4&=\left(\frac{d-(x+c)i}{q}\right)_4=\left(\frac{d-(x+c)i}{b+ai}\right)_4\left(\frac{d-(x+c)i}{b-ai}\right)_4\\&=\left(\frac{d-(x+c)i}{b+ai}\right)_4\overline{\left(\frac{d+(x+c)i}{b+ai}\right)_4}=\left(\frac{d-(x+c)i}{b+ai}\right)_4\left(\frac{d+(x+c)i}{b+ai}\right)_4^{-1}\\&=\left(\frac{\frac{d+(x+c)i}{d-(x+c)i}}{b+ai}\right)_4^{-1}=\left(\frac{\frac{c-di}{-x}}{b+ai}\right)_4^{-1}=\left(\frac{-a}{b+ai}\right)_4\left(\frac{(ac-adi)/x}{b+ai}\right)_4^{-1}\\&=(-1)^{\frac a2}\left(\frac{a}{b+ai}\right)_4\left(\frac{(ac+bd)/x}{b+ai}\right)_4^{-1}=(-1)^{\frac a2}\left(\frac{a}{b+ai}\right)_4 i^{-m}\\&=\begin{cases}-(-1)^{\frac{b-1}{2}}i\cdot i^{-m}=(-1)^{\frac{b+1}{2}}i^{1-m}&\text{if } 2\parallel a,\\1\cdot 1\cdot i^{-m}=i^{-m}&\text{if } 4\mid a.\end{cases}\end{aligned}$$

Combining this with Theorem 3.3 we deduce the result. The proof is now complete.

REMARK 4.1. Let p be a prime of the form $4k+1$, $q \in \mathbb{Z}$, $2 \nmid q$, $p \nmid q$, and $p = c^2 + d^2 = x^2 + qy^2$ with $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. We conjecture that one can always choose the sign of x such that $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Thus the condition $(c, x+d) = 1$ or $(d_0, x+c) = 1$ in Theorems 4.1–4.5 and Corollaries 4.1–4.5 can be canceled. See also related conjectures in [S4] and [S5].

Acknowledgements. The author is supported by the National Natural Sciences Foundation of China (No. 10971078).

References

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

[E] R. J. Evans, *Residuacity of primes*, Rocky Mountain J. Math. 19 (1989), 1069–1081.

[H] R. H. Hudson, *Diophantine determinations of* $3^{(p-1)/8}$ *and* $5^{(p-1)/4}$, Pacific J. Math. 111 (1984), 49–55.

[HW] R. H. Hudson and K. S. Williams, *Some new residuacity criteria*, Pacific J. Math. 91 (1980), 135–143.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer, New York, 1990.

[Lem] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer, Berlin, 2000.

[S1] Z. H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. 97 (2001), 361–377.

[S2] Z. H. Sun, *Quartic residues and binary quadratic forms*, J. Number Theory 113 (2005), 10–52.

[S3] Z. H. Sun, *On the quadratic character of quadratic units*, J. Number Theory 128 (2008), 1295–1335.

[S4] Z. H. Sun, *Quartic, octic residues and Lucas sequences*, J. Number Theory 129 (2009), 499–550.

[S5] Z. H. Sun, *Congruences for* $(A+\sqrt{A^2+mB^2})^{(p-1)/2}$ *and* $(b+\sqrt{a^2+b^2})^{(p-1)/4}$ $(\bmod p)$, Acta Arith. 149 (2011), 275–296.

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

Received on 26.10.2011
and in revised form on 24.9.2012 (6865)