J. Number Theory 147(2015), 694-707

New reciprocity laws for octic residues and nonresidues

ZHI-HONG SUN

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

ABSTRACT. Let $\mathbb{Z}$ be the set of integers, and let p be a prime of the form $8k+1$. Suppose $q \in \mathbb{Z}$, $2 \nmid q$, $p \nmid q$, $p = c^2 + d^2 = x^2 + 2qy^2$, $c, d, x, y \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. In this paper we establish congruences for $(-q)^{(p-1)/8} \pmod p$ and present new reciprocity laws.

MSC: Primary 11A15, Secondary 11A07, 11B39, 11E25
Keywords: Reciprocity law; octic residue; congruence; quartic Jacobi symbol; Lucas sequence

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 $(\frac{a}{m})$ be the (quadratic) Jacobi symbol. For convenience we also define $(\frac{a}{1}) = 1$ and $(\frac{a}{-m}) = (\frac{a}{m})$. Then for any two odd numbers m and n with $m > 0$ or $n > 0$ we have the following general quadratic reciprocity law: $(\frac{m}{n}) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}(\frac{n}{m})$.

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 [S1,S2,S4]. From [IR] we know that $\left(\frac{a-bi}{c-di}\right)_4 = \left(\frac{a+bi}{c+di}\right)_4^{-1}$. In Section 2 we list main properties of the quartic Jacobi symbol. See also [IR], [BEW] and [S4]. For the history of quartic reciprocity laws, see [Lem].

Let p be a prime of the form $4k+1$, $q \in \mathbb{Z}$, $2 \nmid q$ and $p \nmid q$. Suppose that $p = c^2 + d^2 = x^2 + qy^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume that $(c, x+d) = 1$ or $(d_0, x+c) = 1$, where (m, n) is the greatest common divisor of m and n. In [S5], using the quartic reciprocity law the author deduced some congruences for $q^{[p/8]} \pmod p$ in terms of c, d, x and y, where $[a]$ is the greatest integer not exceeding a.

Let p be a prime of the form $8k+1$, $q \in \mathbb{Z}$, $2 \nmid q$ and $p \nmid q$. Then q is an octic residue $\pmod p$ if and only if $q^{(p-1)/8} \equiv 1 \pmod p$. In the classical octic reciprocity laws (see [Lem] and [BEW]), we always assume that $p = c^2 + d^2 = a^2 + 2b^2$ $(a, b, c, d \in \mathbb{Z})$. Inspired by [S5], in this paper we continue to discuss congruences for $(-q)^{(p-1)/8} \pmod p$ and present new reciprocity laws, but we assume that $p = c^2 + d^2 = x^2 + 2qy^2$. Here are some typical results:

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

$\star$ Let p and q be primes such that $p \equiv 1 \pmod 8$, $q \equiv 7 \pmod 8$, $p = c^2+d^2 = x^2+2qy^2$, $c,d,x,y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $(-q)^{\frac{p-1}{8}} \equiv (\frac{d}{c})^m \pmod p$ if and only if $(\frac{c-di}{c+di})^{\frac{q+1}{8}} \equiv i^m \pmod q$.

$\star$ Let $p \equiv 1 \pmod 8$ be a prime, $p = c^2+d^2 = x^2+2(a^2+b^2)y^2$, $a,b,c,d,x,y \in \mathbb{Z}$, $a \neq 0$, $4 \mid a$, $(a,b) = 1$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $(-a^2-b^2)^{\frac{p-1}{8}} \equiv (-1)^{\frac{d}{4}+\frac{y}{2}}(\frac{c}{d})^m \pmod p$ if and only if $(\frac{(ac+bd)/x}{b+ai})_4 = i^m$.

$\star$ Let p be a prime of the form $8k+1$ and $a \in \mathbb{Z}$ with $2 \nmid a$. Suppose that $p = c^2+d^2 = x^2+(a^2+1)y^2$, $c,d,x,y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0 (2 \nmid d_0)$ and $4 \mid y$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $(a+\sqrt{a^2+1})^{\frac{p-1}{4}} \equiv (-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p$.

When a is even, a congruence for $(a+\sqrt{a^2+1})^{(p-1)/4} \pmod p$ was given by the author in [S6, Corollary 4.1]. When $a \geq 3$ is a positive integer and a^2+1 is squarefree, $a+\sqrt{a^2+1}$ is just the fundamental unit ε_{a^2+1} of the quadratic field $\mathbb{Q}(\sqrt{a^2+1})$. For early results and conjectures on $\varepsilon_d^{(p-1)/4} \pmod p$, see [L2],[LW1],[LW2],[HK],[Lem] and [S2].

Throughout this paper, if $n \in \mathbb{Z}$, $2^\alpha \mid n$ and $2^{\alpha+1} \nmid n$, then we write that $2^\alpha \parallel n$.

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*

$$\Big(\frac{i}{a+bi}\Big)_4 = i^{\frac{a^2+b^2-1}{4}} = (-1)^{\frac{a^2-1}{8}} i^{(1-(-1)^{\frac{b}{2}})/2}$$

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

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

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

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:*

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

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 $(m, a^2+b^2) = 1$. Then $(\frac{a+bi}{m})_4^2 = (\frac{a^2+b^2}{m})$.*

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

Lemma 2.6 ([S5, 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* $(\frac{c+di}{m})_4=(\frac{x(x+d)}{m})$.

Lemma 2.7. *Let p be a prime of the form $8k+1$, $q\in\mathbb{Z}$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+2qy^2$ with $c,d,x,y\in\mathbb{Z}$, $c\equiv 1 \pmod 4$, $d=2^rd_0$ and $d_0\equiv 1 \pmod 4$. If $\big(\frac{x/y}{c+di}\big)_4=(-1)^{s+\frac{p-1}{8}}i^n$, then*

$$(-q)^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^s(\frac dc)^{n-1} \pmod p & \text{if } 8\mid d-4,\\ (-1)^{s+\frac d8}(\frac dc)^n \pmod p & \text{if } 8\mid d.\end{cases}$$

Proof. As $c\equiv 1 \pmod 4$ and $4\mid d$ we see that $c+di$ is primary in $\mathbb{Z}[i]$. Since $i\equiv d/c \pmod{c+di}$ we have $(\frac xy)^{\frac{p-1}{4}}\equiv(\frac{x/y}{c+di})_4=(-1)^{s+\frac{p-1}{8}}i^n\equiv(-1)^{s+\frac{p-1}{8}}(\frac dc)^n \pmod{c+di}$. As $(\frac xy)^2\equiv -2q \pmod p$ and the norm of $c+di$ is p, from the above we deduce that $(-2q)^{\frac{p-1}{8}}\equiv(\frac xy)^{\frac{p-1}{4}}\equiv(-1)^{s+\frac{p-1}{8}}(\frac dc)^n \pmod p$. By [L1] or [HW, (1.4) and (1.5)],

$$(2.1)\qquad (-2)^{\frac{p-1}{8}}\equiv\Big(\frac cd\Big)^{-\frac d4}\equiv\begin{cases}(\frac cd)^{-d_0}\equiv(\frac cd)^{-1}=\frac dc \pmod p & \text{if } 8\mid d-4,\\ (-1)^{\frac d8} \pmod p & \text{if } 8\mid d.\end{cases}$$

Thus the result follows.

3. Congruences for $(-q)^{(p-1)/8} \pmod p$ with $p=c^2+d^2=x^2+2qy^2$.

Theorem 3.1. *Let p be a prime of the form $8n+1$, $q\in\mathbb{Z}$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+2qy^2$ with $c,d,x,y\in\mathbb{Z}$, $c\equiv 1 \pmod 4$, $d=2^rd_0$, $d_0\equiv 1 \pmod 4$ and $(c,x+d)=1$. Assume that $(\frac{c/(x+d)+i}{q})_4=i^k$. Then*

$$(-q)^{\frac{p-1}{8}}\equiv\begin{cases}(-1)^{\frac{q-1}{8}+\frac d4+\frac y2}(\frac dc)^k \pmod p & \text{if } q\equiv 1 \pmod 8,\\ (-1)^{\frac{q-3}{8}+\frac{x-1}{2}}(\frac dc)^{k+1} \pmod p & \text{if } q\equiv 3 \pmod 8,\\ (-1)^{\frac{q-5}{8}+\frac d4+\frac{x-1}{2}+\frac y2}(\frac dc)^{k-1} \pmod p & \text{if } q\equiv 5 \pmod 8,\\ (-1)^{\frac{q+1}{8}}(\frac dc)^k \pmod p & \text{if } q\equiv 7 \pmod 8.\end{cases}$$

Proof. We choose the sign of y so that $y=2^ty_0$ and $y_0\equiv 1 \pmod 4$. Since $p=c^2+d^2=x^2+2qy^2\equiv 1 \pmod 8$ we see that $2\nmid x$, $2\mid y$, $4\mid d$, $(x,qy)=1$ and $p\nmid x$. Thus $(x,c^2+(x+d)^2)=(x,p)=1$. As $2qy^2=c^2+(d+x)(d-x)=c^2+(x+d)^2-2x(x+d)$ we see that $(qy,x+d)\mid c^2$, $(qy,x+d)=1$ and $(qy^2,(c^2+(x+d)^2)/2)=1$. It is easily seen that $c+(x+d)i=i^{\frac{1\mp1}{2}}(1+i)(\frac{x+d\pm c}{2}+\frac{\pm(x+d)-c}{2}i)$ and so $(\frac{x+d\pm c}{2})^2+(\frac{\pm(x+d)-c}{2})^2=\frac{c^2+(x+d)^2}{2}$. Set $\varepsilon=(-1)^{\frac{x-1}{2}}$. As $4\mid d$ and $4\mid c-1$ we have $x+d\equiv\varepsilon \pmod 4$ and $4\mid(\varepsilon(x+d)-c)$. From Lemmas 2.1-2.5, [S5, Lemma 2.10(ii)] and the above we see that

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

and

$$\Big(\frac{q}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4=\Big(\frac{qy^2}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{y^2}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4$$

$$=\Big(\frac{(c^2+(x+d)^2)/2-x(x+d)}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{y}{(\frac{x+d+\varepsilon c}{2})^2+(\frac{\varepsilon(x+d)-c}{2})^2}\Big)$$

$$=\Big(\frac{-x(x+d)}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4\Big(\frac{y}{(c^2+(x+d)^2)/2}\Big)$$

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

Clearly, $(-1)^{\frac{c^2-(x+d)^2}{8}}=(-1)^{\frac{c^2-x^2-2dx}{8}}=(-1)^{\frac{c-\varepsilon x}{4}\cdot\frac{c+\varepsilon x}{2}-\frac{d}{4}\varepsilon}=(-1)^{\frac{c-\varepsilon x}{4}-\frac{d}{4}\varepsilon}=(-1)^{\frac{\varepsilon(x+d)-c}{4}}$. Also,

$$\Big(\frac{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}{x(x+d)}\Big)_4=\Big(\frac{d+\varepsilon c+(\varepsilon d-c)i}{x}\Big)_4\Big(\frac{\varepsilon c-ci}{x+d}\Big)_4$$

$$=\Big(\frac{(\varepsilon-i)(c+di)}{x}\Big)_4\Big(\frac{\varepsilon-i}{x+d}\Big)_4=\Big(\frac{\varepsilon-i}{x(x+d)}\Big)_4\Big(\frac{c+di}{x}\Big)_4$$

$$=\Big(\frac{i^{\frac{5+\varepsilon}{2}}(1+i)}{x(x+d)}\Big)_4\Big(\frac{c+di}{x}\Big)_4=\Big(\frac{i}{x(x+d)}\Big)_4^{\frac{5+\varepsilon}{2}}\Big(\frac{1+i}{x(x+d)}\Big)_4\Big(\frac{x}{c+di}\Big)_4$$

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

Hence

$$\Big(\frac{q}{\frac{x+d+\varepsilon c}{2}+\frac{\varepsilon(x+d)-c}{2}i}\Big)_4=(-1)^{\frac{\varepsilon(x+d)-c}{4}(1+t)+\frac{d}{4}t}\cdot(-1)^{\frac{d}{4}\cdot\frac{x+1}{2}+\frac{x^2-1}{8}}i^{\frac{dx}{4}}\Big(\frac{x/y}{c+di}\Big)_4$$

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

Therefore

$$i^k=(-1)^{\frac{q-(\frac{-1}{q})}{4}\cdot\frac{x-1}{2}+\frac{q-1}{2}(\frac{\varepsilon x-c}{4}+\frac{d}{4})}i^{\frac{(\frac{-1}{q})q-1}{4}}$$

$$\times(-1)^{\frac{\varepsilon x-c}{4}(1+t)+\frac{d}{4}\cdot\frac{x-1}{2}+\frac{x^2-1}{8}}i^{\frac{dx}{4}}\Big(\frac{x/y}{c+di}\Big)_4.$$

It is clear that

$$i^{\frac{dx}{4}}=i^{\frac{d}{4}(x-1)+\frac{d}{4}}=(-1)^{\frac{d}{4}\cdot\frac{x-1}{2}}i^{\frac{d}{4}},\ (-1)^{\frac{x^2-1}{8}}=(-1)^{\frac{p-1-2qy^2}{8}}=(-1)^{\frac{p-1}{8}+\frac{y}{2}},$$

$$(-1)^{\frac{\varepsilon x-c}{4}}=(-1)^{\frac{\varepsilon x-c}{4}\cdot\frac{\varepsilon x+c}{2}}=(-1)^{\frac{x^2-c^2}{8}}=(-1)^{\frac{d^2-8q(\frac{y}{2})^2}{8}}=(-1)^{\frac{y}{2}}$$

and so $(-1)^{\frac{\varepsilon x-c}{4}(1+t)}=(-1)^{\frac{y}{2}(1+t)}=1$. Thus,

$$\Big(\frac{x/y}{c+di}\Big)_4=(-1)^{\frac{q-(\frac{-1}{q})}{4}\cdot\frac{x-1}{2}+\frac{q-1}{2}(\frac{y}{2}+\frac{d}{4})+\frac{p-1}{8}+\frac{y}{2}}i^{k-\frac{d}{4}-\frac{q(\frac{-1}{q})-1}{4}}.$$

Now applying Lemma 2.7 we deduce the result.

Theorem 3.2. *Let p be a prime of the form $8n+1$, $q\in\mathbb{Z}$, $2\nmid q$ and $p\nmid q$. Suppose that $p=c^2+d^2=x^2+2qy^2$ with $c,d,x,y\in\mathbb{Z}$, $c\equiv 1 \pmod 4$, $d=2^r d_0$, $d_0\equiv 1 \pmod 4$, $(d_0,x+c)=1$ and $(\frac{-d/(x+c)+i}{q})_4=i^k$. Then*

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

Proof. Suppose $2^m \parallel (x+c)$ and $y=2^t y_0$ with $y_0\equiv 1 \pmod 4$. Since $p=c^2+d^2=x^2+2qy^2\equiv 1 \pmod 8$ we see that $2\nmid x$, $2\mid y$, $4\mid d$, $(x,qy)=1$ and $p\nmid x$. Thus $(x,d^2+(x+c)^2)=(x,p)=1$. As $2qy^2=d^2+(c+x)(c-x)=d^2+(x+c)^2-2x(x+c)$ we see that $(qy_0,x+c)\mid d_0^2$, $(qy_0,x+c)=1$ and $(qy_0^2,(x+c)^2+d^2)=1$. We prove the theorem by considering the three cases $m<r$, $m=r$ and $m>r$. We only give details for the first case. The other two cases can be proved similarly by using Lemmas 2.1-2.7. For the details, see the author's preprint "Congruences for $q^{[p/8]} \pmod p$ II" at arXiv:1401.0493.

Now suppose $m<r$. Using Lemmas 2.1-2.5 and the fact $\left(\frac{a}{q}\right)_4=1$ for $a\in\mathbb{Z}$ with $(a,q)=1$ we see that

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

By [S5, p.15], $(\frac{y}{((x+c)^2+d^2)/2^{2m}})=(-1)^{\frac{d}{2^{m+1}}t+\frac{d}{4}t}(\frac{y^{-1}}{c+di})_4$. We also have $(\frac{2^m}{\frac{x+c}{2^m}+\frac{d}{2^m}i})_4=(\frac{2}{\frac{x+c}{2^m}+\frac{d}{2^m}i})_4^m=i^{\frac{x+c}{2^m}\cdot\frac{dm}{2^{m+1}}}$ and

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

Thus,

$$\begin{aligned}i^k=\Big(\frac{d-(x+c)i}{q}\Big)_4&=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}i^{\frac{x+c}{2^m}\cdot\frac{dm}{2^{m+1}}}\\&\times(-1)^{\frac{x(x+c)/2^m+1}{2}\cdot\frac{d}{2^{m+1}}+\frac{(\frac{x+c}{2^m})^2-1}{8}}(-1)^{\frac{d}{2^{m+1}}t+\frac{d}{4}t}\Big(\frac{x/y}{c+di}\Big)_4.\end{aligned}\tag{3.1}$$

As $2qy^2 = d^2 - (x+c)^2 + 2c(x+c)$ we have

$$q\frac{y^2}{2^m} = 2^{2r-m-1}d_0^2 - 2^{m-1}\Big(\frac{x+c}{2^m}\Big)^2 + c\cdot\frac{x+c}{2^m}. \tag{3.2}$$

Suppose $m=1$. Then $x \equiv 1 \pmod 4$. From (3.2) we see that $2^{2t-1}q \equiv 2^{2r-2} - 1 + c\cdot\frac{x+c}{2} \pmod 8$ and so $\frac{x+c}{2} \equiv c(2^{2t-1}q - 2^{2r-2}+1) \pmod 8$. If $8 \nmid d$, then $r=2$ and $\frac{x+c}{2} \equiv c(2^{2t-1}q-3) \pmod 8$. Thus,

$$\begin{aligned}(-1)^{\frac{(\frac{x+c}{2})^2-1}{8}} &= (-1)^{\frac{c^2-1}{8}+\frac{(2^{2t-1}q-3)^2-1}{8}} = (-1)^{\frac{c^2-1}{8}+\frac{(2^{2t-2}q-2)(2^{2t-2}q-1)}{2}}\\ &= (-1)^{\frac{c^2-1}{8}+1+\frac{q+1}{2}\cdot\frac{y}{2}} = (-1)^{\frac{p-1}{8}+1+\frac{q+1}{2}\cdot\frac{y}{2}},\\ (-1)^{\frac{(x+c)/2+1}{2}}i^{\frac{x+c}{2}} &= (-1)^{2^{2t-2}q-1}i^{2^{2t-1}q-3} = -(-1)^{2^{2t-2}}\cdot(-1)^{2^{2t-2}}i = -i.\end{aligned}$$

Hence, from (3.1) we deduce that

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

That is, $(\frac{x/y}{c+di})_4 = (-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}+\frac{p-1}{8}+\frac{q+1}{2}\cdot\frac{y}{2}}i^{k-1}$. Now applying Lemma 2.7 we obtain the result.

If $8 \mid d$, from (3.2) we see that $2^{2t-1}q \equiv qy^2/2 \equiv -1 + c\cdot\frac{x+c}{2} \pmod 8$ and so $\frac{x+c}{2} \equiv c(2^{2t-1}q+1) \pmod 8$. Thus,

$$\begin{aligned}(-1)^{\frac{(\frac{x+c}{2})^2-1}{8}} &= (-1)^{\frac{c^2-1}{8}+\frac{(2^{2t-1}q+1)^2-1}{8}} = (-1)^{\frac{c^2+d^2-1}{8}+\frac{2^{2t-2}q(2^{2t-2}q+1)}{2}}\\ &= (-1)^{\frac{p-1}{8}+\frac{q+1}{2}\cdot\frac{y}{2}}.\end{aligned}$$

From (3.1) and the above we derive that

$$i^k = (-1)^{\frac{q^2-1}{8}}i^{\frac{x+c}{2}\cdot\frac{d}{4}}(-1)^{\frac{(\frac{x+c}{2})^2-1}{8}}\Big(\frac{x/y}{c+di}\Big)_4 = (-1)^{\frac{q^2-1}{8}+\frac{d}{8}+\frac{p-1}{8}+\frac{q+1}{2}\cdot\frac{y}{2}}\Big(\frac{x/y}{c+di}\Big)_4.$$

Now applying Lemma 2.7 we obtain

$$(-q)^{\frac{p-1}{8}} \equiv (-1)^{\frac{q^2-1}{8}+\frac{q+1}{2}\cdot\frac{y}{2}}\Big(\frac{d}{c}\Big)^k = \begin{cases}(-1)^{\frac{q-1}{4}+\frac{d}{4}+\frac{y}{2}}(\frac{d}{c})^k \pmod p & \text{if } 4 \mid q-1,\\ (-1)^{\frac{q+1}{4}}(\frac{d}{c})^k \pmod p & \text{if } 4 \mid q-3.\end{cases}$$

This yields the result.

Now assume $r > m \geq 2$. Then $x \equiv 3 \pmod 4$, $2r - m - 1 \geq 2(m+1) - m - 1 = m + 1 \geq 3$ and so $q\frac{y^2}{2^m} \equiv -2^{m-1} + c \cdot \frac{x+c}{2^m} \pmod 8$ by (3.2). Hence $2^m \parallel y^2$, $m = 2t$ and so $q \equiv -2^{m-1} + c \cdot \frac{x+c}{2^m} \pmod 8$. That is, $\frac{x+c}{2^m} \equiv c(2^{m-1} + q) \pmod 8$. Thus,

$$\begin{aligned}
&(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}(-1)^{\frac{x(x+c)/2^m+1}{2}\cdot\frac{d}{2^{m+1}}+\frac{(\frac{x+c}{2^m})^2-1}{8}}\cdot(-1)^{\frac{d}{2^{m+1}}t+\frac{d}{4}t}i^{-\frac{x+c}{2^m}\cdot\frac{dm}{2^{m+1}}}\\
&=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot\frac{d}{2^{m+1}}}(-1)^{\frac{-(2^{m-1}+q)+1}{2}\cdot 2^{r-m-1}d_0+\frac{c^2(2^{m-1}+q)^2-1}{8}}(-1)^{\frac{d}{2^{m+1}}t+\frac{d}{4}t}(-1)^{\frac{dt}{2^{m+1}}}\\
&=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot 2^{r-m-1}d_0}\cdot(-1)^{(2^{m-2}+\frac{q-1}{2})2^{r-m-1}+\frac{c^2-1}{8}+\frac{(2^{m-1}+q)^2-1}{8}}\cdot(-1)^{\frac{d}{4}t}\\
&=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}\cdot 2^{r-m-1}}\cdot(-1)^{(2^{m-2}+\frac{q-1}{2})2^{r-m-1}+\frac{p-1}{8}+\frac{q^2-1}{8}+2^{m-3}(2^{m-2}+q)}\\
&=(-1)^{2^{r-3}+\frac{p-1}{8}+2^{m-3}(2^{m-2}+q)}=\begin{cases}(-1)^{\frac{d}{8}+\frac{p-1}{8}+\frac{q+1}{2}} & \text{if } m=2,\\ (-1)^{\frac{p-1}{8}} & \text{if } m>2.\end{cases}
\end{aligned}$$

Hence, from (3.1) and the above we get

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

Now applying Lemma 2.7 and the fact $m = 2t$ we obtain

$$(-q)^{\frac{p-1}{8}} \equiv \begin{cases}(-1)^{\frac{q+1}{2}}(\frac{d}{c})^k = (-1)^{\frac{q+1}{2}(\frac{d}{4}+\frac{y}{2})}(\frac{d}{c})^k \pmod p & \text{if } r>m=2,\\ (-1)^{\frac{d}{8}}(\frac{d}{c})^k = (-1)^{\frac{q+1}{2}(\frac{d}{4}+\frac{y}{2})}(\frac{d}{c})^k \pmod p & \text{if } r>m>2.\end{cases}$$

This yields the result in the case $m < r$. Thus the theorem is proved.

Theorem 3.3. *Let p and q be primes such that $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 4$. Suppose $p = c^2 + d^2 = x^2 + 2qy^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$, $d_0 \equiv 1 \pmod 4$ and $(\frac{c-di}{x})^{\frac{q+1}{4}} \equiv i^m \pmod q$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $(-q)^{\frac{p-1}{8}} \equiv (-1)^{\frac{x-1}{2}\cdot\frac{q+1}{4}}(\frac{d}{c})^m \pmod p$.*

Proof. Clearly $q \nmid x$ and x is odd. We first assume $(c, x+d) = 1$. By the proof of Theorem 3.1, $(q, (x+d)(c^2+(x+d)^2)) = 1$. 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, from [S5, proof of Theorem 4.1] we have

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

Now, applying Theorem 3.1 we derive the result.

Now we assume $(d_0, x+c) = 1$. By the proof of Theorem 3.2, $(q, x+c) = (q, d^2 + (x+c)^2) = 1$. It is easily seen that $\frac{d+(x+c)i}{d-(x+c)i} \equiv \frac{c-di}{-x} \pmod q$. From [S5, p.18] we get $(\frac{-d/(x+c)+i}{q})_4 = i^{m-\frac{q+1}{2}} = (-1)^{\frac{q+1}{4}}i^m$. Thus, applying Theorem 3.2 we deduce the result. The proof is now complete.

Corollary 3.1. *Let p and q be primes such that $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$. Suppose $p = c^2 + d^2 = x^2 + 2qy^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$, $q \mid cd$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then*

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

Proof. If $x \equiv \pm c \pmod q$, then $q \mid d$ and so $(\frac{c-di}{x})^{\frac{q+1}{4}} \equiv (\pm 1)^{\frac{q+1}{4}} = \pm 1 \pmod q$. If $x \equiv \pm d \pmod q$, then $q \mid c$ and so $(\frac{c-di}{x})^{\frac{q+1}{4}} \equiv (\mp i)^{\frac{q+1}{4}} = \mp(-1)^{\frac{q-3}{8}} i \pmod q$. Now applying Theorem 3.3 we deduce the result.

As an example, taking $q = 3$ in Corollary 3.1 we see that if p is a prime of the form $24k+1$ and so $p = c^2 + d^2 = x^2 + 6y^2$, and if $(c, x+d) = 1$ or $(d_0, x+c) = 1$, then

$$(3.3) \qquad (-3)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{\frac{x-1}{2}} \pmod p & \text{if } x \equiv \pm c \pmod 3, \\ \mp(-1)^{\frac{x-1}{2}} \frac{d}{c} \pmod p & \text{if } x \equiv \pm d \pmod 3. \end{cases}$$

Theorem 3.4. *Let p and q be primes such that $p \equiv 1 \pmod 8$, $q \equiv 7 \pmod 8$, $p = c^2 + d^2 = x^2 + 2qy^2$, $c, d, m, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $(-q)^{\frac{p-1}{8}} \equiv (\frac{d}{c})^m \pmod p$ if and only if $(\frac{c-di}{c+di})^{\frac{q+1}{8}} \equiv i^m \pmod q$.*

Proof. Observe that $(\frac{c-di}{c+di})^{\frac{q+1}{8}} = \frac{(c-di)^{\frac{q+1}{4}}}{(c^2+d^2)^{\frac{q+1}{8}}} = \frac{(c-di)^{\frac{q+1}{4}}}{(x^2+2qy^2)^{\frac{q+1}{8}}} \equiv (\frac{c-di}{x})^{\frac{q+1}{4}} \pmod q$. The result follows from Theorem 3.3.

Corollary 3.2. *Let $p \equiv 1 \pmod 8$ and $q \equiv 7 \pmod 8$ be primes such that $p = c^2 + d^2 = x^2 + 2qy^2$ with $c, d, x, y \in \mathbb{Z}$ and $q \mid cd(c^2 - d^2)$. Suppose $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then*

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

Proof. If $q \mid c$, then $\frac{c-di}{c+di} \equiv -1 \pmod q$. If $q \mid d$, then $\frac{c-di}{c+di} \equiv 1 \pmod q$. If $c \equiv \pm d \pmod q$, then $\frac{c-di}{c+di} \equiv \mp i \pmod q$. Thus the result follows from Theorem 3.4.

Theorem 3.5. *Let p and q be distinct primes, $p \equiv 1 \pmod 8$, $q \equiv 1 \pmod 4$, $p = c^2 + d^2 = x^2 + 2qy^2$, $q = a^2 + b^2$, $a, b, c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Suppose $(\frac{ac+bd}{ax})^{\frac{q-1}{4}} \equiv (\frac{b}{a})^m \pmod q$. Then $(-q)^{\frac{p-1}{8}} \equiv (-1)^{\frac{x-1}{2} \cdot \frac{q-1}{4} + \frac{d}{4} + \frac{y}{2}} (\frac{d}{c})^m \pmod p$.*

Proof. Clearly $q \nmid x$. We first assume $(c, x+d) = 1$. By the proof of Theorem 3.1, $(q, (x+d)(c^2+(x+d)^2)) = 1$. It is easily seen that $\frac{ac+b(x+d)}{ac-b(x+d)} \equiv \frac{ac+bd}{ax} \cdot \frac{b}{a} \pmod q$. Thus, from [S5, p.20] we get $(\frac{c/(x+d)+i}{q})_4 = i^{m+\frac{q-1}{4}}$. Now the result follows from Theorem 3.1 immediately.

Suppose $(d_0, x+c) = 1$. By the proof of Theorem 3.2, $(q, (x+c)(d^2+(x+c)^2)) = 1$. It is easily seen that $\frac{ad-b(x+c)}{ad+b(x+c)} \equiv \frac{ac+bd}{-ax} \pmod q$. From [S5, p.21] we know that $(\frac{-d/(x+c)+i}{q})_4 = i^{m-\frac{q-1}{2}}$. Now applying Theorem 3.2 we deduce the result. The proof is now complete.

Corollary 3.3. *Let $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$ be primes such that $p = c^2 + d^2 = x^2 + 2qy^2$ with $c, d, x, y \in \mathbb{Z}$ and $q \mid cd$. Suppose $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then*

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

Proof. Suppose $q = a^2 + b^2$ with $a, b \in \mathbb{Z}$. If $x \equiv \pm c \pmod q$, then $q \mid d$ and so $(\frac{ac+bd}{ax})^{\frac{q-1}{4}} \equiv (\frac{c}{x})^{\frac{q-1}{4}} \equiv (\pm 1)^{\frac{q-1}{4}} = \pm 1 \pmod q$. If $x \equiv \pm d \pmod q$, then $q \mid c$ and so $(\frac{ac+bd}{ax})^{\frac{q-1}{4}} \equiv (\frac{bd}{ax})^{\frac{q-1}{4}} \equiv (\pm\frac{b}{a})^{\frac{q-1}{4}} \equiv \pm(-1)^{\frac{q-5}{8}}\frac{b}{a} \pmod q$. Now combining the above with Theorem 3.5 we deduce the result.

Theorem 3.6. *Let p and q be distinct primes such that $p \equiv 1 \pmod 8$, $q \equiv 1 \pmod 8$, $p = c^2+d^2 = x^2+2qy^2$, $q = a^2+b^2$, $a, b, c, d, m, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then*

$$(-q)^{\frac{p-1}{8}} \equiv (-1)^{\frac{d}{4}+\frac{y}{2}}\Big(\frac{d}{c}\Big)^m \pmod p \iff \Big(\frac{ac+bd}{ac-bd}\Big)^{\frac{q-1}{8}} \equiv \Big(\frac{b}{a}\Big)^m \pmod q.$$

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

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

The result follows from Theorem 3.5.

Corollary 3.4. *Let p and q be distinct primes of the form $8k+1$ such that $p = c^2+d^2 = x^2+2qy^2$ with $c, d, x, y \in \mathbb{Z}$ and $q \mid cd(c^2-d^2)$. Suppose $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then*

$$(-q)^{\frac{p-1}{8}} \equiv \begin{cases} (-1)^{\frac{q-1}{8}+\frac{d}{4}+\frac{y}{2}} \pmod p & \text{if } q \mid c, \\ (-1)^{\frac{d}{4}+\frac{y}{2}} \pmod p & \text{if } q \mid d, \\ (-1)^{\frac{q-1}{16}+\frac{d}{4}+\frac{y}{2}} \pmod p & \text{if } 16 \mid (q-1) \text{ and } c \equiv \pm d \pmod q, \\ \pm(-1)^{\frac{q-9}{16}+\frac{d}{4}+\frac{y}{2}}\frac{d}{c} \pmod p & \text{if } 16 \mid (q-9) \text{ and } c \equiv \pm d \pmod q. \end{cases}$$

Proof. Suppose that $q = a^2+b^2$ with $a, b \in \mathbb{Z}$. Then the result follows from Theorem 3.6 and the congruence for $(\frac{ac+bd}{ac-bd})^{\frac{q-1}{8}} \pmod q$ in [S5, p.23].

Theorem 3.7. *Let $p \equiv 1 \pmod 8$ be a prime, $p = c^2 + d^2 = x^2 + 2(a^2 + b^2)y^2$, $a, b, c, d, m, x, y \in \mathbb{Z}$, $a \neq 0$, $2 \mid a$, $(a, b) = 1$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x + d) = 1$ or $(d_0, x + c) = 1$. Then*

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

$$\iff \Big(\frac{(ac+bd)/x}{b+ai}\Big)_4 = i^m.$$

Proof. Suppose $q = a^2 + b^2$ and $(\frac{(ac+bd)/x}{b+ai})_4 = i^m$. Then clearly $q \equiv 1 \pmod 4$ and $p \nmid q$. We first assume $(c, x + d) = 1$. By the proof of Theorem 3.1, $(q, x + d) = (q, c^2 + (x + d)^2) = 1$. Since $\frac{c-(x+d)i}{c+(x+d)i} \equiv \frac{c-di}{ix} \pmod q$, from [S5, p.24] we know that $(\frac{c/(x+d)+i}{q})_4 = (-1)^{\frac{b+1}{2}\cdot\frac{a}{2}+[\frac{q}{8}]}i^{-m}$. This together with Theorem 3.1 yields the result in this case.

Now we assume $(d_0, x + c) = 1$. By the proof of Theorem 3.2, $(q, x + c) = (q, (x + c)^2 + d^2) = 1$. Since $\frac{d+(x+c)i}{d-(x+c)i} \equiv \frac{c-di}{-x} \pmod q$, from [S5, p.24] we know that

$$\Big(\frac{-d/(x+c)+i}{q}\Big)_4 = \begin{cases} (-1)^{\frac{b+1}{2}}i^{1-m} & \text{if } 4 \mid a-2, \\ i^{-m} & \text{if } 4 \mid a. \end{cases}$$

Now applying Theorem 3.2 we deduce the result in this case. So the theorem is proved.

Corollary 3.5. *Let $p \equiv 1, 9 \pmod{40}$ be a prime and so $p = c^2 + d^2 = x^2 + 10y^2$ with $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x + c) = 1$. Then*

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

Proof. Clearly $5 \mid cd$. When $x \equiv \pm c \pmod 5$ we have $5 \mid d$ and so $(\frac{(2c+d)/x}{1+2i})_4 = (\frac{\pm 2}{1+2i})_4 = \pm i$. When $x \equiv \pm d \pmod 5$ we have $5 \mid c$ and so $(\frac{(2c+d)/x}{1+2i})_4 = (\frac{\pm 1}{1+2i})_4 = \pm 1$. Now taking $a = 2$ and $b = 1$ in Theorem 3.7 we derive the result.

We remark that Corollary 3.5 partially solves [S4, Conjecture 9.8].

4. Congruences for $U_{\frac{p-1}{4}}(2a, -1)$ and $V_{\frac{p-1}{4}}(2a, -1) \pmod p$.

For two numbers P and Q the Lucas sequences $\{U_n(P, Q)\}$ and $\{V_n(P, Q)\}$ are defined by

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

Set $D = P^2 - 4Q$. It is well known that

$$U_n(P, Q) = \frac{1}{\sqrt{D}}\Big\{\Big(\frac{P + \sqrt{D}}{2}\Big)^n - \Big(\frac{P - \sqrt{D}}{2}\Big)^n\Big\} \quad (D \neq 0), \tag{4.1}$$

$$V_n(P, Q) = \Big(\frac{P + \sqrt{D}}{2}\Big)^n + \Big(\frac{P - \sqrt{D}}{2}\Big)^n. \tag{4.2}$$

Theorem 4.1. *Let p be a prime of the form $8k+1$ and $a\in\mathbb{Z}$ with $2\nmid a$. Suppose that $p=c^2+d^2=x^2+(a^2+1)y^2$, $c,d,x,y\in\mathbb{Z}$, $c\equiv 1\pmod 4$, $d=2^rd_0$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1\pmod 4$. Assume $(c,x+d)=1$ or $(d_0,x+c)=1$. Then*

$$U_{\frac{p-1}{4}}(2a,-1)\equiv\begin{cases}(-1)^{\frac{a-1}{2}+\frac d4+\frac{x-1}{2}}\frac yx \pmod p & \text{if } 4\mid y-2,\\ 0\pmod p & \text{if } 4\mid y\end{cases}$$

$$\text{and}\quad V_{\frac{p-1}{4}}(2a,-1)\equiv\begin{cases}0\pmod p & \text{if } 4\mid y-2,\\ 2(-1)^{\frac d4+\frac y4}\pmod p & \text{if } 4\mid y.\end{cases}$$

Proof. Set $a_1=(1-(-1)^{\frac{a-1}{2}}a)/2$ and $b_1=(1+(-1)^{\frac{a-1}{2}}a)/2$. Then $2\mid a_1$, $2\nmid b_1$ and $a^2+1=2(a_1^2+b_1^2)$. It is clear that $\big(\frac{(a_1c+b_1d)/((-1)^{\frac{x-1}{2}}x)}{b_1+a_1i}\big)_4=(-1)^{\frac{x-1}{2}\cdot\frac{a_1}{2}}\big(\frac{(a_1c+b_1d)/x}{b_1+a_1i}\big)_4$. We first assume $a\equiv 1\pmod 4$. Replacing d,x with $-d,(-1)^{\frac{x-1}{2}}x$ in [S4, Theorem 8.3(i)] we obtain

$$U_{\frac{p-1}{4}}(2a,-1)$$
$$\equiv\begin{cases}\mp(-1)^{\frac{x-1}{2}\cdot\frac{a-1}{4}}(-a_1^2-b_1^2)^{\frac{p-1}{8}}(-\frac cd)^{(1-(-1)^{\frac{a-1}{4}})/2}(-1)^{\frac{x-1}{2}}\frac yx\pmod p\\ \qquad\text{if } 4\mid y-2 \text{ and } \big(\frac{(a_1c+b_1d)/x}{b_1+a_1i}\big)_4=\pm1,\\ \mp(-1)^{\frac{x-1}{2}\cdot\frac{a-1}{4}}(-a_1^2-b_1^2)^{\frac{p-1}{8}}(-\frac cd)^{1+(1-(-1)^{\frac{a-1}{4}})/2}(-1)^{\frac{x-1}{2}}\frac yx\pmod p\\ \qquad\text{if } 4\mid y-2 \text{ and } \big(\frac{(a_1c+b_1d)/x}{b_1+a_1i}\big)_4=\pm i,\\ 0\pmod p\quad \text{if } 4\mid y\end{cases}$$

and

$$V_{\frac{p-1}{4}}(2a,-1)\equiv\begin{cases}\pm2(-1)^{\frac{x-1}{2}\cdot\frac{a-1}{4}+\frac y4}(-a_1^2-b_1^2)^{\frac{p-1}{8}}(-\frac cd)^{(1-(-1)^{\frac{a-1}{4}})/2}\pmod p\\ \qquad\text{if } 4\mid y \text{ and } \big(\frac{(a_1c+b_1d)/x}{b_1+a_1i}\big)_4=\pm1,\\ \pm2(-1)^{\frac{x-1}{2}\cdot\frac{a-1}{4}+\frac y4}(-a_1^2-b_1^2)^{\frac{p-1}{8}}(-\frac cd)^{1+(1-(-1)^{\frac{a-1}{4}})/2}\pmod p\\ \qquad\text{if } 4\mid y \text{ and } \big(\frac{(a_1c+b_1d)/x}{b_1+a_1i}\big)_4=\pm i,\\ 0\pmod p\quad \text{if } 4\mid y-2.\end{cases}$$

From Theorem 3.7 we know that

$$(-a_1^2-b_1^2)^{\frac{p-1}{8}}$$
$$\equiv\begin{cases}\pm(-1)^{\frac d4+\frac y2}\pmod p & \text{if } 4\mid a_1 \text{ and } (\frac{(a_1c+b_1d)/x}{b_1+a_1i})_4=\pm1,\\ \pm(-1)^{\frac{b_1-1}{2}+\frac d4+\frac y2+\frac{x-1}{2}}\frac dc\pmod p & \text{if } 4\mid a_1-2 \text{ and } (\frac{(a_1c+b_1d)/x}{b_1+a_1i})_4=\pm1,\\ \pm(-1)^{\frac d4+\frac y2}\frac cd\pmod p & \text{if } 4\mid a_1 \text{ and } (\frac{(a_1c+b_1d)/x}{b_1+a_1i})_4=\pm i,\\ \pm(-1)^{\frac{b_1-1}{2}+\frac d4+\frac y2+\frac{x-1}{2}}\pmod p & \text{if } 4\mid a_1-2 \text{ and } (\frac{(a_1c+b_1d)/x}{b_1+a_1i})_4=\pm i.\end{cases}$$

Now putting the above together we deduce the result in the case $a\equiv 1\pmod 4$. The case $a\equiv 3\pmod 4$ can be proved similarly by using [S4, Theorem 8.3(ii)] and Theorem 3.7.

Corollary 4.1. *Let p be a prime of the form $8k+1$ and $a \in \mathbb{Z}$ with $2 \nmid a$. Suppose that $p = c^2 + d^2 = x^2 + (a^2+1)y^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$, $y = 2^t y_0$ and $d_0 \equiv y_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then*

$$(a+\sqrt{a^2+1})^{\frac{p-1}{4}} \equiv \begin{cases} (-1)^{\frac{d}{4}+\frac{y}{4}} \pmod p & \text{if } 4 \mid y, \\ (-1)^{\frac{a-1}{2}+\frac{d}{4}+\frac{x-1}{2}} \frac{y}{x}\sqrt{a^2+1} \pmod p & \text{if } 4 \mid y-2. \end{cases}$$

Proof. By (4.1) and (4.2), $(a+\sqrt{a^2+1})^{\frac{p-1}{4}} = \frac{1}{2}V_{\frac{p-1}{4}}(2a,-1) + \sqrt{a^2+1}U_{\frac{p-1}{4}}(2a,-1)$. Now applying Theorem 4.1 we deduce the result.

Corollary 4.2. *Let p be a prime of the form $8k+1$ and $a \in \mathbb{Z}$ with $2 \nmid a$. Suppose that $p = c^2 + d^2 = x^2 + (a^2+1)y^2$, $c, d, x, y \in \mathbb{Z}$, $c \equiv 1 \pmod 4$, $d = 2^r d_0$ and $d_0 \equiv 1 \pmod 4$. Assume $(c, x+d) = 1$ or $(d_0, x+c) = 1$. Then $p \mid U_{\frac{p-1}{8}}(2a,-1)$ if and only if $4 \mid y$ and $\frac{p-1}{8} \equiv \frac{d}{4} + \frac{y}{4} \pmod 2$.*

Proof. By [S4, (1.5)], $p \mid U_{\frac{p-1}{8}}(2a,-1) \iff V_{\frac{p-1}{4}}(2a,-1) \equiv 2(-1)^{\frac{p-1}{8}} \pmod p$. Now applying Theorem 4.1 we obtain the result.

Remark 4.1 Theorem 4.1 and Corollary 4.2 were conjectured by the author in [S4, Conjectures 9.17 and 9.19].

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.

[HK] F. Halter-Koch, *On the quartic character of certain quadratic units and the representation of primes by binary quadratic forms*, Rocky Mountain J. Math. **16** (1986), 95-102.

[HW] R.H. Hudson and K.S. Williams, *Extensions of theorems of Cunningham-Aigner and Hasse-Evans*, Pacific J. Math. **104** (1983), 111-132.

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

[L1] E. Lehmer, *On Euler's criterion*, J. Austral. Math. Soc. **1** (1959/1961), 64-70.

[L2] E. Lehmer, *On the quartic character of quadratic units*, J. Reine Angew. Math. **268/269** (1974), 294-301.

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

[LW1] P.A. Leonard and K.S. Williams, *The quadratic and quartic character of certain quadratic units. I*, Pacific J. Math. **71** (1977), 101-106.

[LW2] P.A. Leonard and K.S. Williams, *The quadratic and quartic character of certain quadratic units. II*, Rocky Mountain J. Math. **9** (1979), 683-692.

[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 $q^{[p/8]}$ (mod p)*, Acta Arith. **159** (2013), 1-25.

[S6] Z.H. Sun, *On the quartic character of quadratic units*, Acta Arith. **159** (2013), 89-100.