Int. J. Number Theory 11(2015), 1301-1312.

Congruences for $q^{[p/8]} \pmod p$ under the condition $4n^2p = x^2 + qy^2$

Zhi-Hong Sun
School of Mathematical Sciences
Huaiyin Normal University
Huaian, Jiangsu 223001, PR China
zhihongsun@yahoo.com
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 $4k+1$ and so $p = c^2+d^2$ with $c, d \in \mathbb{Z}$. Let q be an integer of the form $4k+3$. Assume that $4n^2p = x^2+qy^2$ with $c, d, n, x, y \in \mathbb{Z}$ and $(q, n) = (x, y) = 1$, where (a, b) is the greatest common divisor of integers a and b. In this paper we establish congruences for $(-q)^{[p/8]} \pmod p$ in terms of c, d, n, x and y, where $[\cdot]$ is the greatest integer function. In particular, we establish a reciprocity law and give an explicit criterion for $(-11)^{[p/8]} \pmod p$.

Keywords: Congruence; quartic Jacobi symbol; octic residue; reciprocity law; binary quadratic form

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

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 [9,10,12]. From [6] 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. For $m, n \in \mathbb{Z}$ (not both zero) let (m, n) be the greatest common divisor of m and n. From [9,11,12,13] we have the following properties of the quartic Jacobi symbol:

(1.1) ([12]) Let $a, b \in \mathbb{Z}$ with $2 \nmid a$ and $2 \mid b$. Then

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

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

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

(1.2) ([12]) 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 $\big(\frac{a+bi}{c+di}\big)_4=(-1)^{\frac{a-1}{2}\cdot\frac d2}\big(\frac{c+di}{a+bi}\big)_4$.

(1.3) ([2], [9, Lemma 2.1]) Let $a,b,m\in\mathbb{Z}$ with $2\nmid m$ and $(m,a^2+b^2)=1$. Then $(\frac{a+bi}{m})_4^2=(\frac{a^2+b^2}{m})$.

(1.4) ([11, 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 $(\frac{x^2}{a+bi})_4=(\frac{x}{a^2+b^2})$.

(1.5) ([13, 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 $(\frac{c+di}{m})_4=(\frac{x(x+d)}{m})$.

For the history of quartic reciprocity laws, see [6,7]. 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 $q^{(p-1)/8}\equiv1\pmod p$. In the classical octic reciprocity laws (see [1,7]), we always write that $p=c^2+d^2=a^2+2b^2$ $(a,b,c,d\in\mathbb{Z})$.

For a prime $p=24k+1=c^2+d^2=x^2+3y^2$ with $k,c,d,x,y\in\mathbb{Z}$ and $c\equiv1\pmod 4$, by using cyclotomic numbers and Jacobi sums Hudson and Williams ([4,5]) proved that

$$3^{\frac{p-1}{8}}\equiv\begin{cases}\pm1\pmod p & \text{if } c\equiv\pm(-1)^{\frac y4}\pmod 3,\\ \pm\dfrac dc\pmod p & \text{if } d\equiv\pm(-1)^{\frac y4}\pmod 3.\end{cases}$$

Let p be a prime of the form $4k+1$ and so $p=c^2+d^2$ with $c,d\in\mathbb{Z}$, $c\equiv1\pmod 4$, $d=2^rd_0$ and $d_0\equiv1\pmod 4$. Suppose $q,x,y\in\mathbb{Z}$, $2\nmid q$, $p\nmid q$ and $p=x^2+qy^2$. Assume that $(c,x+d)=1$ or $(d_0,x+c)=1$. In [13], using (1.1)-(1.5) 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.

In 1890 Stickelberger (see [3,8]) proved the following elegant theorem.

Theorem 1.1 Let $\mathbb{Q}(\sqrt{-q})$ be an imaginary quadratic field of discriminant $-q$ and class number h. Assume that $q\neq3,4,8$. Let p be an odd prime such that $(\frac{-q}{p})=1$. Then there are integers x,y, unique up to sign, for which $4p^h=x^2+qy^2$ and $p\nmid x$.

For $q\in\{11,19,43,67,163\}$ and an odd prime p with $(\frac pq)=1$, it follows from Theorem 1.1 that $4p=x^2+qy^2$ for some $x,y\in\mathbb{Z}$.

Inspired by [13] and Theorem 1.1, in this paper we establish congruences for $(-q)^{[p/8]}\pmod p$ under the condition that $p=c^2+d^2$ and $4n^2p=x^2+qy^2$, where $p\equiv1\pmod 4$ is a prime and $q\equiv3\pmod 4$. In particular, we establish a reciprocity law and give a useful and explicit criterion for $(-11)^{[p/8]}\pmod p$, see Theorems 2.3-2.5.

2. Main results

Theorem 2.1. *Let p be a prime of the form $4m+1$ and so $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $c\equiv1\pmod 4$. Suppose that $q,n,x,y\in\mathbb{Z}$, $q\equiv3\pmod 4$, $p\nmid q$, $4n^2p=x^2+qy^2$,*

$y\equiv 1\pmod 4$, $(q,n)=(x,y)=1$, $(c,x+2nd)=1$ *and* $(\frac{2cn/(x+2dn)+i}{q})_4=i^k$. *Then*

$$(-q)^{[\frac p8]}\equiv\begin{cases}(-1)^{\frac{x-1}{2}n+\frac{x^2-1}{8}+[\frac{q+1}{8}]}(\frac{d}{c})^{k-n}\pmod p & \textit{if } 8\mid p-1,\\ (-1)^{\frac{x+1}{2}n+\frac{x-1}{2}+\frac{x^2-1}{8}+[\frac{q+1}{8}]}(\frac{d}{c})^{k-n}\frac{y}{x}\pmod p & \textit{if } 8\mid p-5.\end{cases}$$

Proof. Clearly $(n,x)^2\mid 4n^2p-x^2$ and so $(n,x)^2\mid qy^2$. Since $(q,n)=(x,y)=1$ we get $(n,x)=1$. Note that $(y,n)^2\mid x^2$ and $(x,y)=1$. We also have $(y,n)=1$. Since $4n^2p=x^2+qy^2$, $(x,y)=1$ and $p\nmid q$ we see that $2\nmid x$ and $p\nmid x$. Thus $(x,(2cn)^2+(x+2dn)^2)=(x,4n^2p)=1$. As $qy^2=(2cn)^2+(x+2dn)(2dn-x)$ we see that $(qy,x+2dn)\mid 4c^2n^2$. Recall that $(qy,n)=1$ and $(c,x+2dn)=1$. We get $(qy,x+2dn)=1$. Also,

$$\begin{aligned}&(qy^2,(2cn)^2+(x+2dn)^2)\\&=((2cn)^2+(x+2dn)^2-2x(x+2dn),(2cn)^2+(x+2dn)^2)\\&=(2x(x+2dn),(2c)^2+(x+2dn)^2)\\&=(x+2dn,(2c)^2+(x+2dn)^2)=(x+2dn,4c^2)=1.\end{aligned}$$

Since $n^2p=\frac{q+1}{4}+\frac{x^2-1}{4}+\frac{y^2-1}{4}q$ we see that $n\equiv n^2p\equiv\frac{q+1}{4}\pmod 2$. Now using (1.1)-(1.4) and the fact that $(\frac am)_4=1$ for $a,m\in\mathbb Z$ with $2\nmid m$ and $(a,m)=1$ we see that

$$\begin{aligned}i^k&=\Big(\frac{2cn+(x+2dn)i}{q}\Big)_4=\Big(\frac iq\Big)_4\Big(\frac{x+2dn-2cni}{q}\Big)_4\\
&=(-1)^{\frac{q^2-1}{8}+\frac{q-1}{2}n}\Big(\frac{q}{x+2dn-2cni}\Big)_4\\
&=(-1)^{\frac{q+1}{4}+n}\Big(\frac{qy^2}{x+2dn-2cni}\Big)_4\Big(\frac{y^2}{x+2dn-2cni}\Big)_4\\
&=\Big(\frac{(x+2dn)^2+(2cn)^2-2x(x+2dn)}{x+2dn-2cni}\Big)_4\Big(\frac{y}{(x+2dn)^2+4c^2n^2}\Big)\\
&=\Big(\frac{-2x(x+2dn)}{x+2dn-2cni}\Big)_4\Big(\frac{y}{(x+2dn)^2+4c^2n^2}\Big)\\
&=(-1)^n\Big(\frac{2}{x+2dn-2cni}\Big)_4\Big(\frac{x(x+2dn)}{x+2dn-2cni}\Big)_4\Big(\frac{y}{(x+2dn)^2+4c^2n^2}\Big)\\
&=(-1)^n i^{(-1)^{(x+1)/2}n}(-1)^{\frac{x(x+2dn)-1}{2}}\Big(\frac{x+2dn-2cni}{x(x+2dn)}\Big)_4\Big(\frac{(x+2dn)^2+4c^2n^2}{y}\Big)\\
&=(-1)^n\cdot((-1)^{\frac{x+1}{2}}i)^n\Big(\frac{2n(d-ci)}{x}\Big)_4\Big(\frac{-2cni}{x+2dn}\Big)_4\Big(\frac{2x(x+2dn)+qy^2}{y}\Big)\\
&=(-1)^{\frac{x-1}{2}n}i^n\Big(\frac{d-ci}{x}\Big)_4\Big(\frac{i}{x+2dn}\Big)_4\Big(\frac{2x(x+2dn)}{y}\Big).\end{aligned}$$

Thus, applying (1.5) we see that

$$\begin{aligned}i^k&=(-1)^{\frac{x-1}{2}n}i^n\Big(\frac{-i}{x}\Big)_4\Big(\frac{c+di}{x}\Big)_4(-1)^{\frac{(x+2dn)^2-1}{8}}\cdot(-1)^{\frac{y^2-1}{8}}\Big(\frac{x(x+2dn)}{y}\Big)\\
&=(-1)^{\frac{x-1}{2}n}i^n\cdot(-1)^{\frac{x^2-1}{8}}\Big(\frac{c+di}{x}\Big)_4(-1)^{\frac{x^2-1}{8}+\frac{dn}{2}}\cdot(-1)^{\frac{4n^2p-x^2-q}{8}}\Big(\frac{\frac{x}{2n}(\frac{x}{2n}+d)}{y}\Big)\end{aligned}$$

$$= (-1)^{\frac{x-1}{2}n+\frac{dn}{2}} i^n \cdot (-1)^{\frac{x-1}{2}\cdot\frac{d}{2}} \Big(\frac{x}{c+di}\Big)_4 (-1)^{\frac{x^2-1}{8}+[\frac{q+1}{8}]} \Big(\frac{c+di}{y}\Big)_4$$
$$= (-1)^{(\frac{x-1}{2}+\frac{d}{2})n+\frac{x-1}{2}\cdot\frac{d}{2}} i^n \Big(\frac{x}{c+di}\Big)_4 (-1)^{\frac{x^2-1}{8}+[\frac{q+1}{8}]} \Big(\frac{y}{c+di}\Big)_4$$
$$= (-1)^{(\frac{x-1}{2}+\frac{d}{2})n+\frac{x-1}{2}\cdot\frac{d}{2}} i^n \cdot (-1)^{\frac{x^2-1}{8}+[\frac{q+1}{8}]} \Big(\frac{x/y}{c+di}\Big)_4 \Big(\frac{y^2}{c+di}\Big)_4$$
$$= (-1)^{(\frac{x-1}{2}+\frac{d}{2})n+\frac{x-1}{2}\cdot\frac{d}{2}} i^n \cdot (-1)^{\frac{x^2-1}{8}+[\frac{q+1}{8}]} \Big(\frac{x/y}{c+di}\Big)_4 \Big(\frac{y}{c^2+d^2}\Big).$$

As $\big(\frac{y}{c^2+d^2}\big) = \big(\frac{c^2+d^2}{y}\big) = \big(\frac{4n^2(c^2+d^2)}{y}\big) = \big(\frac{x^2+qy^2}{y}\big) = \big(\frac{x^2}{y}\big) = 1$, from the above we deduce that

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

Clearly $(-1)^{\frac{d}{2}} = (-1)^{\frac{p-1}{4}}$ and $i \equiv d/c \pmod{c+di}$. Since $c+di$ or $-c-di$ is primary in $\mathbb{Z}[i]$, we have

$$\Big(\frac{x}{y}\Big)^{\frac{p-1}{4}} \equiv \Big(\frac{x/y}{c+di}\Big)_4 \equiv (-1)^{(\frac{x-1}{2}+\frac{d}{2})n+\frac{x-1}{2}\cdot\frac{d}{2}+\frac{x^2-1}{8}+[\frac{q+1}{8}]} \Big(\frac{d}{c}\Big)^{k-n} \pmod{c+di}.$$

Note that $(x/y)^2 \equiv -q \pmod p$ and $p = (c+di)(c-di)$. We then have

$$(-q)^{[\frac{p}{8}]} \equiv \begin{cases} (\frac{x}{y})^{\frac{p-1}{4}} \equiv (-1)^{(\frac{x-1}{2}+\frac{d}{2})n+\frac{x-1}{2}\cdot\frac{d}{2}+\frac{x^2-1}{8}+[\frac{q+1}{8}]}(\frac{d}{c})^{k-n} \pmod p \\ \qquad\qquad \text{if } 8 \mid p-1, \\ (\frac{x}{y})^{\frac{p-1}{4}}\frac{y}{x} \equiv (-1)^{(\frac{x-1}{2}+\frac{d}{2})n+\frac{x-1}{2}\cdot\frac{d}{2}+\frac{x^2-1}{8}+[\frac{q+1}{8}]}(\frac{d}{c})^{k-n}\frac{y}{x} \pmod p \\ \qquad\qquad \text{if } 8 \mid p-5. \end{cases}$$

Since $(-1)^{\frac{d}{2}} = (-1)^{\frac{p-1}{4}}$ we deduce the result.

Theorem 2.2. *Let p be a prime of the form $4m+1$ and so $p = c^2+d^2$ with $c, d \in \mathbb{Z}$ and $c \equiv 1 \pmod 4$. Suppose that $q, n, x, y \in \mathbb{Z}$, $q \equiv 3 \pmod 4$, $p \nmid q$, $4n^2p = x^2+qy^2$, $y \equiv 1 \pmod 4$, $(q,n) = (x,y) = 1$, $(d, x+2cn) = 1$ and $(\frac{-2dn/(x+2cn)+i}{q})_4 = i^k$. Then*

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

Proof. By the proof of Theorem 2.1, $2 \nmid x$, $p \nmid x$ and $(n, xy) = 1$. Thus $(x, (2dn)^2 + (x+2cn)^2) = (x, 4n^2p) = 1$. As $qy^2 = (2dn)^2 + (x+2cn)(2cn-x)$ we see that $(qy, x+2cn) \mid (2dn)^2$. Note that $(qy, n) = 1$ and $(d, x+2cn) = 1$. We get $(qy, x+2cn) = 1$. Since $(n, x+2cn) = (n, x) = 1$ and $(d, x+2cn) = 1$ we see that

$$\begin{aligned} &(qy^2, (2dn)^2 + (x+2cn)^2) \\ &= ((2dn)^2 + (x+2cn)^2 - 2x(x+2cn), (2dn)^2 + (x+2cn)^2) \\ &= (2x(x+2cn), (2dn)^2 + (x+2cn)^2) \\ &= (x+2cn, (2dn)^2 + (x+2cn)^2) = (x+2cn, (2dn)^2) = 1. \end{aligned}$$

Now using (1.1)-(1.4) and the fact that $(\frac{a}{m})_4=1$ for $a,m\in\mathbb{Z}$ with $2\nmid m$ and $(a,m)=1$ we deduce that

$$\begin{aligned} i^k&=\Big(\frac{-2dn+(x+2cn)i}{q}\Big)_4=\Big(\frac{i}{q}\Big)_4\Big(\frac{x+2cn+2dni}{q}\Big)_4\\ &=(-1)^{\frac{q^2-1}{8}}\Big(\frac{q}{x+2cn+2dni}\Big)_4=(-1)^{\frac{q+1}{4}}\Big(\frac{qy^2}{x+2cn+2dni}\Big)_4\Big(\frac{y^2}{x+2cn+2dni}\Big)_4\\ &=(-1)^n\Big(\frac{(x+2cn)^2+(2dn)^2-2x(x+2cn)}{x+2cn+2dni}\Big)_4\Big(\frac{y}{(x+2cn)^2+4d^2n^2}\Big)\\ &=(-1)^n\Big(\frac{2}{x+2cn+2dni}\Big)_4\Big(\frac{x(x+2cn)}{x+2cn+2dni}\Big)_4\Big(\frac{y}{(x+2cn)^2+4d^2n^2}\Big)\\ &=(-1)^{n+\frac{dn}{2}}\Big(\frac{x+2cn+2dni}{x(x+2cn)}\Big)_4\Big(\frac{(x+2cn)^2+4d^2n^2}{y}\Big)\\ &=(-1)^{n+\frac{p-1}{4}n}\Big(\frac{2n(c+di)}{x}\Big)_4\Big(\frac{2dni}{x+2cn}\Big)_4\Big(\frac{2x(x+2cn)+qy^2}{y}\Big). \end{aligned}$$

Thus, applying (1.5) we see that

$$\begin{aligned} i^k&=(-1)^{n+\frac{p-1}{4}n}\Big(\frac{c+di}{x}\Big)_4\Big(\frac{i}{x+2cn}\Big)_4\Big(\frac{2x(x+2cn)}{y}\Big)\\ &=(-1)^{n+\frac{p-1}{4}n}\Big(\frac{c+di}{x}\Big)_4(-1)^{\frac{(x+2cn)^2-1}{8}}\Big(\frac{2}{y}\Big)\Big(\frac{x(x+2cn)}{y}\Big)\\ &=(-1)^{n+\frac{p-1}{4}n}\Big(\frac{c+di}{x}\Big)_4(-1)^{\frac{x^2-1}{8}+\frac{cn(x+cn)}{2}}\Big(\frac{i}{y}\Big)_4\Big(\frac{\frac{x}{2n}(\frac{x}{2n}+c)}{y}\Big)\\ &=(-1)^{n+\frac{p-1}{4}n}\cdot(-1)^{\frac{x-1}{2}\cdot\frac{d}{2}}\Big(\frac{x}{c+di}\Big)_4(-1)^{\frac{x^2-1}{8}+\frac{n(x+n)}{2}}\Big(\frac{i}{y}\Big)_4\Big(\frac{d+ci}{y}\Big)_4\\ &=(-1)^{(1+\frac{p-1}{4})n+\frac{p-1}{4}\cdot\frac{x-1}{2}+\frac{x^2-1}{8}+\frac{n(x+n)}{2}}\Big(\frac{x}{c+di}\Big)_4\Big(\frac{-c+di}{y}\Big)_4\\ &=(-1)^{(1+\frac{p-1}{4})n+\frac{p-1}{4}\cdot\frac{x-1}{2}+\frac{x^2-1}{8}+\frac{n(x+n)}{2}}\Big(\frac{x}{c+di}\Big)_4\Big(\frac{c+di}{y}\Big)_4^{-1}\\ &=(-1)^{(1+\frac{p-1}{4})n+\frac{p-1}{4}\cdot\frac{x-1}{2}+\frac{x^2-1}{8}+\frac{n(x+n)}{2}}\Big(\frac{x}{c+di}\Big)_4\Big(\frac{y}{c+di}\Big)_4^{-1}\\ &=(-1)^{(1+\frac{p-1}{4})n+\frac{p-1}{4}\cdot\frac{x-1}{2}+\frac{x^2-1}{8}+\frac{n(x+n)}{2}}\Big(\frac{x/y}{c+di}\Big)_4. \end{aligned}$$

Clearly $i\equiv d/c\pmod{c+di}$. Since $c+di$ or $-c-di$ is primary in $\mathbb{Z}[i]$, we have

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

Note that $(x/y)^2\equiv-q\pmod p$ and $p=(c+di)(c-di)$. We then have

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

This is the result.

Theorem 2.3. *Let p be a prime of the form $4k+1$ and so $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $c\equiv 1\pmod 4$. Let q be a prime of the form $4k+3$. Suppose that $4n^2p=x^2+qy^2$, $n,x,y\in\mathbb{Z}$, $y\equiv 1\pmod 4$ and $(q,n)=(x,y)=1$. Assume that $(c,x+2dn)=1$ or $(d,x+2cn)=1$. Then for $m\in\mathbb{Z}$,*

$$(-q)^{[\frac{p}{8}]}\equiv\begin{cases}(-1)^{\frac{n(x+n)}{2}+\frac{x^2-1}{8}}(\frac{d}{c})^m \pmod p & \text{if } 8\mid p-1,\\ (-1)^{\frac{n(x+n)}{2}+[\frac{x}{4}]+n}(\frac{d}{c})^m\frac{y}{x} \pmod p & \text{if } 8\mid p-5\end{cases}$$
$$\iff \Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}}\equiv i^m \pmod q.$$

Proof. Clearly $q\nmid x$ and x is odd. We first assume $(c,x+2dn)=1$. By the proof of Theorem 2.1, $(q,(x+2dn)((2cn)^2+(x+2dn)^2))=1$. It is easily seen that $\frac{2cn/(x+2dn)-i}{2cn/(x+2dn)+i}=\frac{2cn-(x+2dn)i}{2cn+(x+2dn)i}\equiv\frac{2n(c-di)}{ix}\pmod q$. Thus, for $m\in\mathbb{Z}$ applying [9, Theorem 2.3(ii)] we get

$$\begin{aligned}&\Big(\frac{2cn/(x+2dn)+i}{q}\Big)_4=i^{m-\frac{q+1}{4}}\\ &\Leftrightarrow \Big(\frac{\frac{2cn}{x+2dn}-i}{\frac{2cn}{x+2dn}+i}\Big)^{\frac{q+1}{4}}\equiv i^{m-\frac{q+1}{4}}\pmod q\Leftrightarrow\Big(\frac{2n(c-di)}{ix}\Big)^{\frac{q+1}{4}}\equiv i^{m-\frac{q+1}{4}}\pmod q\\ &\Leftrightarrow\Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}}\equiv i^m\pmod q.\end{aligned}$$

Now applying Theorem 2.1 we derive that

$$\begin{aligned}&\Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}}\equiv i^m\pmod q\\ &\Leftrightarrow (-q)^{[\frac{p}{8}]}\equiv\begin{cases}(-1)^{\frac{x-1}{2}n+\frac{x^2-1}{8}+[\frac{q+1}{8}]}(\frac{d}{c})^{m-\frac{q+1}{4}-n}\pmod p & \text{if } 8\mid p-1,\\ (-1)^{\frac{x+1}{2}n+\frac{x-1}{2}+\frac{x^2-1}{8}+[\frac{q+1}{8}]}(\frac{d}{c})^{m-\frac{q+1}{4}-n}\frac{y}{x}\pmod p & \text{if } 8\mid p-5.\end{cases}\end{aligned}$$

Since $n^2p=\frac{q+1}{4}+\frac{x^2-1}{4}+\frac{y^2-1}{4}q$ we see that $n\equiv n^2p\equiv\frac{q+1}{4}\pmod 2$. Hence, $(-1)^{[\frac{q+1}{8}]}(\frac{d}{c})^{-\frac{q+1}{4}-n}\equiv(-1)^{[\frac{q+1}{8}]+\frac{1}{2}(\frac{q+1}{4}+n)}=(-1)^{[\frac{n+1}{2}]}\pmod p$. Therefore,

$$\begin{aligned}&\Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}}\equiv i^m\pmod q\\ &\Leftrightarrow (-q)^{[\frac{p}{8}]}\equiv\begin{cases}(-1)^{\frac{x-1}{2}n+\frac{x^2-1}{8}+[\frac{n+1}{2}]}(\frac{d}{c})^m\\ \quad=(-1)^{\frac{n(x+n)}{2}+\frac{x^2-1}{8}}(\frac{d}{c})^m\pmod p & \text{if } 8\mid p-1,\\ (-1)^{\frac{x+1}{2}n+\frac{x-1}{2}+\frac{x^2-1}{8}+[\frac{n+1}{2}]}(\frac{d}{c})^m\frac{y}{x}\\ \quad=(-1)^{\frac{n(x+n)}{2}+[\frac{x}{4}]+n}(\frac{d}{c})^m\frac{y}{x}\pmod p & \text{if } 8\mid p-5.\end{cases}\end{aligned}$$

Now we assume $(d,x+2cn)=1$. By the proof of Theorem 2.2, $(q,x+2cn)=(q,(2dn)^2+(x+2cn)^2)=1$. It is easily seen that $\frac{2dn+(x+2cn)i}{2dn-(x+2cn)i}\equiv\frac{2n(c-di)}{-x}\pmod q$.

Thus, for $m \in \mathbb{Z}$ applying [9, Theorem 2.3(ii)] we get

$$\Big(\frac{-2dn/(x+2cn)+i}{q}\Big)_4 = i^{m-\frac{q+1}{2}} \Leftrightarrow \Big(\frac{-\frac{2dn}{x+2cn}-i}{-\frac{2dn}{x+2cn}+i}\Big)^{\frac{q+1}{4}} \equiv i^{m-\frac{q+1}{2}} \pmod q$$

$$\Leftrightarrow \Big(\frac{2dn+(x+2cn)i}{2dn-(x+2cn)i}\Big)^{\frac{q+1}{4}} \equiv i^{m-\frac{q+1}{2}} \pmod q$$

$$\Leftrightarrow \Big(\frac{2n(c-di)}{-x}\Big)^{\frac{q+1}{4}} \equiv i^{m-\frac{q+1}{2}} \pmod q \Leftrightarrow \Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}} \equiv i^{m} \pmod q.$$

Note that $(\frac{d}{c})^{-\frac{q+1}{2}} \equiv (-1)^{\frac{q+1}{4}} = (-1)^n \pmod p$ and $(-1)^{\frac{x-1}{2}+\frac{x^2-1}{8}} = (-1)^{[\frac{x}{4}]}$. From the above and Theorem 2.2 (with $k = m - \frac{q+1}{2}$) we deduce the result, which completes the proof.

Example 2.4. Let $n = p = 29$ and $q = 59$. As $29 = 5^2 + 2^2$ and $4 \cdot 29^3 = 159^2 + 59 \cdot 35^2$, we have $c = 5,\ d = 2,\ x = 159,\ y = -35$ and $(d, x + 2cn) = 1$. It is clear that

$$\Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}} = \Big(\frac{58(5-2i)}{159}\Big)^{15} \equiv (-3+13i)^{15} \equiv (19-17i)^5 \equiv i \pmod{59}$$

and

$$(-q)^{[\frac{p}{8}]} = (-59)^3 \equiv -1 \equiv (-1)^{\frac{159+29}{2}+[\frac{159}{4}]+29} \cdot \frac{2}{5} \cdot \frac{-35}{159} \pmod{29}.$$

Thus, Theorem 2.3 is true in this case.

Corollary 2.5. *Let p be a prime of the form $12k+1$ and so $p = c^2 + d^2 = \frac{1}{4}(x^2 + 27y^2)$ with $c, d, x, y \in \mathbb{Z}$. Suppose $c \equiv y \equiv 1 \pmod 4$. Assume $(c, x + 2d) = 1$ or $(d, x + 2c) = 1$. Then*

$$(-3)^{[\frac{p}{8}]} \equiv \begin{cases} \pm(-1)^{[\frac{x}{4}]} \pmod p & \text{if } p \equiv 1 \pmod 8 \text{ and } x \equiv \pm c \pmod 3, \\ \mp(-1)^{[\frac{x}{4}]}\frac{d}{c} \pmod p & \text{if } p \equiv 1 \pmod 8 \text{ and } x \equiv \pm d \pmod 3, \\ \pm(-1)^{\frac{x^2-1}{8}}\frac{3y}{x} \pmod p & \text{if } p \equiv 5 \pmod 8 \text{ and } x \equiv \pm c \pmod 3, \\ \mp(-1)^{\frac{x^2-1}{8}}\frac{3dy}{cx} \pmod p & \text{if } p \equiv 5 \pmod 8 \text{ and } x \equiv \pm d \pmod 3. \end{cases}$$

Proof. If $x \equiv \pm c \pmod 3$, then $d^2 = p - c^2 \equiv 4p - x^2 = 27y^2 \equiv 0 \pmod 3$ and so $3 \mid d$. Thus, $\frac{2(c-di)}{x} \equiv \frac{2c}{x} \equiv \pm 2 \equiv \mp 1 \pmod 3$. If $x \equiv \pm d \pmod 3$, then $c^2 = p - d^2 \equiv 4p - x^2 = 27y^2 \equiv 0 \pmod 3$ and so $3 \mid c$. Thus, $\frac{2(c-di)}{x} \equiv \frac{-2di}{x} \equiv \pm i \pmod 3$. Now taking $q = 3$, $n = 1$ and replacing y with $-3y$ in Theorem 2.3 we deduce the result.

Corollary 2.6. *Suppose that the conditions in Theorem 2.3 hold. If $q \mid cd$, then*

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

Proof. Since $4n^2(c^2+d^2)=x^2+qy^2$ we see that $q\mid d \Leftrightarrow x\equiv \pm 2cn \pmod q$ and $q\mid c\Leftrightarrow x\equiv \pm 2dn \pmod q$. If $x\equiv \pm 2cn \pmod q$, then $\frac{2n(c-di)}{x}\equiv \pm 1 \pmod q$. If $x\equiv \pm 2dn \pmod q$, then $\frac{2n(c-di)}{x}\equiv \mp i \pmod q$. Now applying Theorem 2.3 and the fact $\frac{q+1}{4}\equiv n \pmod 2$ we deduce the result.

Theorem 2.7. *Let p be a prime of the form $4k+1$ and so $p=c^2+d^2$ with $c,d\in\mathbb{Z}$ and $c\equiv 1 \pmod 4$. Let q be a prime of the form $8k+7$. Suppose that $4n^2p=x^2+qy^2$, $n,x,y\in\mathbb{Z}$, $y\equiv 1 \pmod 4$ and $(q,n)=(x,y)=1$. Assume that $(c,x+2dn)=1$ or $(d,x+2cn)=1$. Then for $m\in\mathbb{Z}$,*

$$(-q)^{[\frac{p}{8}]}\equiv\begin{cases}(-1)^{\frac n2+\frac{x^2-1}{8}}(\frac dc)^m \pmod p & \text{if } 8\mid p-1,\\ (-1)^{\frac n2+[\frac x4]}(\frac dc)^m\frac yx \pmod p & \text{if } 8\mid p-5\end{cases}$$
$$\iff \Big(\frac{c-di}{c+di}\Big)^{\frac{q+1}{8}}\equiv i^m \pmod q.$$

Proof. Since $4n^2p=x^2+qy^2\equiv 1+7\equiv 0 \pmod 8$ we see that $2\mid n$. Observe that

$$\Big(\frac{c-di}{c+di}\Big)^{\frac{q+1}{8}}=\frac{(2n(c-di))^{\frac{q+1}{4}}}{(4n^2p)^{\frac{q+1}{8}}}\equiv\Big(\frac{2n(c-di)}{x}\Big)^{\frac{q+1}{4}} \pmod q.$$

The result follows from Theorem 2.3 immediately.

Remark 2.8 Under the conditions in Theorem 2.7, for $d\not\equiv 0 \pmod q$ we see that $(-q)^{[p/8]} \pmod p$ depends only on $c/d \pmod q$.

Example 2.9 Let $p=257$, $n=2$ and $q=31$. As $257=1^2+16^2$ and $16\cdot 257=19^2+31\cdot 11^2$, we have $c=1$, $d=16$, $x=19$ and $y=-11$. Since

$$\Big(\frac{1-16i}{1+16i}\Big)^4=\Big(\frac{-255-32i}{-255+32i}\Big)^2\equiv\Big(\frac{7+i}{7-i}\Big)^2=\frac{24+7i}{24-7i}\equiv\frac{-1+i}{-1-i}=i^3 \pmod{31},$$

by Theorem 2.7 we have

$$(-31)^{[\frac{257}{8}]}\equiv(-1)^{\frac22+\frac{19^2-1}{8}}\Big(\frac{16}{1}\Big)^3=16^2\cdot 16\equiv -16 \pmod{257}.$$

Actually $(-31)^{[\frac{257}{8}]}=31^{32}\equiv 120^8\equiv 8^4\equiv -16 \pmod{257}$.

Corollary 2.10. *Suppose that the conditions in Theorem 2.7 hold. If $c\equiv \pm d \pmod q$, then*

$$(-q)^{[\frac p8]}\equiv\begin{cases}(-1)^{\frac n2+\frac{x^2-1}{8}}(\mp\frac dc)^{\frac{q+1}{8}} \pmod p & \text{if } 8\mid p-1,\\ (-1)^{\frac n2+[\frac x4]}(\mp\frac dc)^{\frac{q+1}{8}}\frac yx \pmod p & \text{if } 8\mid p-5.\end{cases}$$

Proof. Since $c\equiv \pm d \pmod q$ we see that $\frac{c-di}{c+di}\equiv\frac{\pm1-i}{\pm1+i}=\mp i$. Now applying Theorem 2.7 we deduce the result.

Theorem 2.11. *Let p be a prime of the form $4k+1$, $p\equiv 1,3,4,5,9 \pmod{11}$ and so $p=c^2+d^2=\frac14(x^2+11y^2)$ with $c,d,x,y\in\mathbb{Z}$, $c\equiv 1 \pmod 4$, $d=2^rd_0(2\nmid d_0)$, $y=2^ty_0$ and $d_0\equiv y_0\equiv 1 \pmod 4$. Assume that $(c,x+2d)=1$ or $(d_0,x+2c)=1$.*

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

$$(-11)^{\frac{p-1}{8}} \equiv \begin{cases} \pm(-1)^{[\frac{x}{4}]} \pmod p & \text{if } 2\nmid x \text{ and } x \equiv \pm 4c, \pm 9c \pmod{11}, \\ \pm(-1)^{[\frac{x}{4}]}\dfrac{d}{c} \pmod p & \text{if } 2\nmid x \text{ and } x \equiv \pm 4d, \pm 9d \pmod{11}, \\ \mp(-1)^{[\frac{x}{8}]+\frac{y}{8}} \pmod p & \text{if } 2\mid x \text{ and } x \equiv \pm 4c, \pm 9c \pmod{11}, \\ \mp(-1)^{[\frac{x}{8}]+\frac{y}{8}}\dfrac{d}{c} \pmod p & \text{if } 2\mid x \text{ and } x \equiv \pm 4d, \pm 9d \pmod{11}. \end{cases}$$

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

$$(-11)^{\frac{p-5}{8}} \equiv \begin{cases} \mp(-1)^{\frac{x^2-1}{8}}\dfrac{y}{x} \pmod p & \text{if } 2\nmid x \text{ and } x \equiv \pm 4c, \pm 9c \pmod{11}, \\ \mp(-1)^{\frac{x^2-1}{8}}\dfrac{dy}{cx} \pmod p & \text{if } 2\nmid x \text{ and } x \equiv \pm 4d, \pm 9d \pmod{11}, \\ \mp(-1)^{\frac{p-5}{8}}\dfrac{y}{x} \pmod p & \text{if } 2\mid x \text{ and } x \equiv \pm 4c, \pm 9c \pmod{11}, \\ \mp(-1)^{\frac{p-5}{8}}\dfrac{dy}{cx} \pmod p & \text{if } 2\mid x \text{ and } x \equiv \pm 4d, \pm 9d \pmod{11}. \end{cases}$$

Proof. As $(\frac{x}{2})^2 \equiv c^2 + d^2 \pmod{11}$ and $(c-di)^3 = c(c^2-3d^2) + d(d^2-3c^2)i$, we see that

$$\Big(\frac{2(c-di)}{x}\Big)^3 \equiv \begin{cases} \mp 1 \pmod{11} & \text{if } x \equiv \pm 4c, \pm 9c \pmod{11}, \\ \mp i \pmod{11} & \text{if } x \equiv \pm 4d, \pm 9d \pmod{11}. \end{cases}$$

When $2 \nmid x$, from the above and Theorem 2.3 (with $n = 1$ and $q = 11$) we deduce the result. When $2 \mid x$ and $p \equiv 1 \pmod 8$, we have $8 \mid y$ and so $(-1)^{\frac{p-1}{8}+\frac{x/2-1}{2}} = (-1)^{\frac{(x/2)^2-1}{8}+\frac{x/2-1}{2}} = (-1)^{[\frac{x}{8}]}$. Thus, applying the above and [13, Theorem 4.1 (with $q = 11$)] we obtain the result.

Example 2.12. Let $p = 449 = (-7)^2 + 20^2$. Then $4p = 39^2 + 11 \cdot 5^2$. Since $(-7, 39 + 2 \cdot 20) = 1$ and $39 \equiv -4 \cdot (-7) \pmod{11}$, by Theorem 2.11(i) we have $(-11)^{\frac{449-1}{8}} \equiv -(-1)^{[\frac{39}{4}]} = 1 \pmod{449}$. Actually, $12^8 \equiv -11 \pmod{449}$.

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

References

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

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

[3] R.J. Evans, Classical congruences for parameters in binary quadratic forms, Finite Fields Appl. **7**(2001), 110-124.

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

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

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

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

[8] L. Stickelberger, *Über* eine Verallgemeinerung der Kreistheilung, Math. Ann. **37**(1890), 321-367.

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

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

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

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

[13] Z.H. Sun, Congruences for $q^{[p/8]} \pmod p$, Acta Arith. **159** (2013), 1-25.