ACTA ARITHMETICA
149.3 (2011)

Congruences for $(A+\sqrt{A^2+mB^2})^{(p-1)/2}$ and $(b+\sqrt{a^2+b^2})^{(p-1)/4} \pmod p$

by

Zhi-Hong Sun (Huaian)

1. Introduction. Let $\mathbb{Z}$ and $\mathbb{N}$ be the sets of integers and positive integers respectively, $i=\sqrt{-1}$ and $\mathbb{Z}[i]=\{a+bi\mid a,b\in\mathbb{Z}\}$. For $a,b\in\mathbb{Z}$, $a+bi$ is called *primary* if $b\equiv 0 \pmod 2$ and $a\equiv 1-b \pmod 4$. When π or $-\pi$ is primary in $\mathbb{Z}[i]$ and $\alpha\in\mathbb{Z}[i]$, one can define the quartic Jacobi symbol $\left(\frac{\alpha}{\pi}\right)_4$ as in [S2, S4]. For the properties of the quartic Jacobi symbol one may consult [IR], [S4, (2.1)–(2.8)] and [S4, Propositions 2.1–2.6].

For any positive integer m and $a\in\mathbb{Z}$ let $\left(\frac{a}{m}\right)$ be the Legendre–Jacobi–Kronecker symbol. (We 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 we have the following general quadratic reciprocity law:

$$\left(\frac{m}{n}\right)=\begin{cases}(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right) & \text{if } m>0 \text{ or } n>0,\\ -(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}\left(\frac{n}{m}\right) & \text{if } m<0 \text{ and } n<0.\end{cases} \tag{1.1}$$

Let $a,m,A,B,C,D\in\mathbb{Z}$ and let p be an odd prime such that $ap=C^2+mD^2$. In Section 2 we obtain congruences for $\left(\frac{A+\sqrt{A^2+mB^2}}{2}\right)^{(p-1)/2} \pmod p$ using only the quadratic reciprocity law. This generalizes the result for $m=1$ in [S5]. For example, if $p=C^2+2D^2$ is a prime of the form $8k+1$, then

$$(3\pm\sqrt{17})^{(p-1)/2}\equiv\begin{cases}\left(\frac{2C+3D}{17}\right) \pmod p & \text{if } \left(\frac{p}{17}\right)=1,\\ \left(\frac{2C+3D}{17}\right)\frac{(3\mp\sqrt{17})D}{2C} \pmod p & \text{if } \left(\frac{p}{17}\right)=-1.\end{cases}$$

Suppose p is a prime of the form $8k+1$. In Section 3, using Western's formula for octic residues, we determine $(b+\sqrt{a^2+b^2})^{(p-1)/4} \pmod p$ provided that $p=x^2+(a^2+b^2)y^2\neq a^2+b^2$, $a,b,x,y\in\mathbb{Z}$, $2\nmid a$, $4\mid b$ and a^2+b^2 is a prime. See Theorems 3.1 and 3.2. For instance, if $p\neq 17$ is a prime of the form $8k+1$ and so $p=C^2+2D^2$ for some $C,D\in\mathbb{Z}$, then

2010 *Mathematics Subject Classification*: Primary 11A15; Secondary 11A07, 11B39, 11E25.
Key words and phrases: congruence, quartic Jacobi symbol, Lucas sequence, binary quadratic form.

DOI: 10.4064/aa149-3-5

$$(4\pm\sqrt{17})^{(p-1)/4}\equiv 1 \pmod p$$
$$\Leftrightarrow\ p=x^2+17y^2\ (x,y\in\mathbb{Z}) \text{ and } (-1)^y=\Big(\frac{2C-3D}{17}\Big).$$

For $b,c\in\mathbb{Z}$ the *Lucas sequences* $\{U_n(b,c)\}$ and $\{V_n(b,c)\}$ are defined by
$$U_0(b,c)=0,\quad U_1(b,c)=1,\quad U_{n+1}(b,c)=bU_n(b,c)-cU_{n-1}(b,c)\quad (n\ge 1),$$
$$V_0(b,c)=2,\quad V_1(b,c)=b,\quad V_{n+1}(b,c)=bV_n(b,c)-cV_{n-1}(b,c)\quad (n\ge 1).$$
Let $d=b^2-4c$. It is well known that for $n\in\mathbb{N}$,

(1.2) $$U_n(b,c)=\begin{cases}\frac{1}{\sqrt d}\big\{\big(\frac{b+\sqrt d}{2}\big)^n-\big(\frac{b-\sqrt d}{2}\big)^n\big\} & \text{if } d\ne 0,\\ n\big(\frac b2\big)^{n-1} & \text{if } d=0,\end{cases}$$

(1.3) $$V_n(b,c)=\Big(\frac{b+\sqrt d}{2}\Big)^n+\Big(\frac{b-\sqrt d}{2}\Big)^n.$$

Let p be an odd prime. In Section 2 we obtain a criterion for $U_{(p-1)/4}(2A,-mB^2)\equiv 0 \pmod p$ (if $p\equiv 1 \pmod 4$) in terms of binary quadratic forms, in Section 3 we derive a criterion for $p\mid U_{(p-1)/8}(2b,-a^2)$ (if $p\equiv 1 \pmod 8$, $2\nmid a$, $4\mid b$ and a^2+b^2 is a prime), and in Section 4 we pose five conjectures concerning $V_{(p+1)/4}(k,-1) \pmod p$ (if $p\equiv 3 \pmod 4$) and $q^{[p/8]} \pmod p$ (if $p\equiv 1 \pmod 4$ and $q\equiv 3 \pmod 4$), where $[x]$ is the greatest integer not exceeding x.

Throughout the paper we use (m,n) to denote the greatest common divisor of integers m and n.

2. Congruences for $\big(\frac{A+\sqrt{A^2+mB^2}}{2}\big)^{(p-1)/2} \pmod p$. For complex numbers A,B,C,D and m it is clear that

(2.1) $$(A^2+mB^2)(C^2+mD^2)=(AC-mBD)^2+m(AD+BC)^2.$$

LEMMA 2.1. *Suppose $A,B,C,D,m\in\mathbb{Z}$, $A^2+mB^2\ne 0$, $C^2+mD^2>1$, $(A,B)=(C,D)=1$, $2\nmid C^2+mD^2$ and $(A^2+mB^2,C^2+mD^2)=1$. Let*
$$\delta_0=\begin{cases}1 & \text{if } A^2+mB^2>0 \text{ or } AD+BC>0,\\ -1 & \text{if } A^2+mB^2<0 \text{ and } AD+BC<0.\end{cases}$$
Then
$$\delta_0\Big(\frac{AD+BC}{C^2+mD^2}\Big)=\begin{cases}(-1)^{\frac{AD+BC}{2}m}\big(\frac{AD+BC}{A^2+mB^2}\big) & \text{if } AD+BC\equiv 0 \pmod 2,\\ \big(\frac{AD+BC}{A^2+mB^2}\big) & \text{if } AD+BC\equiv 1 \pmod 4,\\ (-1)^{[m/2]D}\big(\frac{-AD-BC}{A^2+mB^2}\big) & \text{if } AD+BC\equiv 3 \pmod 4.\end{cases}$$

Proof. If q is a prime with $q\mid (AD+BC,C^2+mD^2)$, then $D^2(A^2+mB^2)\equiv B^2C^2+mB^2D^2=B^2(C^2+mD^2)\equiv 0 \pmod q$. As $(A^2+mB^2,C^2+mD^2)=1$, we have $q\nmid A^2+mB^2$ and hence $q\mid D$. Thus, $C^2\equiv -mD^2\equiv 0 \pmod q$

and so $q \mid C$. Since $(C, D) = 1$, this is impossible. Therefore, $(AD + BC, C^2 + mD^2) = 1$. By symmetry, we also have $(AD + BC, A^2 + mB^2) = 1$.

Suppose $AD + BC = 2^{\alpha_1} n_1$ $(2 \nmid n_1)$ and $A^2 + mB^2 = 2^{\alpha} n$ $(2 \nmid n)$. By (1.1) and (2.1) we obtain

$$\begin{aligned}
&\Big(\frac{AD+BC}{C^2+mD^2}\Big)\Big(\frac{2^{\alpha_1}}{C^2+mD^2}\Big)\\
&\quad = \Big(\frac{n_1}{C^2+mD^2}\Big) = (-1)^{\frac{n_1-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{C^2+mD^2}{n_1}\Big)\\
&\quad = (-1)^{\frac{n_1-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{A^2+mB^2}{n_1}\Big)\Big(\frac{(A^2+mB^2)(C^2+mD^2)}{n_1}\Big)\\
&\quad = (-1)^{\frac{n_1-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{2^{\alpha}n}{n_1}\Big)\Big(\frac{(AC-mBD)^2+m(AD+BC)^2}{n_1}\Big)\\
&\quad = (-1)^{\frac{n_1-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{2}{n_1}\Big)^{\alpha}\Big(\frac{n}{n_1}\Big)\Big(\frac{(AC-mBD)^2}{n_1}\Big)\\
&\quad = (-1)^{\frac{n_1-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{2}{n_1}\Big)^{\alpha}\delta_0(-1)^{\frac{n_1-1}{2}\cdot\frac{n-1}{2}}\Big(\frac{n_1}{n}\Big)\\
&\quad = \delta_0(-1)^{\frac{n_1-1}{2}\cdot\frac{C^2+mD^2-n}{2}}\Big(\frac{2}{n_1}\Big)^{\alpha}\Big(\frac{2}{n}\Big)^{\alpha_1}\Big(\frac{AD+BC}{n}\Big).
\end{aligned}$$

Hence

$$\begin{aligned}
(2.2)\qquad &\delta_0\Big(\frac{AD+BC}{C^2+mD^2}\Big)\\
&\quad = (-1)^{\frac{n_1-1}{2}\cdot\frac{(C^2+mD^2)n-1}{2}}\Big(\frac{2}{(C^2+mD^2)n}\Big)^{\alpha_1}\Big(\frac{2}{n_1}\Big)^{\alpha}\Big(\frac{AD+BC}{n}\Big).
\end{aligned}$$

If $2 \mid AD + BC$, as $(AD + BC, A^2 + mB^2) = 1$ we have $2 \nmid A^2 + mB^2$. Thus, $\alpha = 0$, $n = A^2 + mB^2$ and $2 \nmid (C^2 + mD^2)n$. By (2.1) we have

$$\begin{aligned}
&(C^2+mD^2)n\\
&\quad = (A^2+mB^2)(C^2+mD^2) = (AC-mBD)^2+m(AD+BC)^2\\
&\quad \equiv \begin{cases} 1 \pmod 8 & \text{if } AD+BC \equiv 0 \pmod 4,\\ 1+4m \pmod 8 & \text{if } AD+BC \equiv 2 \pmod 4.\end{cases}
\end{aligned}$$

Thus,

$$\begin{aligned}
&(-1)^{\frac{n_1-1}{2}\cdot\frac{(C^2+mD^2)n-1}{2}}\Big(\frac{2}{(C^2+mD^2)n}\Big)^{\alpha_1}\\
&\quad = \Big(\frac{2}{(C^2+mD^2)n}\Big)^{\alpha_1} = \begin{cases} 1 & \text{if } AD+BC \equiv 0 \pmod 4,\\ \big(\frac{2}{1+4m}\big) = (-1)^m & \text{if } AD+BC \equiv 2 \pmod 4.\end{cases}
\end{aligned}$$

Hence, by (2.2) we deduce the result.

Now assume $AD+BC \equiv 1 \pmod 4$. Then $\alpha_1 = 0$ and $n_1 = AD+BC \equiv 1 \pmod 4$. Observe that

$$\Big(\frac{2}{n_1}\Big)^{\alpha}\Big(\frac{AD+BC}{n}\Big) = \Big(\frac{2}{AD+BC}\Big)^{\alpha}\Big(\frac{AD+BC}{n}\Big) = \Big(\frac{AD+BC}{2}\Big)^{\alpha}\Big(\frac{AD+BC}{n}\Big) = \Big(\frac{AD+BC}{A^2+mB^2}\Big).$$

Again by (2.2) we deduce the result.

Finally we assume $AD+BC \equiv 3 \pmod 4$. Then $A(-D)+B(-C) \equiv 1 \pmod 4$. From the above we deduce

$$\delta_0\Big(\frac{AD+BC}{C^2+mD^2}\Big) = (-1)^{\frac{C^2+mD^2-1}{2}}\Big(\frac{A(-D)+B(-C)}{A^2+mB^2}\Big).$$

As $(C,D)=1$ and $2 \nmid C^2+mD^2$, we see that $\frac{C^2+mD^2-1}{2} \equiv \big[\frac{m}{2}\big]D \pmod 2$. So the result follows. The proof is now complete.

Lemma 2.2. *Let $C, D, m \in \mathbb{Z}$ with $(C,D)=1$ and $C^2+mD^2 \in \{3,5,7,\dots\}$. Then*

$$\Big(\frac{D}{C^2+mD^2}\Big) = \begin{cases} 1 & \text{if } 4 \mid D, \\ (-1)^m & \text{if } 4 \mid D-2, \\ (-1)^{\frac{D-1}{2}\cdot[\frac{m}{2}]} & \text{if } 2 \nmid D. \end{cases}$$

Proof. Set $D = 2^{\alpha}D_0$ $(2 \nmid D_0)$. If $4 \mid D$, then $C^2+mD^2 \equiv C^2 \equiv 1 \pmod 8$ and so

$$\Big(\frac{D}{C^2+mD^2}\Big) = \Big(\frac{D_0}{C^2+mD^2}\Big) = \Big(\frac{C^2+mD^2}{D_0}\Big) = \Big(\frac{C^2}{D_0}\Big) = 1.$$

If $4 \mid D-2$, then $C^2+mD^2 \equiv 1+4m \pmod 8$ and so

$$\Big(\frac{D}{C^2+mD^2}\Big) = \Big(\frac{2D_0}{C^2+mD^2}\Big) = \Big(\frac{2}{1+4m}\Big)\Big(\frac{C^2+mD^2}{D_0}\Big) = (-1)^m.$$

If $2 \nmid D$, then

$$\begin{aligned}\Big(\frac{D}{C^2+mD^2}\Big) &= (-1)^{\frac{D-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{C^2+mD^2}{D}\Big) = (-1)^{\frac{D-1}{2}\cdot\frac{C^2+mD^2-1}{2}}\Big(\frac{C^2}{D}\Big) \\ &= (-1)^{\frac{D-1}{2}\cdot\frac{C^2+m-1}{2}} = (-1)^{\frac{D-1}{2}\cdot[\frac{m}{2}]}.\end{aligned}$$

So the lemma is proved.

Lemma 2.3. *Let $b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. Let p be an odd prime such that $p \nmid c(b^2-4c)$. Then*

$$p \mid U_n(b,c) \ \Leftrightarrow \ \Big(\frac{b+\sqrt{b^2-4c}}{2}\Big)^{2n} \equiv c^n \pmod p.$$

Proof. From (1.2) we have

$$\begin{aligned} p \mid U_n(b,c) \ &\Leftrightarrow \ \Big(\frac{b+\sqrt{b^2-4c}}{2}\Big)^{n} \equiv \Big(\frac{b-\sqrt{b^2-4c}}{2}\Big)^{n} \pmod p \\ &\Leftrightarrow \ \Big(\frac{b+\sqrt{b^2-4c}}{2}\Big)^{2n} \equiv \Big(\frac{b^2-(b^2-4c)}{4}\Big)^{n} = c^n \pmod p. \end{aligned}$$

This proves the lemma.

For complex numbers A, B and m it is clear that

$$(2.3) \quad (A+B\sqrt{-m})\,\frac{A+\sqrt{A^2+mB^2}}{2} = \Big(\frac{A+B\sqrt{-m}+\sqrt{A^2+mB^2}}{2}\Big)^2.$$

Now using Lemmas 2.1–2.3 and (2.3) we deduce the following main result.

Theorem 2.1. *Let p be an odd prime, $a, m, C, D \in \mathbb{Z}$, $a > 0$, $2 \nmid a$, $(C, D) = 1$ and $ap = C^2 + mD^2$. Let $A, B \in \mathbb{Z}$ with $(A, B) = 1$, $p \nmid mB$ and $(A^2 + mB^2, ap) = 1$. Suppose that δ_0 is given in Lemma 2.1. Let*

$$\delta_1 = \begin{cases} (-1)^{\frac{D}{2}m} & \text{if } 2 \mid D, \\ (-1)^{\frac{D-1}{2}\cdot[\frac{m}{2}]} & \text{if } 2 \nmid D, \end{cases}$$

$$\delta_2 = \begin{cases} 1 & \text{if } AD+BC \equiv 0, 1 \pmod 4, \\ (-1)^m & \text{if } AD+BC \equiv 2 \pmod 4, \\ (-1)^{[\frac{m}{2}]D} & \text{if } AD+BC \equiv 3 \pmod 4, \end{cases}$$

$$\varepsilon = \begin{cases} \delta_0\delta_1\delta_2\big(\frac{AD+BC}{A^2+mB^2}\big) & \text{if } AD+BC \not\equiv 3 \pmod 4, \\ \delta_0\delta_1\delta_2\big(\frac{-AD-BC}{A^2+mB^2}\big) & \text{if } AD+BC \equiv 3 \pmod 4. \end{cases}$$

Then

$$\Big(\frac{A \pm \sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2} \equiv \begin{cases} \varepsilon\big(\frac{D(AD+BC)}{a}\big) \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big) = 1, \\ \varepsilon\big(\frac{D(AD+BC)}{a}\big)\frac{D(A\mp\sqrt{A^2+mB^2})}{BC} \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big) = -1. \end{cases}$$

Moreover, if $p\equiv 1\pmod 4$*, then*

$$p\,|\,U_{(p-1)/4}(2A,-mB^2)\iff \Big(\frac{A^2+mB^2}{p}\Big)=1 \text{ and } \varepsilon\Big(\frac{D(AD+BC)}{a}\Big)=\Big(\frac{2BCD}{p}\Big).$$

Proof. As $(\frac{-m}{p})=1$ and $(\sqrt{x})^p=\sqrt{x}\cdot x^{(p-1)/2}\equiv(\frac{x}{p})\sqrt{x}\pmod p$ for $x\in\mathbb{Z}$, using the binomial theorem and Fermat's little theorem we see that

$$\begin{aligned}(A+B\sqrt{-m}+\sqrt{A^2+mB^2})^p &\equiv A^p+(B\sqrt{-m})^p+(\sqrt{A^2+mB^2})^p\\ &\equiv A+B\sqrt{-m}+\Big(\frac{A^2+mB^2}{p}\Big)\sqrt{A^2+mB^2}\pmod p.\end{aligned}$$

Thus,

$$\begin{aligned}\Big(\frac{A+B\sqrt{-m}+\sqrt{A^2+mB^2}}{2}\Big)^{p-1} &\equiv \frac{(A+B\sqrt{-m}+\sqrt{A^2+mB^2})^p}{A+B\sqrt{-m}+\sqrt{A^2+mB^2}}\\ &\equiv \frac{A+B\sqrt{-m}+(\frac{A^2+mB^2}{p})\sqrt{A^2+mB^2}}{A+B\sqrt{-m}+\sqrt{A^2+mB^2}}\\ &\equiv\begin{cases}\frac{A-\sqrt{A^2+mB^2}}{B\sqrt{-m}}\pmod p & \text{if } (\frac{A^2+mB^2}{p})=-1,\\ 1\pmod p & \text{if } (\frac{A^2+mB^2}{p})=1.\end{cases}\end{aligned}$$

Hence applying (2.3) we obtain

$$\begin{aligned}(A+B\sqrt{-m})^{(p-1)/2}&\Big(\frac{A+\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2}\\ &\equiv\begin{cases}\frac{A-\sqrt{A^2+mB^2}}{B\sqrt{-m}}\pmod p & \text{if } (\frac{A^2+mB^2}{p})=-1,\\ 1\pmod p & \text{if } (\frac{A^2+mB^2}{p})=1.\end{cases}\end{aligned}$$

As $(C/D)^2\equiv -m\pmod p$, replacing $\sqrt{-m}$ with C/D in the congruence we have

$$\begin{aligned}\Big(\frac{A+\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2}&\Big(A+\frac{BC}{D}\Big)^{(p-1)/2}\\ &\equiv\begin{cases}\frac{A-\sqrt{A^2+mB^2}}{BC/D}\pmod p & \text{if } (\frac{A^2+mB^2}{p})=-1,\\ 1\pmod p & \text{if } (\frac{A^2+mB^2}{p})=1.\end{cases}\end{aligned}$$

Using Lemmas 2.1 and 2.2 we have

$$\begin{aligned}(A+BC/D)^{(p-1)/2} &\equiv \Big(\frac{A+BC/D}{p}\Big)=\Big(\frac{D}{p}\Big)\Big(\frac{AD+BC}{p}\Big)\\ &=\Big(\frac{D}{a}\Big)\Big(\frac{AD+BC}{a}\Big)\Big(\frac{D}{ap}\Big)\Big(\frac{AD+BC}{ap}\Big)\\ &=\Big(\frac{D}{a}\Big)\Big(\frac{AD+BC}{a}\Big)\Big(\frac{D}{C^2+mD^2}\Big)\Big(\frac{AD+BC}{C^2+mD^2}\Big)\\ &=\varepsilon\Big(\frac{D(AD+BC)}{a}\Big) \pmod p.\end{aligned}$$

Now combining the above we deduce

$$\begin{aligned}&\Big(\frac{A+\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2}\\ &\quad\equiv\begin{cases}\varepsilon\big(\frac{D(AD+BC)}{a}\big) \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=1,\\ \varepsilon\big(\frac{D(AD+BC)}{a}\big)\frac{D(A-\sqrt{A^2+mB^2})}{BC} \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=-1.\end{cases}\end{aligned}$$

Since $ap=C^2+mD^2$ we see that $\big(\frac{-m}{p}\big)=1$ and so

$$\begin{aligned}&\Big(\frac{A+\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2}\Big(\frac{A-\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2}\\ &\qquad\qquad=\Big(-\frac{mB^2}{4}\Big)^{(p-1)/2}\equiv 1 \pmod p.\end{aligned}$$

We also have

$$\frac{D(A+\sqrt{A^2+mB^2})}{BC}\cdot\frac{D(A-\sqrt{A^2+mB^2})}{BC}=\frac{-mB^2D^2}{B^2C^2}\equiv 1 \pmod p.$$

Therefore,

$$\begin{aligned}&\Big(\frac{A-\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2}\\ &\quad\equiv\begin{cases}\varepsilon\big(\frac{D(AD+BC)}{a}\big) \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=1,\\ \varepsilon\big(\frac{D(AD+BC)}{a}\big)\frac{D(A+\sqrt{A^2+mB^2})}{BC} \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=-1.\end{cases}\end{aligned}$$

Now we assume $p\equiv 1 \pmod 4$. From the above and Lemma 2.3 we see that

$$\begin{aligned} &p \mid U_{(p-1)/4}(2A, -mB^2) \\ &\Leftrightarrow\ (A+\sqrt{A^2+mB^2})^{(p-1)/2} \equiv (-mB^2)^{(p-1)/4} \equiv \Big(\frac{BC}{D}\Big)^{(p-1)/2} \pmod p \\ &\Leftrightarrow\ \Big(\frac{A+\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2} \equiv \Big(\frac{2BCD}{p}\Big) \pmod p \\ &\Leftrightarrow\ \Big(\frac{2BCD}{p}\Big)\varepsilon\Big(\frac{D(AD+BC)}{a}\Big) \\ &\qquad \equiv \begin{cases} 1 \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=1, \\ \frac{D(A-\sqrt{A^2+mB^2})}{BC} \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=-1. \end{cases} \end{aligned}$$

Since $p \nmid mB(A^2+mB^2)$ we have $A \not\equiv \pm\sqrt{A^2+mB^2} \pmod p$ and so $A^2 + mB^2 - A\sqrt{A^2+mB^2} \not\equiv 0 \pmod p$. Thus

$$\Big(\frac{D(A-\sqrt{A^2+mB^2})}{BC}\Big)^2 \equiv \frac{2A^2+mB^2-2A\sqrt{A^2+mB^2}}{-mB^2} \not\equiv 1 \pmod p$$

and so $\frac{D(A-\sqrt{A^2+mB^2})}{BC} \not\equiv \pm 1 \pmod p$. Hence,

$$\begin{aligned} &p \mid U_{(p-1)/4}(2A, -mB^2) \\ &\qquad \Leftrightarrow\ \Big(\frac{A^2+mB^2}{p}\Big) = 1 \text{ and } \varepsilon\Big(\frac{D(AD+BC)}{a}\Big) = \Big(\frac{2BCD}{p}\Big). \end{aligned}$$

The proof is now complete.

REMARK 2.1. From (2.1) we see that $(AD+BC, AC-mBD)=1$ implies $(AD+BC, (A^2+mB^2)(C^2+mD^2))=1$. Thus, according to the proof of Lemma 2.1, we may replace the condition $(A^2+mB^2, C^2+mD^2)=1$ with $(AD+BC, AC-mBD)=1$ in Lemma 2.1. Hence, by the proof of Theorem 2.1, we may replace the condition $(A^2+mB^2, ap)=1$ with $(AD+BC, AC-mBD)=1$ in Theorem 2.1.

COROLLARY 2.1. *Let p be an odd prime, $m \in \{2,4,6,\dots\}$ and $p = C^2 + mD^2$ for some $C, D \in \mathbb{Z}$. Suppose $A, B \in \mathbb{Z}$, $(A,B)=1$, $p \nmid B(A^2+mB^2)$ and $AD+BC \not\equiv 3 \pmod 4$. Then*

$$\begin{aligned} &\Big(\frac{A\pm\sqrt{A^2+mB^2}}{2}\Big)^{(p-1)/2} \\ &\equiv \begin{cases} (-1)^{\frac{1-(-1)^D}{2}\cdot\frac{D-1}{2}\cdot\frac{m}{2}}\big(\frac{AD+BC}{A^2+mB^2}\big) \pmod p & \text{if } \big(\frac{A^2+mB^2}{p}\big)=1, \\ (-1)^{\frac{1-(-1)^D}{2}\cdot\frac{D-1}{2}\cdot\frac{m}{2}}\big(\frac{AD+BC}{A^2+mB^2}\big)\frac{D(A\mp\sqrt{A^2+mB^2})}{BC} \pmod p & \\ & \text{if } \big(\frac{A^2+mB^2}{p}\big)=-1. \end{cases} \end{aligned}$$

Moreover, if $p \equiv 1 \pmod 4$, *then*

$$p \mid U_{(p-1)/4}(2A, -mB^2) \Leftrightarrow \left(\frac{A^2+mB^2}{p}\right) = 1 \text{ and } (-1)^{\frac{1-(-1)^D}{2}\cdot\frac{D-1}{2}\cdot\frac{m}{2}}\left(\frac{AD+BC}{A^2+mB^2}\right) = \left(\frac{2B}{p}\right)\left(\frac{m}{C}\right).$$

Proof. For $p \equiv 1 \pmod 4$ we have $\left(\frac{C}{p}\right) = \left(\frac{p}{C}\right) = \left(\frac{C^2+mD^2}{C}\right) = \left(\frac{m}{C}\right)$ and $\left(\frac{D}{p}\right) = \left(\frac{p}{D}\right) = \left(\frac{C^2+mD^2}{D}\right) = \left(\frac{C^2}{D}\right) = 1$. Thus, taking $a = 1$ in Theorem 2.1 we deduce the result.

Corollary 2.2. *Let* p *be a prime of the form* $8k+1$ *and so* $p = C^2+2D^2$ *for some* $C, D \in \mathbb{Z}$. *Suppose* $A, B \in \mathbb{Z}$, $(A,B) = 1$, $p \nmid B(A^2+2B^2)$ *and* $AD+BC \not\equiv 3 \pmod 4$. *Then*

$$\left(A \pm \sqrt{A^2+2B^2}\right)^{(p-1)/2} \equiv \begin{cases} \left(\frac{AD+BC}{A^2+2B^2}\right) \pmod p & \text{if } \left(\frac{p}{A^2+2B^2}\right) = 1, \\ \left(\frac{AD+BC}{A^2+2B^2}\right)\frac{D(A\mp\sqrt{A^2+2B^2})}{BC} \pmod p & \text{if } \left(\frac{p}{A^2+2B^2}\right) = -1. \end{cases}$$

Moreover, if $p \equiv 1 \pmod 4$, *then*

$$p \mid U_{(p-1)/4}(2A, -2B^2) \Leftrightarrow \left(\frac{p}{A^2+2B^2}\right) = 1 \text{ and } \left(\frac{AD+BC}{A^2+2B^2}\right) = \left(\frac{B}{p}\right)\left(\frac{2}{C}\right).$$

Proof. If $2 \nmid D$, then $p = C^2+2D^2 \equiv 1+2 = 3 \pmod 8$. Thus $2 \mid D$. Now putting $m = 2$ in Corollary 2.1 and noting that $\left(\frac{A^2+2B^2}{p}\right) = \left(\frac{p}{A^2+2B^2}\right)$ we deduce the result.

For instance, if $p = C^2+2D^2$ is a prime of the form $8k+1$, then

$$(2.4)\qquad (3 \pm \sqrt{17})^{(p-1)/2} \equiv \begin{cases} \left(\frac{2C+3D}{17}\right) \pmod p & \text{if } \left(\frac{p}{17}\right) = 1, \\ \left(\frac{2C+3D}{17}\right)\frac{(3\mp\sqrt{17})D}{2C} \pmod p & \text{if } \left(\frac{p}{17}\right) = -1 \end{cases}$$

and

$$(2.5)\qquad p \mid U_{(p-1)/4}(3,-2) \Leftrightarrow p \mid U_{(p-1)/4}(6,-8) \Leftrightarrow \left(\frac{p}{17}\right) = 1 \text{ and } \left(\frac{2C+3D}{17}\right) = \left(\frac{2}{C}\right).$$

Corollary 2.3. *Let* $p \equiv 1, 3, 7, 9 \pmod{20}$ *be a prime different from* 7.

(i) *If* $p \equiv 1, 9 \pmod{20}$ *and hence* $p = C^2+5D^2$ *with* $C, D \in \mathbb{Z}$ *and* $C + D \equiv 1 \pmod 4$, *then*

$$\left(\frac{1 \pm \sqrt{6}}{2}\right)^{(p-1)/2} \equiv \begin{cases} \delta_1\left(\frac{C+D}{6}\right) \pmod p & \text{if } \left(\frac{6}{p}\right) = 1, \\ \delta_1\left(\frac{C+D}{6}\right)\frac{D}{C}(1 \mp \sqrt{6}) \pmod p & \text{if } \left(\frac{6}{p}\right) = -1 \end{cases}$$

and

$$p\,|\,U_{(p-1)/4}(2,-5)\Leftrightarrow\Big(\frac{6}{p}\Big)=1\ \textit{and}\ \delta_1\Big(\frac{C+D}{6}\Big)=(-1)^{\frac{p-1}{4}D}\Big(\frac{C}{5}\Big),$$

where $\delta_1=1$ *or* -1 *according as* $4\nmid D-2$ *or* $4\,|\,D-2$.

(ii) *If* $p\equiv 3,7\pmod{20}$ *and hence* $7p=C^2+5D^2$ *with* $C,D\in\mathbb{Z}$ *and* $C+D\equiv 1\pmod 4$, *then*

$$\Big(\frac{1\pm\sqrt{6}}{2}\Big)^{(p-1)/2}\equiv\begin{cases}\delta_1\big(\frac{C+D}{6}\big)\big(\frac{D(C+D)}{7}\big)\pmod p & \textit{if } \big(\frac{6}{p}\big)=1,\\ \delta_1\big(\frac{C+D}{6}\big)\big(\frac{D(C+D)}{7}\big)\frac{D}{C}(1\mp\sqrt{6})\pmod p & \textit{if } \big(\frac{6}{p}\big)=-1,\end{cases}$$

where $\delta_1=1$ *or* -1 *according as* $4\nmid D-2$ *or* $4\,|\,D-2$.

Proof. If $p=C^2+5D^2$ with $C,D\in\mathbb{Z}$ and $D=2^\alpha D_0$ $(2\nmid D_0)$, then clearly $\big(\frac{C}{p}\big)=\big(\frac{p}{C}\big)=\big(\frac{5}{C}\big)=\big(\frac{C}{5}\big)$ and $\big(\frac{2D}{p}\big)=\big(\frac{2^{\alpha+1}}{p}\big)\big(\frac{D_0}{p}\big)=\big(\frac{2}{p}\big)^{\alpha+1}\big(\frac{p}{D_0}\big)=(-1)^{(p-1)(\alpha+1)/4}=(-1)^{(p-1)D/4}$. Thus, putting $a=A=B=1$ and $m=5$ in Theorem 2.1 we deduce (i). Taking $a=7$, $A=B=1$ and $m=5$ in Theorem 2.1 we deduce (ii).

Corollary 2.4. *Let* $p\equiv 1,2,4\pmod 7$ *be an odd prime and hence* $p=C^2+7D^2$ *for some* $C,D\in\mathbb{Z}$. *Suppose* $C+D\equiv 1\pmod 4$. *Then*

$$(1\pm 2\sqrt{2})^{(p-1)/2}\equiv\begin{cases}(-1)^{\frac{D(D-1)}{2}+\frac{C+D-1}{4}}\pmod p & \textit{if } p\equiv\pm 1\pmod 8,\\ (-1)^{\frac{D(D-1)}{2}+\frac{C+D-1}{4}}\frac{D}{C}(-1\pm 2\sqrt{2})\pmod p & \textit{if } p\equiv\pm 3\pmod 8.\end{cases}$$

Moreover, if $p\equiv 1\pmod 4$, *then*

$$p\,|\,U_{(p-1)/4}(2,-7)\ \Leftrightarrow\ 8\,|\,p-1\ \textit{and}\ (-1)^{\frac{D(D-1)}{2}+\frac{C+D-1}{4}}=(-1)^{(C-1)/2}\Big(\frac{C}{7}\Big).$$

Proof. Taking $a=A=B=1$ and $m=7$ in Theorem 2.1 we obtain the congruence for $(1\pm 2\sqrt{2})^{(p-1)/2}\pmod p$. For $p\equiv 1\pmod 8$ and $D=2^\alpha D_0$ $(2\nmid D_0)$, it is clear that

$$2\nmid C,\quad \Big(\frac{C}{p}\Big)=\Big(\frac{p}{C}\Big)=\Big(\frac{C^2+7D^2}{C}\Big)=\Big(\frac{7}{C}\Big)=(-1)^{(C-1)/2}\Big(\frac{C}{7}\Big)$$

and

$$\Big(\frac{D}{p}\Big)=\Big(\frac{D_0}{p}\Big)=\Big(\frac{p}{D_0}\Big)=\Big(\frac{C^2+7D^2}{D_0}\Big)=\Big(\frac{C^2}{D_0}\Big)=1.$$

Thus, by Theorem 2.1 we have

$$\begin{aligned}&p\,|\,U_{(p-1)/4}(2,-7)\\ \Leftrightarrow\ &8\,|\,p-1\text{ and }(-1)^{\frac{D(D-1)}{2}+\frac{C+D-1}{4}}=\Big(\frac{2CD}{p}\Big)=(-1)^{(C-1)/2}\Big(\frac{C}{7}\Big).\end{aligned}$$

This completes the proof.

COROLLARY 2.5. *Let $p\equiv 1,3 \pmod 8$ be a prime and hence $p=C^2+2D^2$ for some $C,D\in\mathbb{Z}$.*

(i) *If $p\equiv 1 \pmod 8$ and $C+D\equiv 1 \pmod 4$, then*

$$(2\pm\sqrt{3})^{(p-1)/4} \equiv \begin{cases} (-1)^{(C^2-1)/8}\left(\frac{C}{3}\right) \pmod p & \text{if } p\equiv 1 \pmod{24},\\ (-1)^{(C^2-1)/8}\left(\frac{D}{3}\right)\frac{D}{C}(1\mp\sqrt{3}) \pmod p & \text{if } p\equiv 17 \pmod{24}\end{cases}$$

and so

$$p\mid U_{(p-1)/8}(4,1) \iff \left(\frac{C}{3}\right)=(-1)^{(C^2-1)/8}.$$

(ii) *If $p\equiv 3 \pmod 8$, $p>3$ and $C\equiv D\equiv 1 \pmod 4$, then*

$$(2\pm\sqrt{3})^{(p+1)/4} \equiv \begin{cases} (-1)^{(C-1)/4}\left(\frac{C}{3}\right) \pmod p & \text{if } p\equiv 19 \pmod{24},\\ (-1)^{(C-1)/4}\left(\frac{D}{3}\right)\frac{D}{C}(1\pm\sqrt{3}) \pmod p & \text{if } p\equiv 11 \pmod{24}.\end{cases}$$

Proof. If $p\equiv 1 \pmod 8$, then $2\mid D$. If $p\equiv 3 \pmod 8$, then $2\nmid D$. Thus, putting $A=B=1$ and $m=2$ in Corollary 2.1 we see that

$$\left(\frac{1\pm\sqrt{3}}{2}\right)^{(p-1)/2} \equiv \begin{cases} \left(\frac{C+D}{3}\right) \pmod p & \text{if } \left(\frac{3}{p}\right)=1,\\ \left(\frac{C+D}{3}\right)\frac{D}{C}(1\mp\sqrt{3}) \pmod p & \text{if } \left(\frac{3}{p}\right)=-1.\end{cases}$$

If $p\equiv 1 \pmod 3$, then $3\mid D$ and $\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)=(-1)^{(p-1)/2}$. If $p\equiv 2 \pmod 3$, then $3\mid C$ and $\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)=-(-1)^{(p-1)/2}$. Thus,

$$\left(\frac{1\pm\sqrt{3}}{2}\right)^{(p-1)/2} \equiv \begin{cases} \left(\frac{C}{3}\right) \pmod p & \text{if } p\equiv 1 \pmod{24},\\ \left(\frac{D}{3}\right)\frac{D}{C}(1\mp\sqrt{3}) \pmod p & \text{if } p\equiv 17 \pmod{24},\\ \left(\frac{D}{3}\right) \pmod p & \text{if } p\equiv 11 \pmod{24},\\ \left(\frac{C}{3}\right)\frac{D}{C}(1\mp\sqrt{3}) \pmod p & \text{if } p\equiv 19 \pmod{24}.\end{cases}$$

If $p\equiv 1 \pmod 8$, by [S5, p. 1317] we have $2^{(p-1)/4}\equiv(-1)^{(C^2-1)/8} \pmod p$ and so

$$\left(\frac{1\pm\sqrt{3}}{2}\right)^{(p-1)/2} = \left(\frac{2\pm\sqrt{3}}{2}\right)^{(p-1)/4} \equiv (-1)^{(C^2-1)/8}(2\pm\sqrt{3})^{(p-1)/4} \pmod p.$$

Thus, from the above we obtain the congruence for $(2\pm\sqrt{3})^{(p-1)/4} \pmod p$.

Applying Lemma 2.3 we see that

$$\begin{aligned} p \mid U_{(p-1)/8}(4,1) &\Leftrightarrow (2+\sqrt{3})^{(p-1)/4} \equiv 1 \pmod p \\ &\Leftrightarrow p \equiv 1 \pmod{24} \text{ and } (-1)^{(C^2-1)/8}\Big(\frac{C}{3}\Big) \equiv 1 \pmod p \\ &\Leftrightarrow \Big(\frac{C}{3}\Big) = (-1)^{(C^2-1)/8}. \end{aligned}$$

Now assume $p \equiv 3 \pmod 8$ and $C \equiv D \equiv 1 \pmod 4$. By [S5, p. 1317] again, we have $2^{(p-3)/4} \equiv (-1)^{(C-1)/2+(C^2-1)/8}\frac{D}{C} = (-1)^{(C-1)/4}\frac{D}{C} \pmod p$. Thus,

$$\begin{aligned} &(2\pm\sqrt{3})^{(p+1)/4} \\ &= 2^{(p+1)/4}\Big(\frac{1\pm\sqrt{3}}{2}\Big)^{(p+1)/2} = 2^{(p-3)/4}\Big(\frac{1\pm\sqrt{3}}{2}\Big)^{(p-1)/2}(1\pm\sqrt{3}) \\ &\equiv (-1)^{(C-1)/4}\frac{D}{C}\Big(\frac{1\pm\sqrt{3}}{2}\Big)^{(p-1)/2}(1\pm\sqrt{3}) \\ &\equiv \begin{cases} (-1)^{(C-1)/4}\frac{D}{C}\big(\frac{D}{3}\big)(1\pm\sqrt{3}) \pmod p & \text{if } 24 \mid p-11, \\ (-1)^{(C-1)/4}\frac{D}{C}\big(\frac{C}{3}\big)\frac{D}{C}(1-\sqrt{3})(1+\sqrt{3}) \equiv (-1)^{(C-1)/4}\big(\frac{C}{3}\big) \pmod p & \\ & \text{if } 24 \mid p-19. \end{cases} \end{aligned}$$

So (ii) is true and the proof is complete.

We note that we have proved Corollary 2.5 using only the quadratic reciprocity.

Corollary 2.6. *Let* $p \equiv 1, 19 \pmod{24}$ *be a prime and hence* $p = C^2 + 2D^2 = x^2 + 3y^2$ *for some* $C, D, x, y \in \mathbb{Z}$.

(i) *If* $p \equiv 1 \pmod{24}$ *and* $C + D \equiv 1 \pmod 4$, *then* $(-1)^{(C^2-1)/8}\big(\frac{C}{3}\big) = (-1)^{y/4}$.

(ii) *If* $p \equiv 19 \pmod{24}$ *and* $C \equiv 1 \pmod 4$, *then* $(-1)^{(C-1)/4}\big(\frac{C}{3}\big) = (-1)^{x/4+1}$.

Proof. If $p \equiv 1 \pmod{24}$, then clearly $4 \mid y$. In [L] E. Lehmer showed that $(2+\sqrt{3})^{(p-1)/4} \equiv (-1)^{y/4} \pmod p$. If $p \equiv 19 \pmod{24}$, then clearly $4 \mid x$ and $p \equiv 7 \pmod{12}$. By [Lem, Ex. 6.30, p. 206] or [S4, Theorem 8.1(2) (with $m = 4$, $n = 2$, $d = 3$)] we have $(2+\sqrt{3})^{(p+1)/4} \equiv (-1)^{x/4+1} \pmod p$. Now comparing the above results with Corollary 2.5 we deduce the corollary.

3. Congruences for $(b + \sqrt{a^2+b^2})^{(p-1)/4} \pmod p$

Lemma 3.1 (Western's formula ([HW, (2.9)], [Lem, pp. 296–298])). *Let* p *and* q *be distinct primes of the form* $8k+1$. *Suppose* $q = a^2 + b^2 = c^2 + 2d^2$

with $a,b,c,d\in\mathbb{Z}$. *Then for* $j\in\{0,1,\dots,7\}$ *we have*

$$p^{(q-1)/8}\equiv\left(\frac{(a-b)d}{ac}\right)^j \pmod q$$
$$\Leftrightarrow\ q^{(p-1)/8}(a-bi)^{(p-1)/4}(c-d\sqrt{-2})^{(p-1)/2}\equiv\left(\frac{-1+i}{\sqrt{-2}}\right)^j \pmod p.$$

THEOREM 3.1. *Let* p *and* q *be distinct primes of the form* $8k+1$. *Suppose* $p=C^2+2D^2=x^2+qy^2$ *and* $q=a^2+b^2=c^2+2d^2$ *with* $a,b,c,d,C,D,x,y\in\mathbb{Z}$ *and* $a\equiv 1 \pmod 4$. *Then*

$$\left(\frac{b-ix/y}{a}\right)^{(p-1)/4}\equiv(-1)^{by/4}\left(\frac{dC-cD}{q}\right)\left(\frac{x+byi}{a}\right)_4 \pmod p$$

and so

$$p\mid U_{(p-1)/8}(2b,-a^2)\ \Leftrightarrow\ \left(\frac{x+byi}{a}\right)_4=(-1)^{(p-1)/8+by/4}\left(\frac{dC-cD}{q}\right).$$

Proof. It is easily seen that

$$-2i(a-bi)(b-i\sqrt{-a^2-b^2})=(\sqrt{-a^2-b^2}-a+bi)^2.$$

Thus

$$(-2i)^{(p-1)/4}(a-bi)^{(p-1)/4}(b-i\sqrt{-a^2-b^2})^{(p-1)/4}=(\sqrt{-a^2-b^2}-a+bi)^{(p-1)/2}.$$

By [S6, Theorem 5.1(ii)] we have

$$\left(\frac{x/y-a+bi}{p}\right)_4=\left(\frac{x-ay+byi}{p}\right)_4=(-1)^{by/4}\left(\frac{x+byi}{a}\right)_4\left(\frac{x}{-a+bi}\right)_4.$$

Since $p\equiv 1 \pmod 8$, applying [S6, Lemma 6.1] we deduce

$$\left(\frac{x}{y}-a+bi\right)^{(p-1)/2}\equiv(2a)^{(p-1)/4}(-a^2-b^2)^{(p-1)/8}\cdot(-1)^{by/4}\left(\frac{x+byi}{a}\right)_4\left(\frac{x}{-a+bi}\right)_4 \pmod p.$$

Note that $(x/y)^2\equiv -a^2-b^2 \pmod p$. From the above we derive

$$\begin{aligned}(-1)^{(p-1)/8}2^{(p-1)/4}&(a-bi)^{(p-1)/4}(b-ix/y)^{(p-1)/4}\\ &\equiv(x/y-a+bi)^{(p-1)/2}\\ &\equiv(2a)^{(p-1)/4}(-a^2-b^2)^{(p-1)/8}(-1)^{by/4}\left(\frac{x+byi}{a}\right)_4\left(\frac{x}{-a+bi}\right)_4 \pmod p.\end{aligned}$$

Therefore,

$$(3.1)\qquad (a^2+b^2)^{(p-1)/8}(a-bi)^{(p-1)/4}\Big(b-i\frac{x}{y}\Big)^{(p-1)/4} \equiv a^{(p-1)/4}(a^2+b^2)^{(p-1)/4}(-1)^{by/4}\Big(\frac{x+byi}{a}\Big)_4\Big(\frac{x}{-a+bi}\Big)_4 \pmod p.$$

Clearly $q\nmid x$. Suppose $x^{(q-1)/4}\equiv\big(\frac{b}{a}\big)^k \pmod q$ for $k\in\mathbb{Z}$. Then

$$p^{(q-1)/8}=(x^2+qy^2)^{(q-1)/8}\equiv x^{(q-1)/4}\equiv\Big(\frac{b}{a}\Big)^k\equiv\Big(\frac{(a-b)d}{ac}\Big)^{2k} \pmod q.$$

Hence, appealing to Lemma 3.1 we have

$$(a^2+b^2)^{(p-1)/8}(a-bi)^{(p-1)/4}(c-d\sqrt{-2})^{(p-1)/2}\equiv\Big(\frac{-1+i}{\sqrt{-2}}\Big)^{2k}=i^k \pmod p.$$

As $c^2D^2-d^2C^2\equiv c^2D^2-d^2(-2D^2)=qD^2 \pmod p$ and $c^2D^2-d^2C^2\equiv -2d^2D^2-d^2C^2=-pd^2 \pmod q$, we see that $(c^2D^2-d^2C^2,pq)=1$. Set $D=2^sD_0$ and $cD-dC=2^rA$ with $2\nmid AD_0$. Then $(A,pq)=1$. Thus,

$$\begin{aligned}&\Big(\frac{c-dC/D}{p}\Big)\\ &=\Big(\frac{D}{p}\Big)\Big(\frac{cD-dC}{p}\Big)=\Big(\frac{D_0}{p}\Big)\Big(\frac{A}{p}\Big)=\Big(\frac{p}{D_0}\Big)\Big(\frac{p}{A}\Big)\\ &=\Big(\frac{C^2+2D^2}{D_0}\Big)\Big(\frac{C^2+2D^2}{A}\Big)=\Big(\frac{C^2}{D_0}\Big)\Big(\frac{q}{A}\Big)\Big(\frac{(c^2+2d^2)(C^2+2D^2)}{A}\Big)\\ &=\Big(\frac{q}{A}\Big)\Big(\frac{(cC+2dD)^2+2(cD-dC)^2}{A}\Big)=\Big(\frac{q}{A}\Big)=\Big(\frac{A}{q}\Big)=\Big(\frac{cD-dC}{q}\Big).\end{aligned}$$

Note that $\big(\frac{C}{D}\big)^2\equiv -2 \pmod p$. From the above we deduce

$$\begin{aligned}(a^2+b^2)^{(p-1)/8}(a-bi)^{(p-1)/4}&\equiv(c-d\sqrt{-2})^{-(p-1)/2}i^k\\ &\equiv\Big(\frac{c-dC/D}{p}\Big)i^k=\Big(\frac{cD-dC}{q}\Big)i^k \pmod p.\end{aligned}$$

Substituting this into (3.1) we see that

$$\begin{aligned}&\Big(\frac{b-ix/y}{a}\Big)^{(p-1)/4}\\ &\equiv\Big(\frac{cD-dC}{q}\Big)i^{-k}q^{(p-1)/4}(-1)^{by/4}\Big(\frac{x+byi}{a}\Big)_4\Big(\frac{x}{-a+bi}\Big)_4 \pmod p.\end{aligned}$$

From [S5, Corollary 4.6(i)] we know that $q^{(p-1)/4}\equiv\big(\frac{x}{q}\big) \pmod p$. As $x^{(q-1)/4}\equiv\big(\frac{b}{a}\big)^k \pmod q$ we have $x^{(q-1)/2}\equiv(-1)^k \pmod q$ and so $\big(\frac{x}{q}\big)=(-1)^k$.

Thus $q^{(p-1)/4} \equiv \left(\frac{x}{q}\right) = (-1)^k \pmod p$. Since $q = a^2 + b^2$ and $a - bi$ is primary in $\mathbb{Z}[i]$, we have $x^{(q-1)/4} \equiv \left(\frac{b}{a}\right)^k \equiv (-i)^k = i^{-k} \pmod{a - bi}$ and so $\left(\frac{x}{-a+bi}\right)_4 = \left(\frac{x}{a-bi}\right)_4 = i^{-k}$. Thus,

$$q^{(p-1)/4}\left(\frac{x}{-a+bi}\right)_4 i^{-k} \equiv (-1)^k \cdot i^{-k} \cdot i^{-k} = 1 \pmod p$$

and therefore

$$\left(\frac{b - ix/y}{a}\right)^{(p-1)/4} \equiv (-1)^{by/4}\left(\frac{cD - dC}{q}\right)\left(\frac{x + byi}{a}\right)_4 \pmod p.$$

Note that $(\frac{ix}{y})^2 \equiv a^2 + b^2 \pmod p$. From Lemma 2.3 and the above we deduce

$$\begin{aligned} p \mid U_{(p-1)/8}(2b, -a^2) \iff & (b + \sqrt{b^2 + a^2})^{(p-1)/4} \equiv (-a^2)^{(p-1)/8} \pmod p \\ \iff & \left(\frac{b + \sqrt{a^2 + b^2}}{a}\right)^{(p-1)/4} \equiv (-1)^{(p-1)/8} \pmod p \\ \iff & (-1)^{by/4}\left(\frac{cD - dC}{q}\right)\left(\frac{x + byi}{a}\right)_4 \equiv (-1)^{(p-1)/8} \pmod p \\ \iff & \left(\frac{x + byi}{a}\right)_4 = (-1)^{(p-1)/8 + by/4}\left(\frac{cD - dC}{q}\right). \end{aligned}$$

This completes the proof.

Corollary 3.1. *Let $p \neq 17$ be a prime of the form $8k + 1$ and so $p = C^2 + 2D^2$ for some $C, D \in \mathbb{Z}$. Then*

$$\begin{aligned} &(4 \pm \sqrt{17})^{(p-1)/4} \equiv 1 \pmod p \\ &\qquad \iff p = x^2 + 17y^2 \ (x, y \in \mathbb{Z}) \text{ and } (-1)^y = \left(\frac{2C - 3D}{17}\right) \end{aligned}$$

and so

$$\begin{aligned} &p \mid U_{(p-1)/8}(8, -1) \\ &\qquad \iff p = x^2 + 17y^2 \ (x, y \in \mathbb{Z}) \text{ and } (-1)^{(p-1)/8 + y} = \left(\frac{2C - 3D}{17}\right). \end{aligned}$$

Proof. If $\left(\frac{17}{p}\right) = -1$, then

$$\begin{aligned} (4 \pm \sqrt{17})^{p-1} &= \frac{(4 \pm \sqrt{17})^p}{4 \pm \sqrt{17}} \equiv \frac{4 \pm (\sqrt{17})^p}{4 \pm \sqrt{17}} \equiv \frac{4 \mp \sqrt{17}}{4 \pm \sqrt{17}} \\ &= -(4 \mp \sqrt{17})^2 \not\equiv 1 \pmod p \end{aligned}$$

and so $(4\pm\sqrt{17})^{(p-1)/2}\not\equiv 1 \pmod p$. If $\left(\frac{17}{p}\right)=1$, by [Br] or [S5, p. 1324] we have

$$(4\pm\sqrt{17})^{(p-1)/2}\equiv 1 \pmod p \iff p=x^2+17y^2 \ (x,y\in\mathbb{Z}).$$

Assume $p=x^2+17y^2$ for some $x,y\in\mathbb{Z}$. Taking $q=17$, $a=1$, $b=4$, $c=3$ and $d=2$ in Theorem 3.1 we deduce

$$(4\pm\sqrt{17})^{(p-1)/4}\equiv(-1)^y\left(\frac{2C-3D}{17}\right) \pmod p.$$

By Lemma 2.3 we have

$$p\,|\,U_{(p-1)/8}(8,-1) \iff (4+\sqrt{17})^{(p-1)/4}\equiv(-1)^{(p-1)/8} \pmod p.$$

Thus the result follows.

Corollary 3.2. *Let $p\equiv 1 \pmod 8$ be a prime such that $p=C^2+2D^2=x^2+257y^2\neq 257$ for $C,D,x,y\in\mathbb{Z}$. Then*

$$(16\pm\sqrt{257})^{(p-1)/4}\equiv\left(\frac{4C-15D}{257}\right) \pmod p$$

and so

$$p\,|\,U_{(p-1)/8}(32,-1) \iff \left(\frac{4C-15D}{257}\right)=(-1)^{(p-1)/8}.$$

Proof. Taking $q=257$, $a=1$, $b=16$, $c=15$ and $d=4$ in Theorem 3.1 we obtain the result.

Corollary 3.3. *Let $p\neq 73$ be a prime of the form $8k+1$ such that $p=C^2+2D^2=x^2+73y^2$ for $C,D,x,y\in\mathbb{Z}$. Then*

$$p\,|\,U_{(p-1)/8}(16,-9) \iff 3\,|\,xy \text{ and } (-1)^{(p-1)/8}\left(\frac{6C-D}{73}\right)=\begin{cases}1 & \text{if } 3\,|\,y,\\ -1 & \text{if } 3\,|\,x.\end{cases}$$

Proof. Taking $q=73$, $a=-3$, $b=8$, $c=1$ and $d=6$ in Theorem 3.1 we see that

$$p\,|\,U_{(p-1)/8}(16,-9) \iff \left(\frac{x+8yi}{3}\right)_4=\left(\frac{x+8yi}{-3}\right)_4=(-1)^{(p-1)/8}\left(\frac{6C-D}{73}\right).$$

Since

$$\left(\frac{x+8yi}{3}\right)_4=\begin{cases}\left(\frac{x}{3}\right)_4=1 & \text{if } 3\,|\,y,\\ \left(\frac{8yi}{3}\right)_4=\left(\frac{i}{3}\right)_4=-1 & \text{if } 3\,|\,x,\\ \left(\frac{1+8i}{3}\right)_4=\left(\frac{i(1+i)}{3}\right)_4=i & \text{if } 3\,|\,x-y,\\ \left(\frac{1-8i}{3}\right)_4=\left(\frac{1+i}{3}\right)_4=-i & \text{if } 3\,|\,x+y,\end{cases}$$

from the above we deduce the result.

Corollary 3.4. *Let $p \neq 41$ be a prime of the form $8k+1$ such that $p = C^2 + 2D^2 = x^2 + 41y^2$ for $C, D, x, y \in \mathbb{Z}$. Then*

$$p \mid U_{(p-1)/8}(8, -25) \iff 5 \mid xy \text{ and } (-1)^{(p-1)/8+y}\Big(\frac{4C-3D}{41}\Big) = \begin{cases} 1 & \text{if } 5 \mid y, \\ -1 & \text{if } 5 \mid x. \end{cases}$$

Proof. Taking $q = 41$, $a = 5$, $b = 4$, $c = 3$ and $d = 4$ in Theorem 3.1 we see that

$$p \mid U_{(p-1)/8}(8, -25) \iff \Big(\frac{x+4yi}{5}\Big)_4 = (-1)^{(p-1)/8+y}\Big(\frac{4C-3D}{41}\Big).$$

Since $x \not\equiv \pm 2y \pmod 5$ and

$$\Big(\frac{x+4yi}{5}\Big)_4 = \begin{cases} \big(\frac{x}{5}\big)_4 = 1 & \text{if } 5 \mid y, \\ \big(\frac{4yi}{5}\big)_4 = \big(\frac{i}{5}\big)_4 = -1 & \text{if } 5 \mid x, \\ \big(\frac{1+4i}{5}\big)_4 = \big(\frac{i(1+i)}{5}\big)_4 = -i & \text{if } 5 \mid x-y, \\ \big(\frac{1-4i}{5}\big)_4 = \big(\frac{1+i}{5}\big)_4 = i & \text{if } 5 \mid x+y, \end{cases}$$

from the above we deduce the result.

Corollary 3.5. *Let $p \neq 89$ be a prime of the form $8k+1$ such that $p = C^2 + 2D^2 = x^2 + 89y^2$ for $C, D, x, y \in \mathbb{Z}$. Then*

$$p \mid U_{(p-1)/8}(16, -25)$$
$$\iff 5 \mid xy \text{ and } (-1)^{(p-1)/8}\Big(\frac{2C-9D}{89}\Big) = \begin{cases} 1 & \text{if } 5 \mid y, \\ -1 & \text{if } 5 \mid x. \end{cases}$$

Proof. Taking $q = 89$, $a = 5$, $b = 8$, $c = 9$ and $d = 2$ in Theorem 3.1 we see that

$$p \mid U_{(p-1)/8}(16, -25) \iff \Big(\frac{x+8yi}{5}\Big)_4 = (-1)^{(p-1)/8}\Big(\frac{2C-9D}{89}\Big).$$

Since $x \not\equiv \pm y \pmod 5$ and

$$\Big(\frac{x+8yi}{5}\Big)_4 = \begin{cases} \big(\frac{x}{5}\big)_4 = 1 & \text{if } 5 \mid y, \\ \big(\frac{8yi}{5}\big)_4 = \big(\frac{i}{5}\big)_4 = -1 & \text{if } 5 \mid x, \\ \big(\frac{1+4i}{5}\big)_4 = \big(\frac{i(1+i)}{5}\big)_4 = -i & \text{if } 5 \mid x-2y, \\ \big(\frac{1-4i}{5}\big)_4 = \big(\frac{1+i}{5}\big)_4 = i & \text{if } 5 \mid x+2y, \end{cases}$$

the result follows.

Lemma 3.2 ([E], [S1, Proposition 1], [S2, Lemma 2.1]). *Let $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ with $2 \nmid m$ and $(m, a^2+b^2) = 1$. Then*

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

Theorem 3.2. *Let $A, B \in \mathbb{Z}$ be such that $2 \nmid A$ and $A^4 + 16B^2$ is a prime, and let $p \equiv 1 \pmod 8$ be a prime such that $p = x^2 + (A^4+16B^2)y^2 \neq$*

A^4+16B^2 for $x,y\in\mathbb{Z}$. Assume $A^4+16B^2=c^2+2d^2$ and $p=C^2+2D^2$ with $c,d,C,D\in\mathbb{Z}$. Then

$$(4B\pm\sqrt{A^4+16B^2})^{(p-1)/4}\equiv(-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)\pmod p$$

and

$$p\,|\,U_{(p-1)/8}(8B,-A^4)\ \Leftrightarrow\ (-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)=(-1)^{(p-1)/8}\Big(\frac{A}{p}\Big).$$

Proof. Putting $q=A^4+16B^2$, $a=A^2$ and $b=4B$ in Theorem 3.1 we see that

$$\Big(\frac{4B-ix/y}{A^2}\Big)^{(p-1)/4}\equiv(-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)\Big(\frac{x+4Byi}{A^2}\Big)_4\pmod p.$$

From Lemma 3.2 we have

$$\Big(\frac{x+4Byi}{A^2}\Big)_4=\Big(\frac{x^2+16B^2y^2}{A}\Big)=\Big(\frac{p-A^4y^2}{A}\Big)=\Big(\frac{p}{A}\Big)=\Big(\frac{A}{p}\Big).$$

Thus,

$$\Big(4B-i\frac{x}{y}\Big)^{(p-1)/4}\equiv(-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)\pmod p$$

and so

$$\Big(4B+i\frac{x}{y}\Big)^{(p-1)/4}\equiv(-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)\pmod p.$$

Since $(ix/y)^2\equiv A^4+16B^2\pmod p$, we deduce

$$(4B\pm\sqrt{A^4+16B^2})^{(p-1)/4}\equiv(-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)\pmod p.$$

Applying Lemma 2.3 we see that

$$\begin{aligned}&p\,|\,U_{(p-1)/8}(8B,-A^4)\\&\quad\Leftrightarrow\ (-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)\equiv(-A^4)^{(p-1)/8}\equiv(-1)^{(p-1)/8}\Big(\frac{A}{p}\Big)\pmod p\\&\quad\Leftrightarrow\ (-1)^{By}\Big(\frac{dC-cD}{A^4+16B^2}\Big)=(-1)^{(p-1)/8}\Big(\frac{A}{p}\Big).\end{aligned}$$

This proves the theorem.

Corollary 3.6. *Let $p\equiv1\pmod 8$ be a prime such that $p=C^2+2D^2=x^2+97y^2\ne97$ for $C,D,x,y\in\mathbb{Z}$. Then*

$$(4\pm\sqrt{97})^{(p-1)/4}\equiv(-1)^{y}\Big(\frac{6C-5D}{97}\Big)\pmod p$$

and so

$$p \mid U_{(p-1)/8}(8,-81) \ \Leftrightarrow\ \left(\frac{6C-5D}{97}\right) = (-1)^{(p-1)/8+y}\left(\frac{p}{3}\right).$$

Proof. Taking $A=3$ and $B=1$ in Theorem 3.2 we obtain the result.

Corollary 3.7. *Let* $p\equiv 1 \pmod 8$ *be a prime such that* $p=C^2+2D^2=x^2+337y^2\neq 337$ *for* $C,D,x,y\in\mathbb{Z}$. *Then*

$$(16\pm\sqrt{337})^{(p-1)/4} \equiv \left(\frac{12C-7D}{337}\right) \pmod p$$

and so

$$p \mid U_{(p-1)/8}(32,-81) \ \Leftrightarrow\ \left(\frac{12C-7D}{337}\right) = (-1)^{(p-1)/8}\left(\frac{p}{3}\right).$$

Proof. Taking $A=3$ and $B=4$ in Theorem 3.2 we obtain the result.

Corollary 3.8. *Let* $p\equiv 1 \pmod 8$ *be a prime such that* $p=C^2+2D^2=x^2+641y^2\neq 641$ *for* $C,D,x,y\in\mathbb{Z}$. *Then*

$$(4\pm\sqrt{641})^{(p-1)/4} \equiv (-1)^y\left(\frac{10C-21D}{641}\right) \pmod p$$

and so

$$p \mid U_{(p-1)/8}(8,-625) \ \Leftrightarrow\ \left(\frac{10C-21D}{641}\right) = (-1)^{(p-1)/8+y}\left(\frac{p}{5}\right).$$

Proof. Taking $A=5$ and $B=1$ in Theorem 3.2 we obtain the result.

4. Five conjectures

Conjecture 4.1. *Let* $p\equiv 3 \pmod 8$ *be a prime and* $k\in\mathbb{Z}$ *with* $2\nmid k$. *Suppose* $p=x^2+(k^2+1)y^2$ *for some* $x,y\in\mathbb{Z}$. *Then*

$$V_{(p+1)/4}(2k,-1)\equiv\begin{cases}-(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}2^{(p+1)/4} \pmod p & \text{if } k\equiv 5,7 \pmod 8,\\ (-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}2^{(p+1)/4} \pmod p & \text{if } k\equiv 1,3 \pmod 8.\end{cases}$$

In the case $k=1$, Conjecture 4.1 was proved by the author in [S6] and by C. N. Beli in [B].

Conjecture 4.2. *Let* $p\equiv 3 \pmod 4$ *be a prime and* $k\in\mathbb{Z}$ *with* $2\nmid k$. *Suppose* $2p=x^2+(k^2+4)y^2$ *for some* $x,y\in\mathbb{Z}$.

(i) *If* $k\equiv 1,3 \pmod 8$, *then*

$$V_{(p+1)/4}(k,-1) \equiv\begin{cases}(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}(-2)^{(p+1)/4} \pmod p & \text{if } k\equiv 1,11 \pmod{16},\\ -(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}(-2)^{(p+1)/4} \pmod p & \text{if } k\equiv 3,9 \pmod{16}.\end{cases}$$

(ii) *If* $k\equiv 5,7\pmod 8$, *then*

$$V_{(p+1)/4}(k,-1)\equiv\begin{cases}(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}2^{(p+1)/4}\pmod p & \text{if } k\equiv 5,15\pmod{16},\\ -(-1)^{\frac{(\frac{p-1}{2}y)^2-1}{8}}2^{(p+1)/4}\pmod p & \text{if } k\equiv 7,13\pmod{16}.\end{cases}$$

In the case $k=1$, Conjecture 4.2 was stated by the author in [S3, S6] and proved by C. N. Beli in [B].

Conjectures 4.1 and 4.2 have been checked for all $1\le k<100$ and $p<20\,000$.

Inspired by [S6, Conjectures 9.1–9.9], we pose the following conjectures.

Conjecture 4.3. *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* $c\equiv 1\pmod 4$, $x=2^\alpha x_0$, $y=2^\beta y_0$ *and* $x_0\equiv y_0\equiv 1\pmod 4$.

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

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

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

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

Conjecture 4.4. *Let* $p\equiv 1\pmod 4$ *and* $q\equiv 7\pmod{16}$ *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* $c\equiv 1\pmod 4$, $x=2^\alpha x_0$, $y=2^\beta y_0$ *and* $x_0\equiv y_0\equiv 1\pmod 4$.

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

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

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

$$q^{(p-5)/8}\equiv\begin{cases}\frac{y}{x}\pmod p & \text{if } q\mid d,\\ -\frac{y}{x}\pmod p & \text{if } q\mid c.\end{cases}$$

Conjecture 4.5. *Let* $p\equiv 1\pmod 4$ *and* $q\equiv 15\pmod{16}$ *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* $x=2^\alpha x_0$, $y=2^\beta y_0$ *and* $x_0\equiv y_0\equiv 1\pmod 4$.

(i) *If* $p\equiv 1\pmod 8$, *then* $q^{(p-1)/8}\equiv(-1)^{y/4}\pmod p$.
(ii) *If* $p\equiv 5\pmod 8$, *then* $q^{(p-5)/8}\equiv\frac{y}{x}\pmod p$.

Conjectures 4.3–4.5 have been checked for all primes $p<200\,000$ and $q<200$.

Added in proof. We have the following generalization of Conjectures 4.4 and 4.5.

CONJECTURE 4.6. *Let q be a prime of the form $8k+7$. Then there exist disjoint subsets S_0, S_1, S_2 of $\{\infty\} \cup \{k \in \mathbb{Z}/q\mathbb{Z} : (\frac{k^2+1}{q}) = 1\}$ such that for any primes $p = c^2 + d^2 = x^2 + qy^2$ with $c, d, x, y \in \mathbb{Z}$, $x = 2^\alpha x_0$, $2^\beta y_0$ and $c \equiv x_0 \equiv y_0 \equiv 1 \pmod 4$,*

$$q^{(p-1)/8} \equiv \begin{cases} (-1)^{y/4} \pmod p & \text{if } c/d \in S_0, \\ -(-1)^{y/4} \pmod p & \text{if } c/d \in S_1, \\ \pm(-1)^{y/4}\,\frac{d}{c} \pmod p & \text{if } \pm c/d \in S_2, \end{cases} \qquad \text{for } p \equiv 1 \pmod 8,$$

and

$$q^{(p-5)/8} \equiv \begin{cases} \frac{y}{x} \pmod p & \text{if } c/d \in S_0, \\ -\frac{y}{x} \pmod p & \text{if } c/d \in S_1, \\ \pm\frac{dy}{cx} \pmod p & \text{if } \pm c/d \in S_2, \end{cases} \qquad \text{for } p \equiv 5 \pmod 8.$$

Here we identify c/d with ∞ when $q \mid d$, and identify a with $a+q\mathbb{Z}$. Moreover, $|S_0| = |S_1| = |S_2| = (q+1)/8$, $a/b \in S_0 \cup S_1$ implies $(\frac{a+bi}{q})_4 = 1$, and $a/b \in S_2$ implies $(\frac{a+bi}{q})_4 = -1$.

For $q = 23$ we have $S_0 = \{\infty, \pm 10\}$, $S_1 = \{0, \pm 7\}$ and $S_2 = \{1, 5, -9\}$. For $q = 31$ we have $S_0 = \{0, \infty, \pm 1\}$, $S_1 = \{\pm 7, \pm 9\}$ and $S_2 = \{-2, 3, 10, -15\}$. For $q = 47$ we have $S_0 = \{0, \infty, \pm 4, \pm 12\}$, $S_1 = \{\pm 1, \pm 10, \pm 14\}$ and $S_2 = \{-6, -7, 8, -11, -17, -20\}$.

Acknowledgments. The author is supported by the Natural Sciences Foundation of China (grant no. 10971078).

References

[B] C. N. Beli, *Two conjectures by Zhi-Hong Sun*, Acta Arith. 137 (2009), 99–131.

[Br] J. A. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory 5 (1973), 271–286.

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

[HW] R. H. Hudson and K. S. Williams, *An application of a formula of Western to the evaluation of certain Jacobsthal sums*, Acta Arith. 41 (1982), 261–276.

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

[L] 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.

[S1] Z. H. Sun, *Notes on quartic residue symbol and rational reciprocity laws*, J. Nanjing Univ. Math. Biquart. 9 (1992), 92–101.

[S2] —, *Supplements to the theory of quartic residues*, Acta Arith. 97 (2001), 361–377.

[S3] Z. H. Sun, *Values of Lucas sequences modulo primes*, Rocky Mountain J. Math. 33 (2003), 1123–1145.
[S4] —, *Quartic residues and binary quadratic forms*, J. Number Theory 113 (2005), 10–52.
[S5] —, *On the quadratic character of quadratic units*, ibid. 128 (2008), 1295–1335.
[S6] —, *Quartic, octic residues and Lucas sequences*, ibid. 129 (2009), 499–550.

Zhi-Hong Sun
School of the 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 7.9.2010 (6484)