ACTA ARITHMETICA
XCVII.4 (2001)

Supplements to the theory of quartic residues

by

Zhi-Hong Sun (Huaiyin)

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 $\pi=a+bi\in\mathbb{Z}[i]$ the *norm* of π is given by $N\pi=\pi\overline{\pi}=a^2+b^2$. Here $\overline{\pi}$ means the complex conjugate of π. When $b\equiv 0 \pmod 2$ and $a+b\equiv 1 \pmod 4$ we say that π is *primary*.

If π or $-\pi$ is primary in $\mathbb{Z}[i]$, then we may write $\pi=\pm\pi_1\dots\pi_r$, where $\pi_1,\dots,\pi_r$ are primary primes. For $\alpha\in\mathbb{Z}[i]$ the *quartic Jacobi symbol* $\left(\frac{\alpha}{\pi}\right)_4$ is defined by

$$\left(\frac{\alpha}{\pi}\right)_4=\left(\frac{\alpha}{\pi_1}\right)_4\dots\left(\frac{\alpha}{\pi_r}\right)_4,$$

where $\left(\frac{\alpha}{\pi_s}\right)_4$ is the *quartic residue character* of α modulo π_s which is given by

$$\left(\frac{\alpha}{\pi_s}\right)_4=\begin{cases}0 & \text{if } \pi_s\mid\alpha,\\ i^r & \text{if } \alpha^{(N\pi_s-1)/4}\equiv i^r \pmod{\pi_s}.\end{cases}$$

According to [IR, pp. 122–123, 311] and [BEW, pp. 242–243, 247] the quartic Jacobi symbol has the following properties:

(1.1) If $a+bi$ is primary in $\mathbb{Z}[i]$, then

$$\left(\frac{i}{a+bi}\right)_4=i^{(a^2+b^2-1)/4} \quad\text{and}\quad \left(\frac{1+i}{a+bi}\right)_4=i^{(a-b-b^2-1)/4}.$$

(1.2) If α and π are relatively prime primary elements of $\mathbb{Z}[i]$, then

$$\overline{\left(\frac{\alpha}{\pi}\right)_4}=\left(\frac{\alpha}{\pi}\right)_4^{-1}=\left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4.$$

(1.3) If $a+bi$ and $c+di$ are relatively prime primary elements of $\mathbb{Z}[i]$, then

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

2000 *Mathematics Subject Classification*: Primary 11A15; Secondary 11E25.

The assertion (1.3) is now called the *general law of biquadratic reciprocity*, which was proposed by Gauss and later proved by Jacobi and Eisenstein.

Let $\left(\frac{a}{p}\right)$ be the Legendre symbol. In the nineteenth century Dirichlet (see [V]) showed

THEOREM 1.1. *Let p and q be distinct primes, $p \equiv 1 \pmod 4$, $p = a^2+b^2$, $2 \mid b$ and $q^* = (-1)^{(q-1)/2}q$. Then q^* is a quartic residue of p if and only if there is an integer m such that $m^2 \equiv p \pmod q$ and $\left(\frac{m(m+b)}{q}\right) = 1$.*

In 1969, K. Burde [B] discovered the following rational quartic reciprocity law.

THEOREM 1.2. *Let p and q be distinct primes of the form $4n+1$, $p = a^2+b^2$ $(2\nmid a)$, $q = c^2+d^2$ $(2\nmid c)$ and $\left(\frac{q}{p}\right) = 1$. If $\left(\frac{ad-bc}{q}\right) = (-1)^{(q-1)/4}$ then q is a quartic residue (mod p) if and only if p is a quartic residue (mod q). If $\left(\frac{ad-bc}{q}\right) = -(-1)^{(q-1)/4}$ then q is a quartic residue (mod p) if and only if p is a quartic nonresidue (mod q).*

In 1979 H. von Lienen [Li] extended Burde's reciprocity law to quartic nonresidues. For further papers along this line one may consult [L1], [L2], [Le1], [Le2], [W], [Y] and [S1].

Let $p > 0$ be an odd number, and let S_p denote the set of those rational numbers whose denominator is prime to p. Inspired by [S2] we introduce the sets $Q_r(p)$ $(r = 0, 1, 2, 3)$ as follows:

$$Q_r(p) = \left\{ k \;\middle|\; \left(\frac{k+i}{p}\right)_4 = i^r,\ k \in S_p \right\} \quad (r = 0, 1, 2, 3).$$

In Section 2 we mainly study the properties of $Q_r(p)$ $(r = 0, 1, 2, 3)$ and the connections between $Q_r(p)$ $(r = 0, 1, 2, 3)$ and quartic reciprocity laws. We also establish a rational quartic reciprocity law which is similar to Theorem 1.2, and give a simple criterion for quartic residuacity.

In Section 3 we concentrate our attention on the structure of $Q_r(p)$ $(r = 0, 1, 2, 3)$. For any odd prime p and $k \in S_p$ set

$$[k]_p = \{x \mid x \equiv k \pmod p,\ x \in S_p\}, \quad [\infty]_p = \{n/m \mid m, n \in \mathbb{Z},\ p \mid m,\ p \nmid n\},$$
$$Q_0'(p) = \{[k]_p \mid k \in Q_0(p)\} \cup \{[\infty]_p\}, \quad Q_r'(p) = \{[k] \mid k \in Q_r(p)\} \quad (r = 1, 2, 3).$$

It is proved that $\bigcup_{r=0}^3 Q_r'(p)$ forms a cyclic group of order $p - \left(\frac{-1}{p}\right)$ and $Q_0'(p)$ is a subgroup of order $\left(p - \left(\frac{-1}{p}\right)\right)/4$.

The main result of Section 4 is the isomorphism between the group $Q'(p)$ and those primitive binary quadratic forms of discriminant $-16p^2$, where $Q'(p) = \bigcup_{r=0}^3 Q_r'(p)$. As an application we obtain a general criterion for quartic residuacity in terms of binary quadratic forms.

For later convenience we list the following notations:

$\mathbb{Z}$—the set of integers, $\mathbb{N}$—the set of natural numbers, $\mathbb{Z}[i]$—the set $\{a+bi \mid a,b \in \mathbb{Z}\}$, $N\pi$—the norm of π, S_p—the set of those rational numbers whose denominator is prime to p, $[x]$—the greatest integer not exceeding x, $[k]_p$—the set $\{x \mid x \equiv k \pmod p,\ x \in S_p\}$, $\gcd(a_1,\dots,a_k)$—the greatest common divisor of $a_1,\dots,a_k$, $m \mid n$—m divides n, $m \nmid n$—m does not divide n, $\left(\frac{a}{p}\right)$—the Legendre symbol, $\left(\frac{\alpha}{\pi}\right)_4$—the quartic Jacobi symbol.

2. The properties of $Q_r(p)$. Let $p \geq 1$ be an odd number. For $a,b \in S_p$ it is clear that there are unique integers $a_0,b_0 \in \{0,1,\dots,p-1\}$ satisfying $a \equiv a_0 \pmod p$ and $b \equiv b_0 \pmod p$. From this we may define

$$\gcd(a,p) = \gcd(a_0,p) \quad \text{and} \quad \left(\frac{a+bi}{p}\right)_4 = \left(\frac{a_0+b_0i}{p}\right)_4 \quad \text{for } p>1.$$

When $p=1$ define $\gcd(a,p)=1$ and $\left(\frac{a+bi}{p}\right)_4 = 1$.

One can easily verify the following facts:

(2.1) If $a,b,c,d \in S_p$, then

$$\left(\frac{a+bi}{p}\right)_4\left(\frac{c+di}{p}\right)_4 = \left(\frac{(a+bi)(c+di)}{p}\right)_4.$$

(2.2) If $n \in S_p$ and $\gcd(p,n)=1$, then $\left(\frac{n}{p}\right)_4 = 1$.

(2.3) If p_1,p_2 are positive odd numbers and $a,b \in S_{p_1p_2}$, then

$$\left(\frac{a+bi}{p_1p_2}\right)_4 = \left(\frac{a+bi}{p_1}\right)_4\left(\frac{a+bi}{p_2}\right)_4.$$

Definition 2.1. Suppose $p \in \mathbb{N}$ and $p \equiv 1 \pmod 2$. For $r = 0,1,2,3$ define

$$Q_r(p) = \left\{k \;\middle|\; \left(\frac{k+i}{p}\right)_4 = i^r,\ k \in S_p\right\}.$$

From the above definition it is easy to prove the following results:

(2.4) $\bigcup_{r=0}^{3} Q_r(p) = \{k \mid \gcd(k^2+1,p)=1,\ k \in S_p\}$.

(2.5) If $r \in \{0,1\}$ then $k \in Q_{2r}(p)$ if and only if $-k \in Q_{2r}(p)$.

(2.6) $k \in Q_1(p)$ if and only if $-k \in Q_3(p)$.

Example 2.1. Let p be an odd prime. For $r = 0,1,2$ set

$$Q_r^*(p) = \{k \mid k \in Q_r(p) \cap \{0, \pm1, \dots, \pm(p-1)/2\}\}.$$

Then

$$\begin{aligned}
&Q_0^*(3)=\emptyset, && Q_1^*(3)=\{-1\}, && Q_2^*(3)=\{0\};\\
&Q_0^*(5)=\emptyset, && Q_1^*(5)=\{1\}, && Q_2^*(5)=\{0\};\\
&Q_0^*(7)=\{0\}, && Q_1^*(7)=\{2,3\}, && Q_2^*(7)=\{-1,1\};\\
&Q_0^*(11)=\{\pm2\}, && Q_1^*(11)=\{1,3,4\}, && Q_2^*(11)=\{0,\pm5\};\\
&Q_0^*(13)=\{\pm3\}, && Q_1^*(13)=\{-1,-2,6\}, && Q_2^*(13)=\{0,\pm4\};\\
&Q_0^*(17)=\{0,\pm1\}, && Q_1^*(17)=\{-2,3,-6,-8\}, && Q_2^*(17)=\{\pm5,\pm7\};\\
&Q_0^*(19)=\{\pm4,\pm9\}, && Q_1^*(19)=\{-1,3,-6,7,-8\}, && Q_2^*(19)=\{0,\pm2,\pm5\}.
\end{aligned}$$

THEOREM 2.1 (The reciprocity law of $Q_r(p)$). *Let p_1 and p_2 be positive odd numbers, $m,n\in\mathbb{Z}$, $\gcd(p_1p_2,n)=1$ and $r\in\{0,1,2,3\}$. If $p_1\equiv\pm p_2 \pmod{8(m^2+n^2)}$, then $m/n\in Q_r(p_1)$ if and only if $m/n\in Q_r(p_2)$.*

Proof. Write $m+ni=i^j(1+i)^k\pi$, $p_1=\left(\frac{-1}{p_1}\right)p_1^*$ and $p_2=\left(\frac{-1}{p_2}\right)p_2^*$, where π is primary in $\mathbb{Z}[i]$. Since $p_1\equiv\pm p_2 \pmod{8(m^2+n^2)}$ we see that

$$\left(\frac{2}{p_1}\right)=\left(\frac{2}{p_2}\right)\quad\text{and}\quad p_1^*\equiv p_2^* \pmod{m^2+n^2}.$$

If $m\not\equiv n \pmod 2$ then $k=0$. By (1.1) and (1.3),

$$\begin{aligned}
\left(\frac{m+ni}{p_1}\right)_4&=\left(\frac{i}{p_1}\right)_4^j\left(\frac{\pi}{p_1}\right)_4=(-1)^{(p_1^2-1)j/8}\left(\frac{\pi}{p_1^*}\right)_4\\
&=\left(\frac{2}{p_1}\right)^j\left(\frac{p_1^*}{\pi}\right)_4=\left(\frac{2}{p_2}\right)^j\left(\frac{p_2^*}{\pi}\right)_4=\left(\frac{m+ni}{p_2}\right)_4.
\end{aligned}$$

If $m\equiv n \pmod 2$ then $p_1^*\equiv p_2^* \pmod{16}$ and $p_1^*\equiv p_2^* \pmod{m^2+n^2}$; using (1.1) and (1.3) we see that

$$\begin{aligned}
\left(\frac{m+ni}{p_1}\right)_4&=\left(\frac{i}{p_1}\right)_4^j\left(\frac{1+i}{p_1}\right)_4^k\left(\frac{\pi}{p_1}\right)_4=(-1)^{(p_1^2-1)j/8}i^{(p_1^*-1)k/4}\left(\frac{p_1^*}{\pi}\right)_4\\
&=(-1)^{(p_2^2-1)j/8}i^{(p_2^*-1)k/4}\left(\frac{p_2^*}{\pi}\right)_4=\left(\frac{m+ni}{p_2}\right)_4.
\end{aligned}$$

So the result follows from Definition 2.1 and (2.2).

Now we point out the connections between $Q_r(p)$ ($r\in\{0,1,2,3\}$) and quartic residues.

THEOREM 2.2. *Let p be a prime of the form $4m+1$, $p=a^2+b^2$ $(a,b\in\mathbb{Z})$, $2\mid b$, $a+b\equiv1 \pmod 4$, $q\in\mathbb{N}$, $2\nmid q$, $p\nmid q$, $\gcd\left(b,\frac{q}{\gcd(b,q)}\right)=1$, $q^*=(-1)^{(q-1)/2}q$ and $r\in\{0,1,2,3\}$. Then*

$$(q^*)^{(p-1)/4}\equiv(b/a)^r \pmod p\quad\textit{if and only if}\quad a/b\in Q_r\left(\frac{q}{\gcd(b,q)}\right).$$

Proof. Set $\pi = a + bi$. Then $p = \pi\overline{\pi}$. Since π is primary it is clear that

$$(q^*)^{(p-1)/4} \equiv (b/a)^r \pmod p \;\Leftrightarrow\; (q^*)^{(p-1)/4} \equiv (b/a)^r \equiv i^r \pmod \pi$$
$$\Leftrightarrow \left(\frac{q^*}{\pi}\right)_4 = i^r \;\Leftrightarrow\; \left(\frac{\pi}{q}\right)_4 = \left(\frac{\pi}{q^*}\right)_4 = i^r.$$

But

$$\left(\frac{\pi}{q}\right)_4 = \left(\frac{a+bi}{q/\gcd(b,q)}\right)_4 \left(\frac{a+bi}{\gcd(b,q)}\right)_4 = \left(\frac{a/b+i}{q/\gcd(b,q)}\right)_4.$$

So the result follows immediately.

THEOREM 2.3. *Let p be an odd prime, $r \in \{0,1,2,3\}$ and $k \in S_p$ for which $k^2 + 1 \not\equiv 0 \pmod p$.*

(i) *If $p \equiv 1 \pmod 4$ and $t^2 \equiv -1 \pmod p$ then $k \in Q_r(p)$ if and only if*

$$\left(\frac{k+t}{k-t}\right)^{(p-1)/4} \equiv t^r \pmod p.$$

(ii) *If $p \equiv 3 \pmod 4$ then $k \in Q_r(p)$ if and only if*

$$\left(\frac{k-i}{k+i}\right)^{(p+1)/4} \equiv i^r \pmod p.$$

Proof. Suppose $p \equiv 1 \pmod 4$, $p = a^2 + b^2$, $2 \mid b$ and $\pi = a + bi$. Then $b/a \equiv i \pmod \pi$. If $a \equiv 1 - b \pmod 4$ then π is primary. So we have

$$\left(\frac{k+i}{p}\right)_4 = \left(\frac{k+i}{\pi}\right)_4 \left(\frac{k+i}{\overline{\pi}}\right)_4 = \left(\frac{k+i}{\pi}\right)_4 \overline{\left(\frac{k-i}{\pi}\right)_4}$$
$$= \left(\frac{k+i}{\pi}\right)_4 \left(\frac{k-i}{\pi}\right)_4^{-1} \equiv \left(\frac{k+i}{k-i}\right)^{(p-1)/4}$$
$$\equiv \left(\frac{k+b/a}{k-b/a}\right)^{(p-1)/4} \pmod \pi.$$

From this it follows that

$$k \in Q_r(p) \;\Leftrightarrow\; \left(\frac{k+i}{p}\right)_4 = i^r$$
$$\Leftrightarrow\; \left(\frac{k+b/a}{k-b/a}\right)^{(p-1)/4} \equiv i^r \equiv \left(\frac{b}{a}\right)^r \pmod \pi$$
$$\Leftrightarrow\; \left(\frac{k+b/a}{k-b/a}\right)^{(p-1)/4} \equiv \left(\frac{b}{a}\right)^r \pmod p$$
$$\Leftrightarrow\; \left(\frac{k-b/a}{k+b/a}\right)^{(p-1)/4} \equiv \left(\frac{a}{b}\right)^r \equiv \left(-\frac{b}{a}\right)^r \pmod p.$$

This together with the fact that $t \equiv \pm b/a \pmod p$ proves (i).

Now consider the case $p \equiv 3 \pmod 4$. Note that $(k+i)^p \equiv k^p + i^p \equiv k - i \pmod p$. So we have

$$\left(\frac{k+i}{p}\right)_4 \equiv (k+i)^{(p^2-1)/4} = \frac{(k+i)^{p(p+1)/4}}{(k+i)^{(p+1)/4}} \equiv \left(\frac{k-i}{k+i}\right)^{(p+1)/4} \pmod p,$$

which implies that

$$k \in Q_r(p) \ \Leftrightarrow \ \left(\frac{k-i}{k+i}\right)^{(p+1)/4} \equiv i^r \pmod p.$$

This completes the proof.

COROLLARY 2.1. *Let $p \equiv 1 \pmod 4$ be a prime, $t^2 \equiv -1 \pmod p$, $r \in \{0,1,2,3\}$ and $m \in S_p$ with $m \not\equiv 0, 1 \pmod p$. Then $m^{(p-1)/4} \equiv t^r \pmod p$ if and only if $\frac{m+1}{m-1} t \in Q_r(p)$.*

COROLLARY 2.2. *Let p and q be distinct primes, $r \in \{0,1,2,3\}$, $p \equiv 1 \pmod 4$ and $p = a^2 + b^2$ with $2 \mid b$.*

(i) *If $q \equiv 1 \pmod 4$ and $q = c^2 + d^2$ with $2 \mid d$ then $q^{(p-1)/4} \equiv \left(\frac{b}{a}\right)^r \pmod p$ if and only if*

$$p^{(q-1)/4} \equiv \left(\frac{ac - bd}{q}\right)\left(\frac{d}{c}\right)^r \pmod q.$$

(ii) *If $q \equiv 3 \pmod 4$ then $(-q)^{(p-1)/4} \equiv \left(\frac{b}{a}\right)^r \pmod p$ if and only if*

$$\left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv i^r \pmod q.$$

Proof. Let $q^* = (-1)^{(q-1)/2} q$. If $q \mid b$, it follows from Theorem 2.2 that $(q^*)^{(p-1)/4} \equiv 1 \pmod p$. From this it is easily seen that the result is true in this case.

Now assume $q \nmid b$. From Theorems 2.2 and 2.3 we know that

$$(q^*)^{(p-1)/4} \equiv (b/a)^r \pmod p \ \Leftrightarrow \ a/b \in Q_r(q)$$

$$\Leftrightarrow \begin{cases} \left(\dfrac{ac+bd}{ac-bd}\right)^{(q-1)/4} \equiv \left(\dfrac{\frac{a}{b}+\frac{d}{c}}{\frac{a}{b}-\frac{d}{c}}\right)^{(q-1)/4} \equiv \left(\dfrac{d}{c}\right)^r \pmod q \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } q \equiv 1 \pmod 4, \\ \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv \left(\dfrac{\frac{a}{b}-i}{\frac{a}{b}+i}\right)^{(q+1)/4} \equiv i^r \pmod q \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } q \equiv 3 \pmod 4. \end{cases}$$

To complete the proof, we note that

$$\begin{aligned}\left(\frac{ac+bd}{ac-bd}\right)^{(q-1)/4} &= \frac{(a^2c^2-b^2d^2)^{(q-1)/4}}{(ac-bd)^{(q-1)/2}}\\ &\equiv (a^2c^2+b^2c^2)^{(q-1)/4}\left(\frac{ac-bd}{q}\right)\\ &\equiv p^{(q-1)/4}\left(\frac{c}{q}\right)\left(\frac{ac-bd}{q}\right)\\ &= p^{(q-1)/4}\left(\frac{ac-bd}{q}\right)q.\end{aligned}$$

(Observe that $\left(\frac{c}{q}\right)=\left(\frac{|c|}{q}\right)=\left(\frac{q}{|c|}\right)=\left(\frac{d^2}{|c|}\right)=1$.)

Remark 2.1. Corollary 2.2(i) is equivalent to the rational quartic reciprocity law given by K. Burde [B] and H. von Lienen [Li].

Lemma 2.1. *Let $p\in\mathbb{N}$ be odd, $m,n\in\mathbb{Z}$ and $\gcd(m^2+n^2,p)=1$. Then*

$$\left(\frac{m+ni}{p}\right)_4^2=\left(\frac{m^2+n^2}{p}\right).$$

Proof. By (2.3), it is sufficient to prove the result for odd primes. Now assume that p is an odd prime. If $p\equiv 1 \pmod 4$ then $p=\pi\overline{\pi}$, where π is primary in $\mathbb{Z}[i]$. It is clear that

$$\begin{aligned}\left(\frac{m+ni}{p}\right)_4^2 &= \left(\frac{m+ni}{\pi}\right)_4^2\left(\frac{m+ni}{\overline{\pi}}\right)_4^2\\ &= \left(\frac{m+ni}{\pi}\right)_4^2\left(\frac{m-ni}{\pi}\right)_4^{-2}\equiv\left(\frac{m+ni}{m-ni}\right)^{(p-1)/2}\\ &= \frac{(m+ni)^{p-1}}{(m^2+n^2)^{(p-1)/2}}\equiv\left(\frac{m^2+n^2}{p}\right)\pmod{\pi}.\end{aligned}$$

Thus, $\left(\frac{m+ni}{p}\right)_4^2=\left(\frac{m^2+n^2}{p}\right)$.

If $p\equiv 3 \pmod 4$, then

$$\begin{aligned}\left(\frac{m+ni}{p}\right)_4^2 &\equiv (m+ni)^{(p^2-1)/2}=\left(\frac{(m+ni)^p}{m+ni}\right)^{(p+1)/2}\\ &\equiv\left(\frac{m-ni}{m+ni}\right)^{(p+1)/2}=\frac{(m^2+n^2)^{(p+1)/2}}{(m+ni)^{p+1}}\\ &\equiv\frac{(m^2+n^2)^{(p+1)/2}}{(m+ni)(m-ni)}\equiv\left(\frac{m^2+n^2}{p}\right)\pmod{p}.\end{aligned}$$

Hence again $\left(\frac{m+ni}{p}\right)_4^2=\left(\frac{m^2+n^2}{p}\right)$.

Combining the above we get the assertion.

THEOREM 2.4. *Let p be an odd prime and $k \in S_p$. Then $k \in Q_0(p)$ if and only if there is an integer n such that $n^2 \equiv k^2+1 \pmod p$ and $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right)$.*

Proof. Since $\left(\frac{i}{p}\right)_4 = i^{(p^2-1)/4} = \left(\frac{2}{p}\right)$ the result holds for $k \equiv 0 \pmod p$. So we may assume $k(k^2+1) \not\equiv 0 \pmod p$. If $p \equiv 1 \pmod 4$, it follows from Theorem 2.3(i) that

$$\begin{aligned} k \in Q_0(p) &\Leftrightarrow \left(\frac{(k+t)^2}{k^2-t^2}\right)^{(p-1)/4} = \left(\frac{k+t}{k-t}\right)^{(p-1)/4} \equiv 1 \pmod p \\ &\Leftrightarrow (k+t)^{(p-1)/2} \equiv (k^2+1)^{(p-1)/4} \pmod p \\ &\Leftrightarrow \text{there is an integer } n \text{ such that} \\ &\qquad n^2 \equiv k^2+1 \pmod p \text{ and } \left(\frac{k+t}{p}\right) = \left(\frac{n}{p}\right). \end{aligned}$$

When $n^2 \equiv k^2+1 \equiv k^2-t^2 \pmod p$ we have

$$\begin{aligned} (k+t+n)^2 &\equiv 2(k+n)(k+t) \pmod p, \\ (k+n+1)^2 &\equiv 2(k+n)(n+1) \pmod p \end{aligned}$$

and so

$$\left(\frac{k+t}{p}\right) = \left(\frac{n+1}{p}\right).$$

Hence, by the above, the result is true in the case $p \equiv 1 \pmod 4$.

Now assume $p \equiv 3 \pmod 4$. If $k \in Q_0(p)$ then $\left(\frac{k^2+1}{p}\right) = 1$ by Lemma 2.1. Let n be an integer such that $n^2 \equiv k^2+1 \pmod p$. It is easily seen that

$$(k+i)\cdot 2(k+n) \equiv (k+n+i)^2 \pmod p.$$

So we have

$$\begin{aligned} \left(\frac{k+i}{p}\right)_4 &\equiv (k+i)^{(p^2-1)/4} \equiv \frac{(k+n+i)^{(p^2-1)/2}}{(2(k+n))^{(p+1)(p-1)/4}} \\ &\equiv \left(\frac{k+n+i}{p}\right)_4^2 \quad \text{(by using Fermat's Little Theorem)} \\ &= \left(\frac{(k+n)^2+1}{p}\right) \quad \text{(by Lemma 2.1)} \\ &= \left(\frac{n}{p}\right)\left(\frac{2(k+n)}{p}\right) \pmod p. \end{aligned}$$

Observing that $(k+n+1)^2 \equiv 2(k+n)(n+1) \pmod p$ we get

$$\left(\frac{2(k+n)}{p}\right) = \left(\frac{n+1}{p}\right).$$

Hence,

$$\left(\frac{k+i}{p}\right)_4 = \left(\frac{n}{p}\right)\left(\frac{n+1}{p}\right).$$

This yields the result.

3. The structure of $Q'_r(p)$. In this section we introduce the sets $Q'_r(p)$ $(r = 0, 1, 2, 3)$ and study their group structure.

DEFINITION 3.1. Let p be an odd prime and $k \in S_p$. Define

$$\begin{aligned}
&[k]_p = \{x \mid x \equiv k \pmod p,\ x \in S_p\},\\
&[\infty]_p = \{n/m \mid m, n \in \mathbb{Z},\ p \mid m,\ p \nmid n\},\\
&Q'_0(p) = \{[k]_p \mid k \in Q_0(p)\} \cup \{[\infty]_p\},\\
&Q'_r(p) = \{[k]_p \mid k \in Q_r(p)\} \quad (r = 1, 2, 3)
\end{aligned}$$

and

$$Q'(p) = \bigcup_{r=0}^{3} Q'_r(p) = \{[\infty]_p\} \cup \{[k]_p \mid p \nmid (k^2+1),\ k \in \{0, 1, \dots, p-1\}\}.$$

For example, we have

$$Q'_0(5) = \{[\infty]_5\}, \quad Q'_1(5) = \{[1]_5\}, \quad Q'_2(5) = \{[0]_5\}, \quad Q'_3(5) = \{[-1]_5\}.$$

Let p be an odd prime, let

$$D_p = \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{if } p \equiv 1 \pmod 4,\\ \mathbb{Z}[i]/p\mathbb{Z}[i] & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

be the residue class ring modulo p, and U_p the multiplicative group of D_p. It is well known that U_p is a cyclic group of order $p^{(3-(\frac{-1}{p}))/2} - 1$. Denote the unique subgroup of order $p - (\frac{-1}{p})$ of U_p by G_p. Then G_p is also a cyclic group. So

$$S(p) = \begin{cases} \{g \mid g^{p-1} \equiv 1 \pmod p,\ g^n \not\equiv 1 \pmod p \\ \qquad (n = 1, 2, \dots, p-2),\ g \in \mathbb{Z}\} & \text{if } p \equiv 1 \pmod 4,\\ \{g \mid g^{p+1} \equiv 1 \pmod p,\ g^n \not\equiv 1 \pmod p \\ \qquad (n = 1, 2, \dots, p),\ g \in \mathbb{Z}[i]\} & \text{if } p \equiv 3 \pmod 4 \end{cases}$$
$$\neq \emptyset.$$

We are now ready to give

THEOREM 3.1. *Let p be an odd prime and $g \in S(p)$. For $r = 0, 1, 2, 3$ we have*

(i) $$|Q'_r(p)| = \frac{p - (\frac{-1}{p})}{4}.$$

(ii) $$Q'_r(p) = \left\{ \left[\left(\frac{-1}{p}\right) g^{(p-(\frac{-1}{p}))/4} \frac{g^{4s+r}+1}{g^{4s+r}-1} \right]_p \;\middle|\; s = 0, 1, \dots, \frac{p-(\frac{-1}{p})}{4} - 1 \right\}.$$

Proof. Suppose $k \in S_p$ with $k^2+1 \not\equiv 0 \pmod p$. If $p \equiv 1 \pmod 4$, then $(g^{(p-1)/4})^2 \equiv \left(\frac{g}{p}\right) = -1 \pmod p$. For $r \in \{0,1,2,3\}$ it follows from Theorem 2.3(i) that

$$k \in Q_r(p) \ \Leftrightarrow\ \left(\frac{k+g^{(p-1)/4}}{k-g^{(p-1)/4}}\right)^{(p-1)/4} \equiv g^{(p-1)r/4} \pmod p$$

$$\Leftrightarrow\ \frac{k+g^{(p-1)/4}}{k-g^{(p-1)/4}} \equiv g^{4s+r} \pmod p \text{ for some } s \in \{0,1,\ldots,(p-1)/4-1\}$$

$$\Leftrightarrow\ k \equiv g^{(p-1)/4}\frac{g^{4s+r}+1}{g^{4s+r}-1} \pmod p \text{ for some } s \in \{0,1,\ldots,(p-1)/4-1\}.$$

If $p \equiv 3 \pmod 4$, it is evident that $g^{(p+1)/4} \equiv \pm i \pmod p$. For $r \in \{0,1,2,3\}$ it follows from Theorem 2.3(ii) that

$$k \in Q_r(p) \Leftrightarrow \left(\frac{k-g^{(p+1)/4}}{k+g^{(p+1)/4}}\right)^{(p+1)/4} \equiv g^{(p+1)r/4} \pmod p$$

$$\Leftrightarrow\ \frac{k-g^{(p+1)/4}}{k+g^{(p+1)/4}} \equiv g^{4s+r} \pmod p \text{ for some } s \in \{0,1,\ldots,(p+1)/4-1\}$$

$$\Leftrightarrow\ k \equiv -g^{(p+1)/4}\frac{g^{4s+r}+1}{g^{4s+r}-1} \pmod p \text{ for some } s \in \{0,1,\ldots,(p+1)/4-1\}.$$

To conclude the proof, we note that

$$\left[\left(\frac{-1}{p}\right)g^{(p-(\frac{-1}{p}))/4}\frac{g^{4\cdot 0+0}+1}{g^{4\cdot 0+0}-1}\right]_p = [\infty]_p$$

and

$$\frac{g^{4s_1+r}+1}{g^{4s_1+r}-1} = 1+\frac{2}{g^{4s_1+r}-1} \not\equiv 1+\frac{2}{g^{4s_2+r}-1} = \frac{g^{4s_2+r}+1}{g^{4s_2+r}-1} \pmod p$$

provided $s_1 \not\equiv s_2 \pmod{\left(p-\left(\frac{-1}{p}\right)\right)/4}$.

Corollary 3.1. *Let p be an odd prime, and let R_p be a complete set of residues modulo p. Then*

$$\sum_{k\in Q_1(p)\cap R_p} k \equiv -\frac{1}{4} \pmod p.$$

Proof. Let $g \in S(p)$ and $m = \left(p-\left(\frac{-1}{p}\right)\right)/4$. It follows from Theorem 3.1 that

$$\sum_{k\in Q_1(p)\cap R_p} k \equiv \left(\frac{-1}{p}\right)g^m \sum_{s=0}^{m-1}\frac{g^{4s+1}+1}{g^{4s+1}-1}$$

$$= \left(\frac{-1}{p}\right)g^m\left(m+\sum_{s=0}^{m-1}\frac{2}{g^{4s+1}-1}\right) \pmod p.$$

Since

$$\sum_{s=0}^{m-1}\frac{1}{g^{4s+1}-1}=\sum_{s=0}^{m-1}\frac{1}{(g^{4s+1})^m-1}\sum_{t=0}^{m-1}(g^{4s+1})^t$$
$$\equiv\sum_{s=0}^{m-1}\frac{1}{g^m-1}\sum_{t=0}^{m-1}g^t\cdot g^{4st}=\frac{1}{g^m-1}\sum_{t=0}^{m-1}g^t\sum_{s=0}^{m-1}g^{4st}$$
$$=\frac{1}{g^m-1}\Bigl(m+\sum_{t=1}^{m-1}g^t\frac{1-g^{4mt}}{1-g^{4t}}\Bigr)\equiv\frac{m}{g^m-1}\pmod p,$$

we find

$$\sum_{k\in Q_1(p)\cap R_p}k\equiv\Bigl(\frac{-1}{p}\Bigr)g^m\Bigl(m+\frac{2m}{g^m-1}\Bigr)=\Bigl(\frac{-1}{p}\Bigr)m\frac{g^m+g^{2m}}{g^m-1}$$
$$\equiv\Bigl(\frac{-1}{p}\Bigr)m\frac{g^m-1}{g^m-1}\equiv-\frac{1}{4}\pmod p.$$

We are done.

THEOREM 3.2. *Let p be an odd prime. For $[k]_p,[k']_p\in Q'(p)$ define*

$$[k]_p[k']_p=\Bigl[\frac{kk'-1}{k+k'}\Bigr]_p\qquad([k]_p[\infty]_p=[\infty]_p[k]_p=[k]_p).$$

Then $Q'(p)$ forms a cyclic group of order $p-\left(\frac{-1}{p}\right)$, the union $Q'_0(p)\cup Q'_2(p)$ is a subgroup of order $\bigl(p-\left(\frac{-1}{p}\right)\bigr)/2$, and $Q'_0(p)$ is a subgroup of order $\bigl(p-\left(\frac{-1}{p}\right)\bigr)/4$. Moreover, $Q'_0(p)$, $Q'_1(p)$, $Q'_2(p)$ and $Q'_3(p)$ are the four distinct cosets of $Q'_0(p)$.

Proof. Suppose $g\in S(p)$. From Theorem 3.1 we know that

$$Q'(p)=\Bigl\{[k_r]_p\;\Big|\;r=0,1,\dots,p-\Bigl(\frac{-1}{p}\Bigr)-1\Bigr\},$$

where

$$[k_r]_p=\Bigl[\Bigl(\frac{-1}{p}\Bigr)g^{(p-(\frac{-1}{p}))/4}\frac{g^r+1}{g^r-1}\Bigr]_p.$$

Since

$$\Bigl[\frac{k_ik_j-1}{k_i+k_j}\Bigr]_p=\Bigl[\frac{\bigl(\left(\frac{-1}{p}\right)g^{(p-(\frac{-1}{p}))/4}\bigr)^2\cdot\frac{g^i+1}{g^i-1}\cdot\frac{g^j+1}{g^j-1}-1}{\left(\frac{-1}{p}\right)g^{(p-(\frac{-1}{p}))/4}\bigl(\frac{g^i+1}{g^i-1}+\frac{g^j+1}{g^j-1}\bigr)}\Bigr]_p$$
$$=\Bigl[\Bigl(\frac{-1}{p}\Bigr)g^{(p-(\frac{-1}{p}))/4}\frac{(g^i+1)(g^j+1)+(g^i-1)(g^j-1)}{(g^i+1)(g^j-1)+(g^i-1)(g^j+1)}\Bigr]_p$$
$$=\Bigl[\Bigl(\frac{-1}{p}\Bigr)g^{(p-(\frac{-1}{p}))/4}\frac{g^{i+j}+1}{g^{i+j}-1}\Bigr]_p,$$

we see that

$$[k_i]_p[k_j]_p=\left[\frac{k_ik_j-1}{k_i+k_j}\right]_p=[k_{\langle i+j\rangle}]_p,$$

where $\langle x\rangle$ denotes the least nonnegative residue of x to modulus $p-\left(\frac{-1}{p}\right)$.

By the above, $Q'(p)$ is a cyclic group generated by $[k_1]_p$. Applying Theorem 3.1 we see that $Q'_0(p)\cup Q'_2(p)$ is a cyclic group generated by $[k_2]_p$, $Q'_0(p)$ is a cyclic group generated by $[k_4]_p$, and that $Q'_0(p)$, $Q'_1(p)$, $Q'_2(p)$ and $Q'_3(p)$ are the four cosets of $Q'_0(p)$. The proof is now complete.

COROLLARY 3.2. *Let p be an odd prime, and $k\in S_p$. Then $k\in Q_0(p)$ if and only if $k\equiv(x^4-6x^2+1)/(4x^3-4x)\pmod p$ for some integer x satisfying $x^2\not\equiv -1\pmod p$.*

Proof. It follows from Theorem 3.2 that

$$\begin{aligned}[k]_p\in Q'_0(p)&\Leftrightarrow [k]_p=[x]_p[x]_p[x]_p[x]_p \text{ for some } [x]_p\in Q'(p)\\&\Leftrightarrow [k]_p=\left[\frac{x^2-1}{2x}\right]_p\left[\frac{x^2-1}{2x}\right]_p=\left[\frac{x^4-6x^2+1}{4x^3-4x}\right]_p\\&\qquad\text{for some integer } x \text{ satisfying } x^2+1\not\equiv 0\pmod p.\end{aligned}$$

So the result follows.

COROLLARY 3.3. *Let p be an odd prime, $r\in\{0,1,2,3\}$ and $[k_r]_p\in Q'_r(p)$. For $[k]_p\in Q'_0(p)$ define*

$$\varphi([k]_p)=\left[\frac{kk_r-1}{k+k_r}\right]_p\qquad(\varphi([\infty]_p)=[k_r]_p).$$

Then φ is a one-to-one correspondence from $Q'_0(p)$ to $Q'_r(p)$.

Proof. In view of Theorem 3.2,

$$Q'_r(p)=[k_r]_pQ'_0(p)=\{\varphi([k]_p)\mid [k]_p\in Q'_0(p)\}.$$

So the result follows.

REMARK 3.1. Corollaries 3.2 and 3.3 provide a simple method of calculating $Q'_0(p)$, $Q'_1(p)$, $Q'_2(p)$ and $Q'_3(p)$ for any odd prime p.

4. Connections with binary quadratic forms. For $a,b,c\in\mathbb{Z}$ let (a,b,c) denote the binary quadratic form $ax^2+bxy+cy^2$. We recall that the discriminant of (a,b,c) is b^2-4ac and (a,b,c) is primitive if $\gcd(a,b,c)=1$.

If a_1,b_1,c_1,a_2,b_2,c_2 are integers, and if there exist integers a,b,c,d such that $ad-bc=1$ and

$$a_1(ax+by)^2+b_1(ax+by)(cx+dy)+c_1(cx+dy)^2=a_2x^2+b_2xy+c_2y^2,$$

we say that the two forms (a_1,b_1,c_1) and (a_2,b_2,c_2) are *equivalent*, and write $(a_1,b_1,c_1)\sim(a_2,b_2,c_2)$.

Let $F(D)$ be the set of equivalence classes of primitive integral binary quadratic forms of discriminant D, and $h(D) = |F(D)|$. Denote by $[f]$ the equivalence class that contains the form f. In the nineteenth century, Gauss introduced the product of two equivalence classes in $F(D)$ by defining the composition of two forms, and showed that $F(D)$ forms a finite Abelian group of order $h(D)$.

LEMMA 4.1 ([C, p. 246]). *Let (a_1, b_1, c_1) and (a_2, b_2, c_2) be two binary quadratic forms of the same discriminant D. Set $s = (b_1 + b_2)/2$, $n = (b_1 - b_2)/2$ and let u, v, w and d be integers such that $ua_1 + va_2 + ws = d = \gcd(a_1, a_2, s)$, and let $d_0 = \gcd(d, c_1, c_2, n)$. Then*

$$[(a_1, b_1, c_1)][(a_2, b_2, c_2)] = [(a_3, b_3, c_3)],$$

where

$$a_3 = a_1 a_2 d_0/d^2, \quad b_3 = b_2 + 2a_2(vn - wc_2)/d, \quad c_3 = (b_3^2 - D)/(4a_3).$$

Using Lemma 4.1 we can prove

THEOREM 4.1. *Let p be an odd prime, and let $F(-16p^2)$ be the set of equivalence classes of primitive binary quadratic forms of discriminant $-16p^2$. If $f_\infty = f_\infty(x, y) = x^2 + 4p^2y^2$ and $f_k = f_k(x, y) = p^2x^2 + 4kpxy + 4(1 + k^2)y^2$, then the mapping*

$$\varphi : [f_m] \rightarrowtail [m]_p \quad (m \in \{k \mid k^2 \not\equiv -1 \pmod p,\ 0 \le k \le p-1,\ k \in \mathbb{Z}\} \cup \{\infty\})$$

is a group isomorphism from $F(-16p^2)$ to $Q'(p)$.

Proof. Suppose $k \in \mathbb{Z}$, $k^2 + 1 \not\equiv 0 \pmod p$, $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. It is clear that f_∞ and f_k are primitive forms of the same discriminant $D = -16p^2$. Since $ad - bc = 1$ we have $a^2 + 4c^2p^2 \neq p^2$. From this and the fact that

$$f_\infty(ax + by, cx + dy) = (a^2 + 4c^2p^2)x^2 + (2ab + 8cdp^2)xy + (b^2 + 4d^2p^2)y^2$$

we see that f_∞ is not equivalent to f_k.

Now assume $k' \in \mathbb{Z}$ and $k'^2 + 1 \not\equiv 0 \pmod p$. We claim that $f_k \sim f_{k'}$ if and only if $k \equiv k' \pmod p$. If $f_k \sim f_{k'}$, then there are integers a, b, c, d satisfying $ad - bc = 1$ and $f_k(ax + by, cx + dy) = p^2x^2 + 4k'pxy + 4(1 + k'^2)y^2$. From this it follows that

$$a^2p^2 + 4kacp + 4(1 + k^2)c^2 = p^2 \tag{4.1}$$

and

$$2abp^2 + 4k(ad + bc)p + 8(1 + k^2)cd = 4k'p. \tag{4.2}$$

Since $p \nmid (k^2 + 1)$, by (4.1) we must have $c = c'p$ for some integer c' and $(a + 2kc')^2 + 4c'^2 = 1$. This means $c = c'p = 0$ and so $ad + bc = 2bc + 1 = 1$. Hence $4k'p = 4kp + 2abp^2$ by (4.2). This implies that $k' \equiv k \pmod p$.

Conversely, if $k' \equiv k \pmod p$, we may take $a = d = 1,\ b = 2(k'-k)/p$ and $c = 0$ so that

$$f_k(ax+by, cx+dy) = f_k(x+2(k'-k)y/p, y) = f_{k'}(x,y).$$

Hence $f_k \sim f_{k'}$ and the claim is true.

From the above we see that $[f_k] \ne [f_\infty]$ and $[f_k] \ne [f_{k'}]$ when $k' \not\equiv k \pmod p$. Since

$$|\{k \mid k \in \{0,1,\ldots,p-1\},\ k^2+1 \not\equiv 0 \pmod p\}| = p - 1 - \left(\frac{-1}{p}\right)$$

there are $p - \left(\frac{-1}{p}\right)$ distinct equivalence classes with the discriminant $-16p^2$. But, according to [Co, p. 217] or [C, p. 233] the class number $h(-16p^2)$ is given by

$$h(-16p^2) = \frac{2}{4}\cdot 2p\left(1 - \frac{1}{p}\left(\frac{-4}{p}\right)\right) = p - \left(\frac{-1}{p}\right).$$

So we have

$$F(-16p^2) = \{[f_k] \mid k \in \{0,1,\ldots,p-1\},\ p\nmid (k^2+1)\} \cup \{[f_\infty]\}. \tag{4.3}$$

Now we prove that φ is an isomorphism from $F(-16p^2)$ to $Q'(p)$. Since $|F(-16p^2)| = |Q'(p)| = p - \left(\frac{-1}{p}\right)$, by the above φ is a one-to-one correspondence. So it is sufficient to show that φ is a homomorphism.

By taking $d = d_0 = 1,\ n = 2kp,\ u = w = 0$ and $v = 1$ in Lemma 4.1 we find $[f_k][f_\infty] = [f_k]$. Also, taking $d = d_0 = 1,\ n = 0,\ u = 1$ and $v = w = 0$ in Lemma 4.1 we see that $[f_\infty][f_\infty] = [f_\infty]$. If $k + k' \equiv 0 \pmod p$, taking $d = p^2,\ d_0 = 1,\ n = 2(k-k')p,\ u = 0,\ v = 1$ and $w = 0$ in Lemma 4.1 we get $[f_k][f_{k'}] = [(1, 4kp, 4(1+k^2)p^2)]$. Set $x' = x + 2kpy$ and $y' = y$. Then we find $x^2 + 4kpxy + 4(1+k^2)p^2y^2 = x'^2 + 4p^2y'^2$. So

$$[f_k][f_{k'}] = [(1, 4kp, 4(1+k^2)p^2)] = [(1,0,4p^2)] = [f_\infty].$$

If $k + k' \not\equiv 0 \pmod p$, we may choose integers u and w such that $up + 2(k+k')w = 1$. By taking $d = p$, $d_0 = 1$ and $v = 0$ in Lemma 4.1 we obtain $[f_k][f_{k'}] = [f_{k''}]$, where $k'' = k' - 2(1+k'^2)w$. Since $w \equiv \frac{1}{2(k+k')} \pmod p$ we see that

$$k'' \equiv k' - \frac{1+k'^2}{k+k'} = \frac{kk'-1}{k+k'} \pmod p.$$

So

$$\varphi([f_k][f_{k'}]) = \varphi([f_{k''}]) = [k'']_p = [k]_p[k']_p = \varphi([f_k])\varphi([f_{k'}]).$$

This is the desired result.

By the above, φ is a homomorphism from $F(-16p^2)$ to $Q'(p)$ and hence the proof is complete.

From Theorems 4.1 and 3.2 we have the following two corollaries.

COROLLARY 4.1. *Let p be an odd prime. Then $F(-16p^2)$ is a cyclic group of order $p-\left(\frac{-1}{p}\right)$.*

COROLLARY 4.2. *Let p be an odd prime and $k \in \mathbb{Z}$. Then $k \in Q_0(p)$ if and only if the quadratic form $p^2x^2+4kpxy+4(1+k^2)y^2$ is the fourth (composition) power of some primitive binary quadratic form of discriminant $-16p^2$.*

LEMMA 4.2. *Let $p \equiv 1 \pmod 4$ be a prime, $p = a^2+b^2$ $(a, b \in \mathbb{Z})$, $2 \mid b$, $q \in \mathbb{N}$ and $k \in \mathbb{Z}$. Then p is represented by the form $q^2x^2+4kqxy+4(1+k^2)y^2$ if and only if $kb \equiv \pm a \pmod q$.*

Proof. If $kb \equiv \pm a \pmod q$, setting $x = (\pm a - kb)/q$ and $y = b/2$ we find $x, y \in \mathbb{Z}$ and

$$p = a^2+b^2 = (qx+k\cdot 2y)^2+(2y)^2 = q^2x^2+4kqxy+4(1+k^2)y^2.$$

So p is represented by the form $(q^2, 4kq, 4(1+k^2))$.

Conversely, if $p = q^2x^2+4kqxy+4(1+k^2)y^2$ for some integers x, y and k, then $p = (qx+2ky)^2+4y^2$. So $qx+2ky = \pm a$ and $2y = \pm b$. This yields $kb \equiv \pm a \pmod q$ and the proof is complete.

Now we can give a criterion for quartic residuacity in terms of binary quadratic forms.

THEOREM 4.2. *Let p and q be two distinct odd primes and $p \equiv 1 \pmod 4$. Then $(-1)^{(q-1)/2}q$ is a quartic residue (mod p) if and only if p can be represented by one of the fourth (composition) powers of primitive binary quadratic forms of discriminant $-16q^2$.*

Proof. Set $q^* = (-1)^{(q-1)/2}q$ and $p = a^2+b^2$ $(a, b \in \mathbb{Z})$ with $2 \mid b$. From Theorem 2.2 we know that q^* is a quartic residue (mod p) (i.e. $(q^*)^{(p-1)/4} \equiv 1 \pmod p$) if and only if $q \mid b$ or $a/b \in Q_0(q)$.

If $q \mid b$, then q^* is a quartic residue (mod p) by the above. Also, $p = x^2+4q^2y^2$ for $x = a$ and $y = b/(2q)$. Since $[(1, 0, 4q^2)]^4 = [(1, 0, 4q^2)]$ by Theorem 4.1, we see that p is represented by the fourth power of the form $(1, 0, 4q^2)$. So the result holds when $q \mid b$.

Now assume $q \nmid b$. Then clearly p cannot be represented by $x^2+4q^2y^2$. Let $k \in \mathbb{Z}$ be such that $kb \equiv \pm a \pmod q$. It follows from Lemma 4.2 that p is represented by the form $q^2x^2+4kqxy+4(1+k^2)y^2$.

If q^* is a quartic residue (mod p), then $a/b \in Q_0(q)$ and therefore $k \in Q_0(q)$. Hence, by the above and Corollary 4.2, p is represented by the fourth power of some primitive binary quadratic form of discriminant $-16q^2$.

Conversely, if p is represented by the fourth power of some primitive binary quadratic form of discriminant $-16q^2$, according to (4.3) we know that p is represented by the fourth power of some form $(q^2, 4mq, 4(1+m^2))$,

where $m \in \{0, 1, \ldots, q-1\}$ and $m^2 \not\equiv -1 \pmod q$. Since p is not represented by $x^2 + 4q^2y^2$, in view of (4.3) we see that

$$[(q^2, 4mq, 4(1+m^2))]^4 = [(q^2, 4nq, 4(1+n^2))]$$

for some $n \in \{0, 1, \ldots, q-1\}$ satisfying $n^2 \not\equiv -1 \pmod q$. Hence p is represented by the form $(q^2, 4nq, 4(1+n^2))$. Applying Lemma 4.2 and Corollary 4.2 we find $n \equiv \pm a/b \pmod q$ and $n \in Q_0(q)$. Thus, $a/b \in Q_0(q)$ and hence q^* is a quartic residue (mod p).

Combining the above we prove the theorem.

REMARK 4.1. Theorem 4.2 can also be proved using class field theory, and the cubic analogue of Theorem 4.2 is already due to Dedekind [D] and Takagi [T]. See also [SW].

References

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

[B] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), 175–184.

[C] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[Co] H. Cohn, *Advanced Number Theory*, Dover, New York, 1962.

[D] R. Dedekind, *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. 121 (1900), 40–123; also: Ges. Math. Werke II, Braunschweig, 1932, 148–233.

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.

[L1] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), 20–29.

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

[Le1] F. Lemmermeyer, *Rational quartic reciprocity*, Acta Arith. 67 (1994), 387–390.

[Le2] —, *Rational quartic reciprocity II*, ibid. 80 (1997), 273–276.

[Li] H. von Lienen, *Reelle kubische und biquadratische Legendre-Symbole*, J. Reine Angew. Math. 305 (1979), 140–154.

[SW] B. K. Spearman and K. S. Williams, *The cubic congruence* $x^3+Ax^2+Bx+C \equiv 0 \pmod p$ *and binary quadratic forms*, J. London Math. Soc. (2) 46 (1992), 397–410.

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

[S2] —, *On the theory of cubic residues and nonresidues*, Acta Arith. 84 (1998), 291–335.

[T] T. Takagi, *Sur les corps résolubles algébriquement*, C. R. Acad. Sci. Paris 171 (1920), 1202–1205; also Collected Papers, 172–174.

[V] B. A. Venkov, *Elementary Number Theory*, translated from the Russian and edited by H. Alderson, Wolters-Noordhoff, Groningen, 1970, 88.

[W] K. S. Williams, *On Yamamoto's reciprocity law*, Proc. Amer. Math. Soc. 111 (1991), 607–609.

[Y] Y. Yamamoto, *Congruences modulo* 2^i $(i = 3, 4)$ *for the class numbers of quadratic fields*, in: Proc. Internat. Conf. on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986), Nagoya Univ., 1986, 205–215.

Department of Mathematics
Huaiyin Teachers College
Huaiyin, Jiangsu 223001
The People's Republic of China
E-mail: hyzhsun@public.hy.js.cn

Received on 24.2.1999
and in revised form on 26.6.2000 (3563)