Quartic Residuacity and Cusp Forms
of Weight One

by

Toyokazu Hiramatsu and Noburo Ishii

(Received November 19, 1984)

§ 1. Introduction

Let $m$ be a positive square free integer and $\varepsilon_m$ denote the fundamental unit of $\mathbb{Q}(\sqrt{m})$. We consider only those $m$ for which $\varepsilon_m$ has norm $+1$. If $l$ is an odd prime such that $(m/l)= (\varepsilon_m/l) = 1$, we can ask for the value of the quartic residue symbol $(\varepsilon_m/l)_4$ (cf. [1], [5]). Let $K$ be the Galois extension of degree 16 over the rational number field $\mathbb{Q}$ generated by $\sqrt{-1}$ and $\sqrt[4]{\varepsilon_m}$. Then its Galois group $G(K/\mathbb{Q})$ has just two irreducible representations of degree 2. We can define a cusp form of weight one by these representations, which will be denoted by $\Theta(\tau; K)$. In this paper, we shall show that $\Theta(\tau; K)$ has three expressions by definite or indefinite theta series and that the value of the symbol $(\varepsilon_m/l)_4$ is expressed by the $l$th Fourier coefficient of $\Theta(\tau; K)$. These results offer us new criterions for $\varepsilon_m$ to be a quartic residue modulo $l$.

§ 2. Cusp forms of weight one

We put $G = G(K/\mathbb{Q})$. Then the group $G$ is generated by three elements $\sigma$, $\varphi$ and $\rho$ in such way that

$$
\begin{align*}
\sigma(\sqrt[4]{\varepsilon_m}) &= \sqrt{-1} \sqrt[4]{\varepsilon_m}, \\
\varphi(\sqrt[4]{\varepsilon_m}) &= \sqrt[4]{\varepsilon_m}^{-1}, \\
\rho(\sqrt{-1}) &= -\sqrt{-1},
\end{align*}
$$

and has defining relations:

$$
\begin{align*}
\sigma^4 &= \varphi^2 = \rho^2 = 1, \\
\varphi \sigma \rho &= \sigma \varphi = \rho \varphi,
\end{align*}
$$

$$
\rho \sigma \rho = \varphi \sigma \rho = \sigma^3.
$$

The group $G$ has three abelian subgroups of index 2 in $G$, which are the following:

$$
\begin{align*}
H_k &= \langle \sigma, \varphi \rho \rangle \longleftrightarrow k = \mathbb{Q}(\sqrt{-m}), \\
H_F &= \langle \sigma^2, \varphi, \rho \rangle \longleftrightarrow F = \mathbb{Q}(\sqrt{t+2}), \\
H_E &= \langle \sigma^2, \varphi, \sigma \rho \rangle \longleftrightarrow E = \mathbb{Q}(\sqrt{-m(t+2)}),
\end{align*}
$$
where \( t = \text{tr}(\varepsilon_m) \). Let \( f \) and \( e \) be the square free part of \( t + 2 \) and \( m(t + 2) \), respectively, and put

\[
K' = \mathbb{Q}(\sqrt{-1}, \sqrt{e_m}), \\
L = \mathbb{Q}(\sqrt{-1}, \sqrt{-m}), \\
L' = \mathbb{Q}(\sqrt{-m}, \sqrt{f}), \\
L'' = \mathbb{Q}(\sqrt{-m}, \sqrt{-f}).
\]

Then we have the following diagram:

\[
\begin{array}{c}
\text{\( K \)} \\
\text{\( K' \)} \\
\text{\( L' \)} \\
\text{\( L \)} \\
\text{\( L'' \)} \\
\text{\( F = \mathbb{Q}(\sqrt{f}) \)} \\
\text{\( E = \mathbb{Q}(\sqrt{-e}) \)} \\
\text{\( Q(\sqrt{-m}) \)} \\
\text{\( Q(\sqrt{e}) \)} \\
\text{\( Q(\sqrt{-f}) \)}
\end{array}
\]

By this diagram, we have the following equivalence for any odd prime \( l \):

(1) \quad l \text{ splits completely in } K' \iff (-1/l) = (f/l) = (e/l) = 1,

where \((*/l)\) denotes the Legendre symbol.

The group \( G \) has the following eight representations \( \gamma_j \) of degree 1, where \( j = 1, \cdots, 8 \).

<table>
<thead>
<tr>
<th>( \gamma_1 )</th>
<th>( \gamma_2 )</th>
<th>( \gamma_3 )</th>
<th>( \gamma_4 )</th>
<th>( \gamma_5 )</th>
<th>( \gamma_6 )</th>
<th>( \gamma_7 )</th>
<th>( \gamma_8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \sigma )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>( \varphi )</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>( \rho )</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
</tbody>
</table>

The group \( G \) has just two irreducible representations of degree 2, which have determinant \( \gamma_4 \). If we denote by \( \psi_0 \) the one of these, then the other is \( \psi_0 \otimes \gamma_3 \). Let \( \sigma_l \) denote the Frobenius substitution associated with \( l \) in \( K \). Then we have the following table which gives the correspondence between quadratic subfields of \( K \) and \( \gamma_j \) (\( 2 \leq j \leq 8 \)).

<table>
<thead>
<tr>
<th>( \gamma_2 )</th>
<th>( \gamma_3 )</th>
<th>( \gamma_4 )</th>
<th>( \gamma_5 )</th>
<th>( \gamma_6 )</th>
<th>( \gamma_7 )</th>
<th>( \gamma_8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \gamma(\sigma_l) )</td>
<td>( \mathbb{Q}(\sqrt{-1}) )</td>
<td>( \mathbb{Q}(\sqrt{m}) )</td>
<td>( k )</td>
<td>( F )</td>
<td>( \mathbb{Q}(\sqrt{-f}) )</td>
<td>( \mathbb{Q}(\sqrt{e}) )</td>
</tr>
<tr>
<td>( \text{(-1/l)} )</td>
<td>( \text{(-m/l)} )</td>
<td>( \text{(f/l)} )</td>
<td>( \text{(-f/l)} )</td>
<td>( \text{(e/l)} )</td>
<td>( (-e/l) )</td>
<td></td>
</tr>
</tbody>
</table>

Put \( \psi_1 = \psi_0 \otimes \gamma_3 \). Let \( L(s; K/Q, \psi_0) \) (resp. \( L(s; K/Q, \psi_1) \)) denote the Artin \( L \)-function associated with \( \psi_0 \) (resp. \( \psi_1 \)), and let \( \Theta(\tau; \psi_0) \) (resp. \( \Theta(\tau; \psi_1) \)) denote the Mellin transformation of \( L(s; K/Q, \psi_0) \) (resp. \( L(s; K/Q, \psi_1) \)). Then we can define the following function which appeared in §1:
\[ \Theta(\tau; K) = \frac{1}{2} \{ \Theta(\tau; \psi_0) + \Theta(\tau; \psi_1) \} . \]

Let \( N \) denote the L.C.M. of the conductor of \( \psi_0 \) and that of \( \psi_1 \). Then the function \( \Theta(\tau; K) \) is a cusp form of weight 1 on the congruence subgroup \( \Gamma_0(N) \) with the character \((-m/l)\). This result is essentially based upon the work of Hecke.

Let \( M \) be one of the three quadratic fields \( k, E \) and \( F \). Then \( K \) is abelian over \( M \). Let \( \mathfrak{Q}_M \) be the ring of integers of \( M \) and \( a \) an ideal of \( \mathfrak{Q}_M \). If \( M \) is imaginary (resp. real), then \( H_M(a) \) denotes the group of ray classes (resp. narrow ray classes) modulo \( a \) of \( M \). Let \( b \) be an ideal of \( M \) prime to \( a \) and \([b]\) the class in \( H_M(a) \) represented by \( b \). If in particular \( b \) is an element of \( M \), then the ideal class \([b]\) represented by the principal ideal \((b)\) is abbreviated as \([b]\). Let \( \widehat{\mathfrak{f}}(K/M) \) (resp. \( \widehat{\mathfrak{f}}((K/M)) \)) be the conductor (resp. the finite part of conductor) of \( K \) over \( M \). Furthermore we denote by \( C_M(K) \) (resp. \( C_M(K') \)) the subgroup of \( H_M(\widehat{\mathfrak{f}}((K/M))) \) corresponding to \( K \) (resp. \( K' \)). The restriction \( \psi_0 \) (resp. \( \psi_1 \)) to the abelian Galois group \( G(K/M) \) decomposes into two distinct linear representations \( \xi_M \) and \( \xi'_M \) (resp. \( \xi_M \otimes \gamma_3 \) and \( \xi'_M \otimes \gamma_3 \)) of \( G(K/M) \):

\[ \psi_i \big| G(K/M) = \xi_M \otimes \gamma_3 + \xi'_M \otimes \gamma_3, \quad (i = 0, 1). \]

By Artin reciprocity law, we can identify \( \xi_M \) and \( \xi'_M \) with characters of \( H_M(\widehat{\mathfrak{f}}((K/M))) \) trivial on \( C_M(K) \) and so we denote these characters by the same notation. Let \( c_M \) be the finite part of conductor of \( \xi_M \). We assume that the finite part of conductor of \( \xi_M \otimes \gamma_3 \) is equal to \( c_M \). Let \( \widehat{C}_M(K) \) (resp. \( \widehat{C}_M(K') \)) be the image of \( C_M(K) \) (resp. \( C_M(K') \)) by the canonical homomorphism of \( H_M(\widehat{\mathfrak{f}}((K/M))) \) to \( H_M(c_M) \). Since \( K \) is the class field over \( M \) with conductor \( \widehat{\mathfrak{f}}((K/M)) \), the Artin L-function \( L(s; K/Q, \psi_0) \) (resp. \( L(s; K/Q, \psi_1) \)) is coincident with the L-function \( L_M(s; \xi_M) \) (resp. \( L_M(s; \xi'_M \otimes \gamma_3) \)) of \( M \) associated with the character \( \xi_M \) (resp. \( \xi'_M \otimes \gamma_3 \)), where \( \xi_M \) (resp. \( \xi'_M \otimes \gamma_3 \)) denotes the primitive character corresponding to \( \xi_M \) (resp. \( \xi'_M \otimes \gamma_3 \)). Therefore we have three expressions of \( \Theta(\tau; K) \).

**Proposition 1.** The notation and the assumption being as above, we have

(2) \[ \Theta(\tau; K) = \sum_{a \in \mathfrak{Q}_M} \chi_M(a)q^{N_M(a)} \quad (q = \exp(2\pi i \tau)), \]

where

\[ \chi_M(a) = \begin{cases} 
1 & \text{if } [a] \in \widehat{C}_M(K), \\
-1 & \text{otherwise}; 
\end{cases} \]

and \( N_M(a) \) denotes the norm of \( a \) with respect to \( M/Q \).

The proof of Proposition 1 is quite similar to that appeared in §3 of [3]. Therefore we omit it.

Let \( f(\alpha) \) be a defining polynomial of \( \sqrt[4]{\xi_m} \) over \( Q \). Then it is easy to see that
\[ f(x) = (x^4 - \varepsilon_m)(x^4 - \varepsilon_m^{-1}) = x^8 - tx^4 + 1. \]

Let \( a(n) \) be the \( n \)th Fourier coefficient of the expansion

\[ \Theta(r; K) = \sum_{n=1}^{\infty} a(n)q^n. \]

Then we have the following relation:

**Proposition 2.** Let \( p \) be any prime not dividing the discriminant \( \Delta_f \) of \( f(x) \) and \( \mathbf{F}_p \) the \( p \) element field. Then we have

\[ \# \{ x \in \mathbf{F}_p \mid \tilde{f}(x) = 0 \} = 1 + (m/p) + (f/p) + (e/p) + 2a(p). \]

**Proof.** Let \( H \) be a group generated by \( \rho \), say \( H = \langle \rho \rangle \). Then \( H \) is the subgroup of \( G \) corresponding to \( \mathbb{Q}(\sqrt{\varepsilon_m}) \). We denote by \( 1^G_H \) the character of \( G \) induced by the identity character of \( H \). Then we have the following scalar product formulas.

\[ (1^G_H \mid \chi_0) = \begin{cases} 1 & \text{if } i = 1, 3, 5, 7, \\ 0 & \text{otherwise}; \end{cases} \]

\[ (1^G_H \mid \chi_i) = 1 \quad (i = 0, 1), \]

where \( \chi_0 \) (resp. \( \chi_1 \)) denotes the character of \( \psi_0 \) (resp. \( \psi_1 \)). Therefore, we have

\[ 1^G_H(\sigma_p) = \sum_{\substack{1 \leq l \leq 7 \\text{odd}}} \gamma_l(\sigma_p) + \chi_0(\sigma_p) + \chi_1(\sigma_p) = 1 + (m/p) + (f/p) + (e/p) + 2a(p). \]

On the other hand, it is easy to see that the left hand side of (3) is equal to \( 1^G_H(\sigma_p) \). This proves our proposition.

Let \( \text{Spl}(f(x)) \) be the set of all primes such that \( f(x) \mod p \) factors into a product of distinct linear polynomials over \( \mathbf{F}_p \). We call a rule to determine the primes belonging to \( \text{Spl}(f(x)) \) a higher reciprocity law for \( f(x) \) (cf. [2]). Then we have the following

**Corollary.** \( \text{Spl}(f(x)) = \{ p : p \nmid \Delta_f, \ a(p) = 2 \} \).

**Proof.** By Proposition 1, we have

\[ |a(p)| \leq 2. \]

Hence our assertion is a direct consequence of Proposition 2.

q.e.d.

§ 3. Fundamental lemmas

In this section, we shall determine the conductors \( (K/M), (K'/M), (L'/M) \)
and \( f(L/M) \). Let \( \mathcal{R}, \mathcal{L} \) and \( \mathfrak{K} \) be fields such that \( \mathcal{R} \supset \mathcal{L} \supset \mathfrak{K} \) and \([\mathcal{L} : \mathfrak{K}] = 2\). Assume that \( \mathcal{R} \) is abelian over \( \mathfrak{K} \). We denote by \( \mathfrak{D}(\mathcal{L}/\mathfrak{K}) \) the different of \( \mathcal{L} \) over \( \mathfrak{K} \). For a prime ideal \( q \) of \( \mathcal{L} \), let \( f(q) \) (resp. \( g(q) \)) denote the \( q \)-exponent of \( f(\mathcal{R}/\mathcal{L}) \) (resp. \( \mathfrak{D}(\mathcal{L}/\mathfrak{K}) \)) and put
\[
e(q) = \max \{ 0, g(q) - f(q) \}.
\]
Then we have the following

**Lemma 1.**

\[
f(\mathcal{R}/\mathfrak{K}) = f(\mathcal{R}/\mathcal{L}) \mathfrak{D}(\mathcal{L}/\mathfrak{K}) \prod q^{e(q)}.
\]

**Proof.** This is deduced from the proof of Lemma 1 in [3].

We assume that \( \mathcal{L} \) is a Galois extension over \( \mathbb{Q} \). Let \( \mathbb{Q}_e \) be the ring of integers of \( \mathcal{L} \) and let \( p \) be a prime ideal of \( \mathbb{Q}_e \) dividing 2. We denote by \( e_p \) the ramification exponent of \( p \). Let \( \mathbb{Q}_e \) denote the completion of \( \mathbb{Q}_e \) with respect to \( p \) and \( \Pi_p \) a prime element of \( \mathbb{Q}_e \). Furthermore, for \( \xi \in \mathbb{Q}_e^\times \), we put
\[
S_p(\xi) = \max \{ t \in \mathbb{Z}^+ \mid \xi \equiv \text{square mod } \Pi_p^t \}.
\]

**Lemma 2.** If \( S_p(\xi) < 2e_p \), then there exists uniquely the odd integer \( t < 2e_p \) such that
\[
\xi = \eta^2 + \delta \Pi_p^t \quad (\eta, \delta \in \mathbb{Q}_e^\times);
\]
and this uniquely determined \( t \) is equal to \( S_p(\xi) \).

**Proof.** The assertion is clear.

**Lemma 3.** Put
\[
t_p(\xi) = \min \{ n \in \mathbb{Z} \mid \xi \Pi_p^{2n} = \text{square mod } \Pi_p^{2e_p}, 0 \leq n \leq e_p \}.
\]
If \( S_p(\xi) < 2e_p \), then we have
\[
S_p(\xi) = 2e_p + 1 - 2t_p(\xi).
\]

**Proof.** This follows immediately from the definition.

Let \( \alpha \) be an element of \( \mathbb{Q}_e \) such that \( (\alpha) \) is a square-free ideal with \( ((\alpha), 2) = 1 \) and put \( \mathcal{R} = \mathbb{Q}(\sqrt{\alpha}) \). We assume that \( \mathcal{R} \) is a Galois extension over \( \mathbb{Q} \). Then \( S_p(\alpha) \) is independent of \( p \) chosen. Since \( \mathcal{R} \) and \( \mathcal{L} \) are the Galois extensions over \( \mathbb{Q} \), the \( p \)-exponent \( f(p) \) of \( f(\mathcal{R}/\mathcal{L}) \) does not depend on \( p \) chosen. Thus we can put \( S_e(\alpha) = S_e(\alpha) \) and \( f(2) = f(p) \).

**Lemma 4.** (i) The prime ideal \( p \) is ramified for \( \mathcal{R}/\mathcal{L} \) if and only if \( S_p(\alpha) < 2e_p \).
(ii) If \( S_e(\alpha) < 2e_p \), then \( S_e(\alpha) \) is equal to the odd number \( t \) \( (\alpha < 2e_p) \) determined by
\[
\alpha = \eta^2 + \delta \Pi_p^t \quad (\eta, \delta \in \mathbb{Q}_e^\times);
\]
and moreover
\[
f(2) = 2e_p + 1 - S_e(\alpha).
Proof. By the assumption on \( \alpha \), we have

\[ \mathfrak{Q}_o = \left\{ \frac{1}{2}(a + b \sqrt{\alpha}) \mid a, b \in \mathfrak{Q}_o, a^2 - 2b^2 \equiv 0 \mod 4 \right\}. \]

Denote by \( \mathfrak{P} \) a prime ideal of \( \mathfrak{K} \) dividing \( p \). Let \( a \) be an ideal of \( \mathfrak{K} \) and denote by \( v_{\mathfrak{P}}(a) \) the \( \mathfrak{P} \)-exponent of \( a \), and let \( \varepsilon \) be a generator of \( G(\mathfrak{K}/\mathfrak{L}) \). Then, by the definition of \( f(p) \),

\[ f(2) = \min_{\xi \in \mathfrak{Q}_o} v_{\mathfrak{P}}(\xi - \varepsilon^2). \]

Denote by \( X \) (resp. \( X_p \)) the group of all elements \( b \) of \( \mathfrak{Q}_o \) satisfying the condition

\[ ab^2 \equiv \text{square mod } 4 \] (resp. \( \mod p^{2e_\varepsilon} \)).

Let \( v_p(b) \) denote the \( p \)-exponent of \( b \). Then, by (4), we have

\[ f(2) = \min_{b \in X} v_p(b) = 2 \min_{b \in X_p} v_p(b). \]

Therefore,

\[ p \text{ is unramified for } \mathfrak{K}/\mathfrak{L} \iff f(2) = 0 \]

\[ \iff \alpha \text{ is square mod } p^{2e_\varepsilon} \iff S_\varepsilon(\alpha) \geq 2e_\varepsilon. \]

If \( p \) is ramified for \( \mathfrak{K}/\mathfrak{L} \), then

\[ \min_{b \in X_p} v_p(b) = t_\varepsilon(\alpha). \]

By Lemma 3, \( S_\varepsilon(\alpha) = 2e_\varepsilon + 1 - f(2) \). Hence by Lemma 2 the assertion (ii) is proved. q.e.d.

Now we assume that \( \mathfrak{L}(\sqrt{\alpha}) \) is a Galois extension over \( \mathbb{Q} \). It is easy to see that there exists a subgroup \( R \) of \( \mathfrak{Q}_o^* \) with order \( |\mathfrak{Q}_o/\mathfrak{P}| - 1 \) such that \( R^* = R \cup \{0\} \) is a complete system of coset representatives of \( \mathfrak{Q}_o \mod \mathfrak{P} \). Put

\[ t = \min\{2e_\varepsilon, S_\varepsilon(\alpha)\} \text{ and } u = \left\lfloor \frac{1}{2}(t + 1) \right\rfloor. \]

Then there exist elements \( a_0, a_1, \cdots, a_{u-1} \) of \( R^* \) such that

\[ \alpha \equiv (a_0 + a_1 \Pi_\varepsilon + \cdots + a_{u-1} \Pi_{p}^{u-1})^2 \mod \Pi_{p}^t. \]

**Lemma 5.** (i) If \( p \) is unramified for \( \mathfrak{K}/\mathfrak{L} \) and there exists a non-zero element in \( \{a_i : \varepsilon \text{ odd}\} \), then

\[ S_{\mathfrak{L}}(\sqrt{\alpha}) = \min \{i : \varepsilon \text{ odd} \mid a_i \neq 0\}. \]

(ii) If \( p \) is ramified for \( \mathfrak{K}/\mathfrak{L} \) and there exists a prime element \( \Pi_{\mathfrak{P}} \) of \( \mathfrak{Q}_o \) such that

\[ \Pi_{\mathfrak{P}} = \Pi_{\mathfrak{P}}^2 \mod \Pi_{\mathfrak{P}}^{u+1}, \text{ then} \]
Quartic Residuacity and Cusp Forms of Weight One

\[ S_{\mathfrak{a}}(\sqrt{2}) = S_{\mathfrak{a}}(\alpha). \]

**Proof.** Put

\[ A = a_0 + a_1 \Pi_\mathfrak{p} + \cdots + a_{u-1} \Pi_\mathfrak{p}^{u-1}. \]

If \( p \) is unramified for \( \mathfrak{R}/\mathfrak{L} \), then we put \( \Pi_{\mathfrak{p}} = \Pi_\mathfrak{p} \). It is easy to see that

\[ \sqrt{\alpha} = A + \varepsilon_1 \Pi_{\mathfrak{p}}^{\varepsilon_0} \quad (\varepsilon_1 \in \mathcal{Q}_{\mathfrak{p}}). \]

Therefore the assertion (i) is an immediate consequence of Lemma 4. On the other hand, if \( p \) is ramified for \( \mathfrak{R}/\mathfrak{L} \), then we take \( \Pi_{\mathfrak{p}} \) which satisfies the condition in (ii). We can take the elements \( b_i \in \mathbb{R}^* \) with \( a_i = b_i^2 \) \( (i = 0, 1, \cdots, u - 1) \). Therefore,

\[ \sqrt{\alpha} = (b_0 + b_1 \Pi_\mathfrak{p} + \cdots + b_{u-1} \Pi_\mathfrak{p}^{u-1})^2 + \varepsilon_2 \Pi_{\mathfrak{p}}^{\varepsilon_0} \quad (\varepsilon_2 \in \mathcal{Q}_{\mathfrak{p}}). \]

Hence we obtain the assertion (ii) by Lemma 4. q.e.d.

Now we put

\[ \mathfrak{L} = L \quad \text{or} \quad K', \alpha = \varepsilon_m. \]

From now on we assume that \( m \) is prime number \( p \) with \( p \equiv 3 \mod 4 \). We put

\[ \varepsilon_p = \varepsilon = A + B\sqrt{p}. \]

Then it is easy to verify that \( A \) is an even number. Since \( A^2 - pB^2 = 1 \), we have \( (A+1)(A-1) = pB^2 \). Therefore we can put

\[ \begin{cases} A - 1 = r^2u, \\ A + 1 = s^2v, \end{cases} \]

with \( (ru, sv) = 1, rs = B \) and \( uv = p \) \( (r, s, u, v \in \mathbb{Z}^+) \). Hence,

\[ 2 = s^2v - r^2u. \]

By considering the above relation mod 8, we have

\[ (u, v) = \begin{cases} (1, p) & \text{if } p \equiv 3 \mod 8, \\ (p, 1) & \text{if } p \equiv 7 \mod 8. \end{cases} \]

Since \( t = \text{tr} (\varepsilon) = 2A \), we have \( t + 2 = 2s^2v \). Hence

\[ (f, e) = \begin{cases} (2p, 2) & \text{if } p \equiv 3 \mod 8, \\ (2, 2p) & \text{if } p \equiv 7 \mod 8. \end{cases} \]

Therefore we have the following lemma.

**Lemma 6.** With \( F \) and \( E \) as in §1, we have

\[ (F, E) = \begin{cases} (\mathbb{Q}(\sqrt{2p}), \mathbb{Q}(\sqrt{-2})) & \text{if } p \equiv 3 \mod 8, \\ (\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2p})) & \text{if } p \equiv 7 \mod 8. \end{cases} \]
Now we shall calculate the conductors \( \mathfrak{f}(K/M) \), \( \mathfrak{f}(K'/M) \), \( \mathfrak{f}(L/M) \) and \( \mathfrak{f}(L'/M) \). Because the method of calculation is very similar for each of three cases, we shall give the details only for the case of \( M = k \). If we put \( \varOmega = L \), then \( K' = L(\sqrt{e}) \). We can take \( e_L = 2 \) and \( \Pi_p = 1 - \sqrt{p} \). Therefore,

\[
\epsilon \equiv 1 - \Pi_p \mod 2.
\]

By Lemma 4, \( S_L(e) = 1 \) and hence \( S_K(\sqrt{e}) = 1 \) by (ii) of Lemma 5. Therefore, again by Lemma 4, we have \( f_K(2) = 5 - 1 = 4 \). Since prime factors of 2 are only ramified for \( K'/L \), we have \( \mathfrak{f}(K'/L) = (4) \), and hence \( \mathfrak{D}(K'/L) = (2) \). By \( e_{K'} = 4 \), \( f_K(2) = 9 - 1 = 8 \). Therefore \( \mathfrak{f}(K/K') = (4) \). Consequently, by Lemma 1, we have

\[
\mathfrak{f}(K/L) = \mathfrak{f}(K/K') \mathfrak{D}(K'/L) = (4) \times (2) = (8).
\]

Thus, we obtain the following:

\[
\begin{align*}
\mathfrak{f}(K/k) &= \mathfrak{f}(K/L) \mathfrak{D}(L/k) = (16), \\
\mathfrak{f}(K'/k) &= \mathfrak{f}(K'/L) \mathfrak{D}(L/k) = (8), \\
\mathfrak{f}(L/k) &= \mathfrak{D}(L/k)^2 = (4).
\end{align*}
\]

Therefore our required conductors are as follows.

<table>
<thead>
<tr>
<th>( M )</th>
<th>( \mathfrak{f}(K/M) )</th>
<th>( \mathfrak{f}(K'/M) )</th>
<th>( \mathfrak{f}(L'/M) )</th>
<th>( \mathfrak{f}(L/M) )</th>
<th>( c_M )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k )</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>( F )</td>
<td>( p \equiv 3 \mod 8 )</td>
<td>( 4p \alpha_1 \alpha_2 )</td>
<td>( (2) \alpha_1 \alpha_2 )</td>
<td>( \infty_1 \alpha_2 )</td>
<td>( 4p )</td>
</tr>
<tr>
<td></td>
<td>( p \equiv 7 \mod 8 )</td>
<td>( (4\sqrt{2}p) \alpha_1 \alpha_2 )</td>
<td>( (2p) \alpha_1 \alpha_2 )</td>
<td>( (p) \alpha_1 \alpha_2 )</td>
<td>( 4p )</td>
</tr>
<tr>
<td>( E )</td>
<td>( p \equiv 3 \mod 8 )</td>
<td>( 4\sqrt{-2p} )</td>
<td>( 2p )</td>
<td>( p )</td>
<td>( 4p )</td>
</tr>
<tr>
<td></td>
<td>( p \equiv 7 \mod 8 )</td>
<td>( 4p )</td>
<td>( 2 )</td>
<td>( 1 )</td>
<td>( 4p )</td>
</tr>
</tbody>
</table>

In the above table, \( \varpi \) denotes a prime ideal of \( M \) dividing \( p \), and \( p_2 \) denotes a prime ideal of \( M \) dividing 2. Further \( \infty_i \) \( (i = 1, 2) \) denote two infinite places of \( F \).

§ 4. Three expressions of \( \Theta(\tau; K) \)

For an integral ideal \( a \) of \( M \), if \( M \) is imaginary (resp. real), then \( P_M(a) \) denotes the subgroup of \( H_M(a) \) generated by principal classes (resp. principal classes represented by totally positive elements). We write simply \( H_M \) and \( P_M \) in place of \( H_M(\mathfrak{f}(K/M)) \) and \( P_M(\mathfrak{f}(K/M)) \) respectively. Suppose that \( a \) divides \( \mathfrak{f}(K/M) \). Then we denote by \( K(a) \) the kernel of the canonical homomorphism: \( P_M \to P_M(a) \). Moreover we put \( C_M^*(\cdot) = P_M \cap C_M(\cdot) \). In the following, we shall obtain \( C_M(K) \) and \( C_M(K') \) under the assumption \( p \equiv 7 \mod 8 \).
Case 1. $M = k \ (= \mathbb{Q}(\sqrt{-p}))$.

By the assumption, we have $2 = p_2 \bar{p}_2$ in $k$, where $\bar{p}_2$ denotes the conjugate of $p_2$. Take the two elements $\mu$ and $v$ of $\mathbb{Q}_k$ such that

\[
\begin{align*}
\mu & \equiv 5 \mod p_2^4, \\
v & \equiv -1 \mod p_2^4, \\
\mu & \equiv 1 \mod \bar{p}_2^4, \\
v & \equiv 1 \mod \bar{p}_2^4.
\end{align*}
\]

Then we have the following relations: $[\mu][\bar{\mu}] = 5$, $[\mu]^4 = [\bar{\mu}]^4 = 1$, $[v] = [\bar{v}]$ and $[v]^2 = 1$. We also have

\[P_k = \langle [\mu], [\bar{\mu}], [v] \rangle, \quad K((4)) = \langle [\mu], [\bar{\mu}] \rangle,\]

\[K((8)) = \langle [\mu]^2, [\bar{\mu}]^2 \rangle.\]

By the above table, we see that

\[[P_k : C_k(L)^*] = [C_k(L)^* : C_k(K)^*] = [C_k(K')^* : C_k(K)^*] = 2.\]

Furthermore,

\[C_k(L)^* \supset K((4)), \quad C_k(K')^* \supset K((8)), \quad \not\supset K((4)), \quad C_k(K)^* \not\supset K((8)).\]

Hence

\[C_k(L)^* = K((4)) = \langle [\mu], [\bar{\mu}] \rangle,\]

\[C_k(K')^* = \langle [\mu]^2, [\bar{\mu}]^2, [\mu][\bar{\mu}] \rangle,\]

\[C_k(K)^* \not\supset [\mu]^2, [\bar{\mu}]^2.\]

Since $G(K/\mathbb{Q})$ is non-abelian and $G(K/k) \cong P_k/C_k(K)^*$, we see $[\mu]^{-1}[\bar{\mu}] \notin C_k(K)^*$. Therefore, $[\mu][\bar{\mu}] \in C_k(K)^*$. Hence we have

\[C_k(K)^* = \langle [\mu][\bar{\mu}] \rangle = \langle [5] \rangle.\]

We put

\[H_k = \sum_{b \in S} [b]P_k,\]

where $S$ denotes the index set of integral ideals $b$. Then

\[C_k(K') = C_k(K) + C_k[K][\mu]^2,\]

\[C_k(K) = \sum_{b \in S} [b]^{-4}C_k(K)^*.\]

Put $\omega = (1 + \sqrt{-p})/2$ and let $a$ be an ideal of $\mathbb{Q}_k$ with $(a, (2)) = 1$. Then, by the above relations, we have $[a] \in C_k(K')$ if and only if there exist $b \in S$ and $\eta = x + y\omega \in b^4$ such that $x \equiv 1 \mod 2$, $y \equiv 0 \mod 8$ and $a = b^{-4}(\eta)$. Moreover
\[ [a] \in C_k(K) \iff y \equiv 0 \mod 16. \]

Therefore, if \( M = k \), then the right hand side of (2) is as follows:

\[
\Theta(\tau; K) = \sum_{b \in \mathfrak{S}} \sum_{4x+1+4y \sqrt{-p} = b^4} (-1)^y \cdot q^{(4x+1+y)^2 + 16py^2/N_kq(b)^4}.
\]

Case 2. \( M = F (= \mathbb{Q}(\sqrt{2})) \).

Let \( \alpha \) be an element of \( \mathfrak{Q}_F \). Then there exists an element \( \alpha^* \) of \( \mathfrak{Q}_F \) such that

\[
\begin{aligned}
\alpha^* & \text{ is totally positive,} \\
\alpha^* & \equiv \alpha \mod 4\sqrt{2}, \\
\alpha^* & \equiv 1 \mod p.
\end{aligned}
\]

Let \( p = p_\alpha \) in \( F \), and \( r(p) \) denote a generator of the multiplicative group \( (\mathfrak{Q}_F/p)^* \). Take a totally positive element \( \lambda \) of \( \mathfrak{Q}_F \) such that

\[
\begin{aligned}
\lambda & \equiv 1 \mod 4\sqrt{2}, \\
\lambda & \equiv r(p) \mod p, \\
\lambda & \equiv 1 \mod p_\alpha.
\end{aligned}
\]

Then

\[
H_F = P_F = \langle [e_2^*], [3^*], [5^*], [\lambda], [\lambda] \rangle;
\]

and

\[
[e_2^*]^4 = [3^*]^2 = [5^*]^2 = [\lambda]^{p-1} = 1,
\]

\[
[\sqrt{e_2^*}] = [3^*][5^*][e_2^*]^3.
\]

Furthermore,

\[
\begin{aligned}
K_F(p) = & \langle [e_2^*], [3^*], [5^*], [\lambda] \rangle, \\
K_F((p)) = & \langle [e_2^*], [3^*], [5^*] \rangle, \\
K_F(2p) = & \langle [3^*], [5^*], [e_2^*]^2 \rangle, \\
K_F(4p) = & \langle [5^*] \rangle.
\end{aligned}
\]

Therefore, by the above table of conductors, we see that

\[
[P_F : C_F(L')] = [C_F(L') : C_F(K')] = [C_F(K') : C_F(K)] = 2;
\]

\[
C_F(L') \supseteq K_F((p)), \quad \# F(p),
\]

\[
C_F(K') \supseteq K_F((2p)), \quad \# K_F((p)),
\]

\[
C_F(K) \supsetneq K_F((4p)).
\]
Hence we obtain
\[ C_f(L') = \langle [e_2^*], [3^*], [5^*], [\lambda]; [\lambda], [\lambda] \rangle. \]

Since the Galois group \( G(K'/\mathbb{Q}) \) is isomorphic to \( P_f/C_f(K') \), we have
\[ C_f(K') \equiv [\lambda]^2, [\lambda]^2, [\lambda]^{-1}[\lambda]. \]

Hence
\[ C_f(K') = \langle [\lambda]^2, [\lambda]^2, [\lambda]^2, [\lambda][\lambda] \rangle. \]

Next we shall calculate \( C_f(K) \). First we notice that
\[ \begin{cases} C_f(K) \equiv [\lambda]^2, [\lambda]^2, [e_2^*]^2, \\ C_f(K) \not\equiv [5^*]. \end{cases} \]

Take a prime \( q \) such that \( q \equiv 3 \mod 8 \) and \( (q/p) = -1 \). Then \( q \) remains prime in \( F \) and \( [q] = [3^*][[\lambda][\lambda]] \) (\( a : \text{odd} \)). Since \( (-p/q) = -1 \), \( q \) remains prime in \( k \) also. Hence, by the result of Case 1, \( q \) splits completely for \( K/k \). Therefore \([q] \in C_f(K)\), i.e.,
\[ C_f(K) \equiv [3^*][[\lambda][\lambda]]. \]

Similarly, \([5^*][[\lambda][\lambda]] \in C_f(K)\). Therefore we obtain
\[ C_f(K) = \langle [e_2^*]^2, [\lambda]^2, [\lambda]^2, [3^*][\lambda][\lambda], [5^*][\lambda][\lambda] \rangle. \]

Let \( r \) be a rational integer with \( r^2 \equiv 2 \mod p \) and \( \mu = x + y\sqrt{2} \) be a totally positive element of \( \mathcal{O}_F \) such that \( (2p, \mu) = 1 \). Then we have
\[ [\mu] \in C_f(K') \iff x: \text{odd}, y: \text{even}, ((x^2 - 2y^2)/p) = 1. \]

Further
\[ [\mu] \in C_f(K) \iff (\text{sgn}x)((ry - x)/p)(2/x) = 1. \]

We put
\[ \begin{cases} E^+ = \{ e \in \mathcal{O}_F^\times \mid e: \text{totally positive} \}, \\ E^0 = \{ e \in E^+ \mid e - 1 \in \mathfrak{f}(K/F) \}, \end{cases} \]
and \( e = [E^+: E^0] \). Then, the right hand side of (2) has the following expression for \( M = F \).

(6)
\[ \Theta(\tau; K) = e^{-1} \sum_{x^2 + 2y^2 = 2, x \equiv 1 \mod 4, N_\mathbb{Q}(\mu) > 0, \mu \mod E^0} \text{sgn}(x)((2ry - x)/p)(2/x)q^{x^2 - 8y^2}. \]

Case 3. \( M = E (= \mathcal{O}(\sqrt{-2p})) \).

By a similar calculation of Case 2, we have the following:
\[ \Theta(\tau; K) = \sum_{a} \sum_{4x + 1 + 2y \sqrt{-2p} e} (-1)^{x+y} \cdot q^{[(4x+1)^2 + 8py^2]/N_{E/Q}(a)}, \]

where \( \{a\} \) denotes the set of integral ideals of \( E \) which are representatives of all square classes in \( H_E/P_E \).

Summing up (5), (6) and (7), we obtain the following theorem which is our main purpose.

**THEOREM.** Let \( p \) be any prime with \( p \equiv 7 \mod 8 \). Then, the notation and the assumption being kept as above, we have the three expressions of \( \Theta(\tau; K) \):

\[ \Theta(\tau; K) = \sum_{a} \sum_{4x + 1 + 2y \sqrt{-2p} e} (-1)^{x+y} \cdot q^{[(4x+1)^2 + 8py^2]/N_{E/Q}(a)} \] (via \( E \))

\[ = \sum_{b} \sum_{4x + 1 + 4y \sqrt{-p} b t} (-1)^{y} \cdot q^{[(4x+1)^2 + 16py^2]/N_{E/Q}(b)} \] (via \( k \))

\[ = e^{-1} \sum_{\mu=1+2x'} \frac{(\text{sgn} \mu(2ry-x)/p)(2/x)q^{x^2-8y^2}}{\mu \mod E} \] (via \( F \))

Let \( l \) be an odd prime number satisfying the conditions \( (p/l) = 1 \) and \( l \equiv 1 \mod 8 \). Then we have \( (\varepsilon_p/l) = 1 \) by (1), and we have also the following from the theorem above:

\[ l = ((4a+1)^2 + 8pb^2)/N_{E/Q}(a), \]

\[ l = ((4x+1)^2 + 16p\beta^2)/N_{E/Q}(b), \]

\[ l = x^2 - 8y^2, \quad x \equiv 1 \mod 4, \quad ((x^2 - 8y^2)/p) = 1; \]

\[ a(l) = \pm 2. \]

Moreover, we have the following criterions for \( \varepsilon_p \) to be a quartic residue modulo \( l \) which are our conclusion.

\[ (\varepsilon_p/l)_4 = 1 \iff a + b: \text{even} \]

\[ \iff \beta: \text{even} \]

\[ \iff (\text{sgn} x)(2ry - x)/p(2/x) = 1 \]

\[ \iff a(l) = 2. \]

For prime \( p \) with \( p \equiv 3 \mod 8 \), we shall only state the result as a remark.

**Remark 1.** Let \( p \equiv 3 \mod 8 \) and \( p \neq 3 \). Then, the following may be obtained in a way similar to the proof of the above theorem.
Quartic Residuacity and Cusp Forms of Weight One

\[ \Theta(\tau; K) = \sum_{x, y \in \mathbb{Z}} \frac{(-1)^{(x-1)/4}((x-2ry)/p)}{q^{x^2 + 8y^2}} \]

[\text{mod 4}]

[\text{mod 8}]

[\text{mod 4}]

**Remark 2.** A similar problem for the rational case was discussed in [4].

**References**


Department of Mathematics
Kobe University
Rokko, Kobe 657
Japan

Department of Mathematics
University of Osaka Prefecture
Sakai, Osaka 591
Japan