COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 34, No. 1, 1985

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

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 ε_m denote the fundamental unit of $\mathbf{Q}(\sqrt{m})$. We consider only those m for which ε_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 $\mathbf{Q}$ generated by $\sqrt{-1}$ and $\sqrt[4]{\varepsilon_m}$. Then its Galois group $G(K/\mathbf{Q})$ 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 lth Fourier coefficient of $\Theta(\tau; K)$. These results offer us new criterions for ε_m to be a quartic residue modulo l.

§ 2. Cusp forms of weight one

We put $G=G(K/\mathbf{Q})$. Then the group G is generated by three elements σ, φ and ρ in such way that

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

and has defining relations:

$$\sigma^4=\varphi^2=\rho^2=1\,, \qquad \varphi\rho=\rho\varphi\,,$$
$$\rho\sigma\rho=\varphi\sigma\varphi=\sigma^3\,.$$

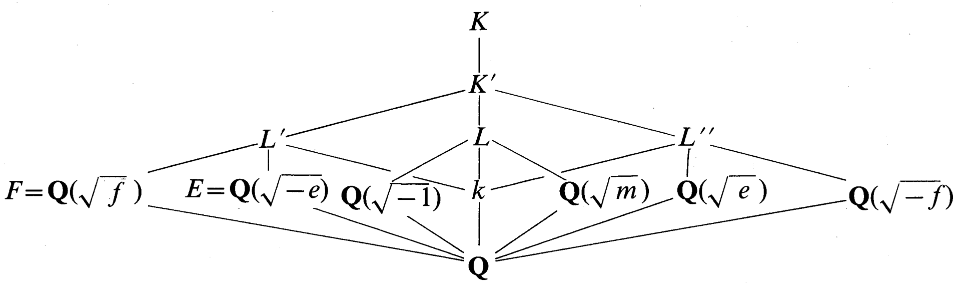
The group G has three abelian subgroups of index 2 in G, which are the following:

$$H_k=\langle\sigma, \varphi\rho\rangle \longleftrightarrow k=\mathbf{Q}(\sqrt{-m})\,,$$
$$H_F=\langle\sigma^2, \varphi, \rho\rangle \longleftrightarrow F=\mathbf{Q}(\sqrt{t+2})\,,$$
$$H_E=\langle\sigma^2, \sigma\varphi, \sigma\rho\rangle \longleftrightarrow E=\mathbf{Q}(\sqrt{-m(t+2)})\,,$$

where $t=\mathrm{tr}(\varepsilon_m)$. Let f and e be the square free part of $t+2$ and $m(t+2)$, respectively, and put

$$K'=\mathbf{Q}(\sqrt{-1},\sqrt{\varepsilon_m}),\qquad L=\mathbf{Q}(\sqrt{-1},\sqrt{-m}),$$
$$L'=\mathbf{Q}(\sqrt{-m},\sqrt{f}),\qquad L''=\mathbf{Q}(\sqrt{-m},\sqrt{-f}).$$

Then we have the following diagram:



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

(1) $\quad l$ splits completely in $K' \Leftrightarrow (-1/l)=(f/l)=(e/l)=1$,

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

The group G has the following eight representations γ_j of degree 1, where $j=1,\cdots,8$.

	γ_1	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
σ	1	1	1	1	-1	-1	-1	-1
φ	1	1	-1	-1	1	1	-1	-1
ρ	1	-1	1	-1	1	-1	1	-1

The group G has just two irreducible representations of degree 2, which have determinant γ_4. If we denote by ψ_0 the one of these, then the other is $\psi_0\otimes\gamma_3$. Let σ_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 γ_j $(2\leq j\leq 8)$.

	γ_2	γ_3	γ_4	γ_5	γ_6	γ_7	γ_8
	$\mathbf{Q}(\sqrt{-1})$	$\mathbf{Q}(\sqrt{m})$	k	F	$\mathbf{Q}(\sqrt{-f})$	$\mathbf{Q}(\sqrt{e})$	E
$\gamma_j(\sigma_l)$	$(-1/l)$	(m/l)	$(-m/l)$	(f/l)	$(-f/l)$	(e/l)	$(-e/l)$

Put $\psi_1=\psi_0\otimes\gamma_3$. Let $L(s;K/\mathbf{Q},\psi_0)$ (resp. $L(s;K/\mathbf{Q},\psi_1)$) denote the Artin L-function associated with ψ_0 (resp. ψ_1), and let $\Theta(\tau;\psi_0)$ (resp. $\Theta(\tau;\psi_1)$) denote the Mellin transformation of $L(s;K/\mathbf{Q},\psi_0)$ (resp. $L(s;K/\mathbf{Q},\psi_1)$). 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 ψ_0 and that of ψ_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 $\mathfrak{O}_M$ be the ring of integers of M and $\mathfrak{a}$ an ideal of $\mathfrak{O}_M$. If M is imaginary (resp. real), then $H_M(\mathfrak{a})$ denotes the group of ray classes (resp. narrow ray classes) modulo $\mathfrak{a}$ of M. Let $\mathfrak{b}$ be an ideal of M prime to $\mathfrak{a}$ and $[\mathfrak{b}]$ the class in $H_M(\mathfrak{a})$ represented by $\mathfrak{b}$. 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 $\tilde{\mathfrak{f}}(K/M)$ (resp. $\mathfrak{f}(K/M)$) 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 $H_M(\mathfrak{f}(K/M))$ corresponding to K (resp. K'). The restriction ψ_0 (resp. ψ_1) to the abelian Galois group $G(K/M)$ decomposes into two distinct linear representations ξ_M and ξ'_M (resp. $\xi_M\otimes\gamma_3$ and $\xi'_M\otimes\gamma_3$) of $G(K/M)$:

$$\psi_i\,|\,G(K/M)=\xi_M\otimes\gamma_3^i+\xi'_M\otimes\gamma_3^i\,, \qquad (i=0,\ 1)\,.$$

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

$$\Theta(\tau; K)=\sum_{\substack{\mathfrak{a}\subset\mathfrak{O}_M\\ [\mathfrak{a}]\in\widetilde{C_M(K')}}}\chi_M(\mathfrak{a})q^{N_{M/\mathbf{Q}}(\mathfrak{a})} \qquad (q=\exp(2\pi i\tau))\,, \tag{2}$$

where

$$\chi_M(\mathfrak{a})=\begin{cases}1 & \text{if } [\mathfrak{a}]\in\widetilde{C_M(K)}\,,\\ -1 & \text{otherwise};\end{cases}$$

and $N_{M/\mathbf{Q}}(\mathfrak{a})$ denotes the norm of $\mathfrak{a}$ with respect to $M/\mathbf{Q}$.

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

Let $f(x)$ be a defining polynomial of $\sqrt[4]{\varepsilon_m}$ over $\mathbf{Q}$. 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 nth Fourier coefficient of the expansion

$$\Theta(\tau;\,K)=\sum_{n=1}^{\infty}a(n)q^n\,.$$

Then we have the following relation:

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

(3) $$\#\{x\in\mathbf{F}_p\,|\,f(x)=0\}=1+(m/p)+(f/p)+(e/p)+2a(p)\,.$$

Proof. Let H be a group generated by ρ, say $H=\langle\rho\rangle$. Then H is the subgroup of G corresponding to $\mathbf{Q}(\sqrt[4]{\varepsilon_m})$. We denote by 1_H^G the character of G induced by the identity character of H. Then we have the following scalar product formulas.

$$(1_H^G\,|\,\gamma_i)=\begin{cases}1 & \text{if}\quad i=1,\,3,\,5,\,7\,,\\ 0 & \text{otherwise};\end{cases}$$

$$(1_H^G\,|\,\chi_i)=1\qquad (i=0,\,1)\,,$$

where χ_0 (resp. χ_1) denotes the character of ψ_0 (resp. ψ_1). Therefore, we have

$$1_H^G(\sigma_p)=\sum_{\substack{1\le i\le 7\\ i:\mathrm{odd}}}\gamma_i(\sigma_p)+\chi_0(\sigma_p)+\chi_1(\sigma_p)$$
$$=1+(m/p)+(f/p)+(e/p)+2a(p)\,.$$

On the other hand, it is easy to see that the left hand side of (3) is equal to $1_H^G(\sigma_p)$. This proves our proposition. q.e.d.

Let $Spl\{f(x)\}$ 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 $Spl\{f(x)\}$ a higher reciprocity law for $f(x)$ (cf. [2]). Then we have the following

COROLLARY. $Spl\{f(x)\}=\{p: p\nmid\Delta_f,\ a(p)=2\}$.

Proof. By Proposition 1, we have

$$|a(p)|\le 2\,.$$

Hence our assertion is a direct consequence of Proposition 2. q.e.d.

§ 3. Fundamental lemmas

In this section, we shall determine the conductors $\mathfrak{f}(K/M)$, $\mathfrak{f}(K'/M)$, $\mathfrak{f}(L'/M)$

and $\mathfrak{f}(L/M)$. Let $\mathfrak{K}$, $\mathfrak{L}$ and $\mathfrak{F}$ be fields such that $\mathfrak{K}\supset\mathfrak{L}\supset\mathfrak{F}$ and $[\mathfrak{L}:\mathfrak{F}]=2$. Assume that $\mathfrak{K}$ is abelian over $\mathfrak{F}$. We denote by $\mathfrak{D}(\mathfrak{L}/\mathfrak{F})$ the different of $\mathfrak{L}$ over $\mathfrak{F}$. For a prime ideal $\mathfrak{q}$ of $\mathfrak{L}$, let $f(\mathfrak{q})$ (resp. $g(\mathfrak{q})$) denote the $\mathfrak{q}$-exponent of $\mathfrak{f}(\mathfrak{K}/\mathfrak{L})$ (resp. $\mathfrak{D}(\mathfrak{L}/\mathfrak{F})$) and put

$$e(\mathfrak{q})=\max\{0, g(\mathfrak{q})-f(\mathfrak{q})\}\ .$$

Then we have the following

LEMMA 1.

$$\mathfrak{f}(\mathfrak{K}/\mathfrak{F})=\mathfrak{f}(\mathfrak{K}/\mathfrak{L})\mathfrak{D}(\mathfrak{L}/\mathfrak{F})\prod_{\mathfrak{q}}\mathfrak{q}^{e(\mathfrak{q})}\ .$$

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

We assume that $\mathfrak{L}$ is a Galois extension over $\mathbf{Q}$. Let $\mathfrak{O}_{\mathfrak{L}}$ be the ring of integers of $\mathfrak{L}$ and let $\mathfrak{p}$ be a prime ideal of $\mathfrak{O}_{\mathfrak{L}}$ dividing 2. We denote by $e_{\mathfrak{L}}$ the ramification exponent of $\mathfrak{p}$. Let $\mathfrak{O}_{\mathfrak{p}}$ denote the completion of $\mathfrak{O}_{\mathfrak{L}}$ with respect to $\mathfrak{p}$ and $\Pi_{\mathfrak{p}}$ a prime element of $\mathfrak{O}_{\mathfrak{p}}$. Furthermore, for $\xi\in\mathfrak{O}_{\mathfrak{p}}^{\times}$, we put

$$S_{\mathfrak{p}}(\xi)=\max\{t\in\mathbf{Z}^{+}\mid\xi\equiv\text{square}\bmod\Pi_{\mathfrak{p}}^{t}\}\ .$$

LEMMA 2. *If $S_{\mathfrak{p}}(\xi)<2e_{\mathfrak{L}}$, then there exists uniquely the odd integer $t<2e_{\mathfrak{L}}$ such that*

$$\xi=\eta^2+\delta\Pi_{\mathfrak{p}}^{t}\qquad\{\eta, \delta\in\mathfrak{O}_{\mathfrak{p}}^{\times})\ ;$$

and this uniquely determined t is equal to $S_{\mathfrak{p}}(\xi)$.

Proof. The assertion is clear.

LEMMA 3. *Put*

$$t_{\mathfrak{p}}(\xi)=\min\{n\in\mathbf{Z}\mid\xi\Pi_{\mathfrak{p}}^{2n}=\textit{square}\bmod\Pi_{\mathfrak{p}}^{2e_{\mathfrak{L}}},\ 0\le n\le e_{\mathfrak{L}}\}\ .$$

If $S_{\mathfrak{p}}(\xi)<2e_{\mathfrak{L}}$, then we have

$$S_{\mathfrak{p}}(\xi)=2e_{\mathfrak{L}}+1-2t_{\mathfrak{p}}(\xi)\ .$$

Proof. This follows immediately from the definition.

Let α be an element of $\mathfrak{O}_{\mathfrak{L}}$ such that (α) is a square-free ideal with $((\alpha), 2)=1$ and put $\mathfrak{K}=\mathfrak{L}(\sqrt{\alpha})$. We assume that $\mathfrak{K}$ is a Galois extension over $\mathbf{Q}$. Then $S_{\mathfrak{p}}(\alpha)$ is independent of $\mathfrak{p}$ chosen. Since $\mathfrak{K}$ and $\mathfrak{L}$ are the Galois extensions over $\mathbf{Q}$, the $\mathfrak{p}$-exponent $f(\mathfrak{p})$ of $\mathfrak{f}(\mathfrak{K}/\mathfrak{L})$ does not depend on $\mathfrak{p}$ chosen. Thus we can put $S_{\mathfrak{L}}(\alpha)=S_{\mathfrak{p}}(\alpha)$ and $f(2)=f(\mathfrak{p})$.

LEMMA 4. (i) *The prime ideal $\mathfrak{p}$ is ramified for $\mathfrak{K}/\mathfrak{L}$ if and only if $S_{\mathfrak{L}}(\alpha)<2e_{\mathfrak{L}}$.*
(ii) *If $S_{\mathfrak{L}}(\alpha)<2e_{\mathfrak{L}}$, then $S_{\mathfrak{L}}(\alpha)$ is equal to the odd number t $(<2e_{\mathfrak{L}})$ determined by*

$$\alpha=\eta^2+\delta\Pi_{\mathfrak{p}}^{t}\qquad(\eta, \delta\in\mathfrak{O}_{\mathfrak{p}}^{\times})\ ;$$

and moreover

$$f(2)=2e_{\mathfrak{L}}+1-S_{\mathfrak{L}}(\alpha)\ .$$

Proof. By the assumption on α, we have

$$\mathfrak{O}_{\mathfrak{K}}=\left\{\frac{1}{2}(a+b\sqrt{\alpha})\,\middle|\, a,\ b\in\mathfrak{O}_{\mathfrak{L}},\ a^2-\alpha b^2\equiv 0 \bmod 4\right\}.$$

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

$$f(2)=\min_{\xi\in\mathfrak{O}_{\mathfrak{K}}} \mathfrak{v}_{\mathfrak{P}}(\xi-\xi^{\varepsilon})\,. \tag{4}$$

Denote by X (resp. $X_{\mathfrak{p}}$) the group of all elements b of $\mathfrak{O}_{\mathfrak{L}}$ satisfying the condition

$$\alpha b^2\equiv \text{square} \bmod 4 \ (\text{resp.} \bmod \mathfrak{p}^{2e_{\mathfrak{L}}}).$$

Let $\mathfrak{v}_{\mathfrak{p}}(\mathfrak{b})$ denote the $\mathfrak{p}$-exponent of (b). Then, by (4), we have

$$\begin{aligned} f(2)&=2\min_{b\in X} \mathfrak{v}_{\mathfrak{p}}(b)\\ &=2\min_{b\in X_{\mathfrak{p}}} \mathfrak{v}_{\mathfrak{p}}(b)\,. \end{aligned}$$

Therefore,

$$\begin{aligned} &\mathfrak{p}\quad \text{is unramified for}\quad \mathfrak{K}/\mathfrak{L}\Leftrightarrow f(2)=0\\ \Leftrightarrow &\alpha\quad \text{is square} \bmod \mathfrak{p}^{2e_{\mathfrak{L}}}\Leftrightarrow S_{\mathfrak{L}}(\alpha)\geq 2e_{\mathfrak{L}}\,. \end{aligned}$$

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

$$\min_{b\in X_{\mathfrak{p}}} \mathfrak{v}_{\mathfrak{p}}(b)=t_{\mathfrak{p}}(\alpha)\,.$$

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

Now we assume that $\mathfrak{L}(\sqrt[4]{\alpha})$ is a Galois extension over $\mathbf{Q}$. It is easy to see that there exists a subgroup R of $\mathfrak{O}_{\mathfrak{p}}^{\times}$ with order $|\mathfrak{O}_{\mathfrak{L}}/\mathfrak{p}|-1$ such that $R^*=R\cup\{0\}$ is a complete system of coset representatives of $\mathfrak{O}_{\mathfrak{L}} \bmod \mathfrak{p}$. Put

$$t=\min\{2e_{\mathfrak{L}},\ S_{\mathfrak{L}}(\alpha)\}\quad \text{and}\quad u=\left[\frac{1}{2}(t+1)\right].$$

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

$$\alpha\equiv(a_0+a_1\Pi_{\mathfrak{p}}+\cdots+a_{u-1}\Pi_{\mathfrak{p}}^{u-1})^2 \bmod \Pi_{\mathfrak{p}}^{t}\,.$$

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

$$S_{\mathfrak{K}}(\sqrt{\alpha})=\min\{i:\text{odd}\,|\,a_i\neq 0\}\,.$$

(ii) *If $\mathfrak{p}$ is ramified for $\mathfrak{K}/\mathfrak{L}$ and there exists a prime element $\Pi_{\mathfrak{P}}$ of $\mathfrak{O}_{\mathfrak{P}}$ such that $\Pi_{\mathfrak{p}}=\Pi_{\mathfrak{P}}^2 \bmod \Pi_{\mathfrak{P}}^{t+1}$, then*

$$S_{\mathfrak{K}}(\sqrt{\alpha})=S_{\mathfrak{L}}(\alpha)\,.$$

Proof. Put

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

If $\mathfrak{p}$ is unramified for $\mathfrak{K}/\mathfrak{L}$, then we put $\Pi_{\mathfrak{P}}=\Pi_{\mathfrak{p}}$. It is easy to see that

$$\sqrt{\alpha}=A+\varepsilon_1\Pi_{\mathfrak{P}}^{e_{\mathfrak{L}}}\qquad(\varepsilon_1\in\mathfrak{O}_{\mathfrak{K}})\,.$$

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

$$\sqrt{\alpha}=(b_0+b_1\Pi_{\mathfrak{P}}+\cdots+b_{u-1}\Pi_{\mathfrak{P}}^{u-1})^2+\varepsilon_2\Pi_{\mathfrak{P}}^{t}\qquad(\varepsilon_2\in\mathfrak{O}_{\mathfrak{P}}^{\times})\,.$$

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 $p\equiv 3 \bmod 4$. 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 $uv=p$ $(r, s, u, v\in\mathbf{Z}^+)$. Hence,

$$2=s^2v-r^2u\,.$$

By considering the above relation mod 8, we have

$$(u, v)=\begin{cases}(1, p) & \text{if}\quad p\equiv 3 \bmod 8\,,\\ (p, 1) & \text{if}\quad p\equiv 7 \bmod 8\,.\end{cases}$$

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

$$(f, e)=\begin{cases}(2p, 2) & \text{if}\quad p\equiv 3 \bmod 8\,,\\ (2, 2p) & \textit{if}\quad p\equiv 7 \bmod 8\,.\end{cases}$$

Therefore we have the following lemma.

LEMMA 6. *With F and E as in § 1, we have*

$$(F, E)=\begin{cases}(\mathbf{Q}(\sqrt{2p}), \mathbf{Q}(\sqrt{-2})) & \text{if}\quad p\equiv 3 \bmod 8\,,\\ (\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{-2p})) & \text{if}\quad p\equiv 7 \bmod 8\,.\end{cases}$$

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 $\mathfrak{L}=L$, then $K'=L(\sqrt{\varepsilon})$. We can take $e_L=2$ and $\Pi_p=1-\sqrt{p}$. Therefore,

$$\varepsilon \equiv 1-\Pi_p \bmod 2 .$$

By Lemma 4, $S_L(\varepsilon)=1$ and hence $S_{K'}(\sqrt{\varepsilon})=1$ 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

$$\begin{aligned}\mathfrak{f}(K/L)&=\mathfrak{f}(K/K')\mathfrak{D}(K'/L)\\&=(4)\times(2)=(8) .\end{aligned}$$

Thus, we obtain the following:

$$\begin{cases}\mathfrak{f}(K/k)=\mathfrak{f}(K/L)\mathfrak{D}(L/k)=(16) ,\\ \mathfrak{f}(K'/k)=\mathfrak{f}(K'/L)\mathfrak{D}(L/k)=(8) ,\\ \mathfrak{f}(L/k)=\mathfrak{D}(L/k)^2=(4) .\end{cases}$$

Therefore our required conductors are as follows.

M		$\mathfrak{f}(K/M)$	$\mathfrak{f}(K'/M)$	$\mathfrak{f}(L'/M)$	$\mathfrak{f}(L/M)$	c_M
	k	16	8	8	4	16
F	$p\equiv 3 \bmod 8$	$4\mathfrak{p}_2\infty_1\infty_2$	$(2)\infty_1\infty_2$	$\infty_1\infty_2$		$4\mathfrak{p}_2$
	$p\equiv 7 \bmod 8$	$(4\sqrt{2p})\infty_1\infty_2$	$(2p)\infty_1\infty_2$	$(p)\infty_1\infty_2$		$4\tilde{\mathfrak{p}}$
E	$p\equiv 3 \bmod 8$	$4\sqrt{-2p}$	$2p$	p		$4\tilde{\mathfrak{p}}$
	$p\equiv 7 \bmod 8$	$4\mathfrak{p}_2$	2	1		$4\mathfrak{p}_2$

In the above table, $\tilde{\mathfrak{p}}$ denotes a prime ideal of M dividing p, and $\mathfrak{p}_2$ denotes a prime ideal of M dividing 2. Further ∞_i $(i=1, 2)$ denote two infinite places of F.

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

For an integral ideal $\mathfrak{a}$ of M, if M is imaginary (resp. real), then $P_M(\mathfrak{a})$ denotes the subgroup of $H_M(\mathfrak{a})$ 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 $\mathfrak{a}$ divides $\mathfrak{f}(K/M)$. Then we denote by $K(\mathfrak{a})$ the kernel of the canonical homomorphism: $P_M \rightarrow P_M(\mathfrak{a})$. Moreover we put $C_M(\ \ )^*=P_M \cap C_M(\ \ )$. In the following, we shall obtain $C_M(K)$ and $C_M(K')$ under the assumption $p\equiv 7 \bmod 8$.

Case 1. $M=k\ (=\mathbf{Q}(\sqrt{-p}))$.

By the assumption, we have $2=\mathfrak{p}_2\bar{\mathfrak{p}}_2$ in k, where $\bar{\mathfrak{p}}_2$ denotes the conjugate of $\mathfrak{p}_2$. Take the two elements μ and ν of $\mathfrak{O}_k$ such that

$$\begin{cases}\mu\equiv 5 \bmod \mathfrak{p}_2^4 ; \\ \mu\equiv 1 \bmod \bar{\mathfrak{p}}_2^4 ,\end{cases} \qquad \begin{cases}\nu\equiv -1 \bmod \mathfrak{p}_2^4 , \\ \nu\equiv 1 \bmod \bar{\mathfrak{p}}_2^4 .\end{cases}$$

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

$$P_k=\langle[\mu],[\bar{\mu}],[\nu]\rangle , \qquad K((4))=\langle[\mu],[\bar{\mu}]\rangle ,$$
$$K((8))=\langle[\mu]^2,[\bar{\mu}]^2\rangle .$$

By the above table, we see that

$$\begin{aligned}[P_k : C_k(L)^*]&=[C_k(L)^* : C_k(K')^*]\\ &=[C_k(K')^* : C_k(K)^*]=2 .\end{aligned}$$

Furthermore,

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

Hence

$$\begin{aligned}&C_k(L)^*=K((4))=\langle[\mu],[\bar{\mu}]\rangle ,\\ &C_k(K')^*=\langle[\mu]^2,[\bar{\mu}]^2,[\mu][\bar{\mu}]\rangle ,\\ &C_k(K)^*\not\ni[\mu]^2,[\bar{\mu}]^2 .\end{aligned}$$

Since $G(K/\mathbf{Q})$ 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

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

We put

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

where S denotes the index set of integral ideals $\mathfrak{b}$. Then

$$\begin{aligned}&C_k(K')=C_k(K)+C_k(K)[\mu]^2 ,\\ &C_k(K)=\sum_{\mathfrak{b}\in S}[\mathfrak{b}]^{-4}C_k(K)^* .\end{aligned}$$

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

$$[\mathfrak{a}]\in C_k(K)\Leftrightarrow y\equiv 0 \bmod 16\,.$$

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

$$\Theta(\tau;\,K)=\sum_{\mathfrak{b}\in S}\ \sum_{4x+1+4y\sqrt{-p}\in\mathfrak{b}^4}(-1)^y\cdot q^{\{(4x+1)^2+16py^2\}/N_{k/\mathbf{Q}}(\mathfrak{b})^4}\,. \tag{5}$$

Case 2. $M=F\,(=\mathbf{Q}(\sqrt{2}))$.

Let α be an element of $\mathfrak{O}_F$. Then there exists an element α^* of $\mathfrak{O}_F$ such that

$$\begin{cases}\alpha^* \quad \text{is totally positive}\,,\\ \alpha^*\equiv\alpha \bmod 4\sqrt{2}\,,\\ \alpha^*\equiv 1 \bmod p\,.\end{cases}$$

Let $p=\mathfrak{p}\bar{\mathfrak{p}}$ in F, and $r(\mathfrak{p})$ denote a generator of the multiplicative group $(\mathfrak{O}_F/\mathfrak{p})^\times$. Take a totally positive element λ of $\mathfrak{O}_F$ such that

$$\begin{cases}\lambda\equiv 1 \bmod 4\sqrt{2}\,,\\ \lambda\equiv r(\mathfrak{p}) \bmod \mathfrak{p}\,,\\ \lambda\equiv 1 \bmod \bar{\mathfrak{p}}\,.\end{cases}$$

Then

$$H_F=P_F=\langle[\varepsilon_2^*],\,[3^*],\,[5^*],\,[\lambda],\,[\bar{\lambda}]\rangle\,;$$

and

$$[\varepsilon_2^*]^4=[3^*]^2=[5^*]^2=[\lambda]^{p-1}=1\,,$$
$$[\sqrt{\varepsilon_2^*}]=[3^*][5^*][\varepsilon_2^*]^3\,.$$

Furthermore,

$$\begin{cases}K_F(\mathfrak{p})=\langle[\varepsilon_2^*],\,[3^*],\,[5^*],\,[\bar{\lambda}]\rangle\,,\\ K_F((p))=\langle[\varepsilon_2^*],\,[3^*],\,[5^*]\rangle\,,\\ K_F((2p))=\langle[3^*],\,[5^*],\,[\varepsilon_2^*]^2\rangle\,,\\ K_F((4p))=\langle[5^*]\rangle\,.\end{cases}$$

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

$$\begin{aligned}[P_F:C_F(L')]&=[C_F(L'):C_F(K')]\\ &=[C_F(K'):C_F(K)]=2\,;\end{aligned}$$

$$C_F(L')\supset K_F((p)),\ \not\supset K_F(\mathfrak{p})\,,$$
$$C_F(K')\supset K_F((2p)),\ \not\supset K_F((p))\,,$$
$$C_F(K)\not\supset K_F((4p))\,.$$

Hence we obtain

$$C_F(L')=\langle[\varepsilon_2^*], [3^*], [5^*], [\lambda]\cdot[\bar{\lambda}], [\lambda]^2\rangle .$$

Since the Galois group $G(K'/\mathbf{Q})$ is isomorphic to $P_F/C_F(K')$, we have

$$C_F(K')\ni[\lambda]^2, [\bar{\lambda}]^2, [\lambda]^{-1}[\bar{\lambda}] .$$

Hence

$$C_F(K')=\langle[\varepsilon_2^*]^2, [3^*], [5^*], [\lambda]^2, [\bar{\lambda}]^2, [\lambda][\bar{\lambda}]\rangle .$$

Next we shall calculate $C_F(K)$. First we notice that

$$\begin{cases} C_F(K)\ni[\lambda]^2, [\bar{\lambda}]^2, [\varepsilon_2^*]^2 , \\ C_F(K)\not\ni[5^*] . \end{cases}$$

Take a prime q such that $q\equiv 3 \bmod 8$ and $(q/p)=-1$. Then q remains prime in F and $[q]=[3^*]([\lambda][\bar{\lambda}])^a$ (a : 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.,

$$C_F(K)\ni[3^*]([\lambda][\bar{\lambda}]) .$$

Similarly, $[5^*]([\lambda][\bar{\lambda}])\in C_F(K)$. Therefore we obtain

$$C_F(K)=\langle[\varepsilon_2^*]^2, [\lambda]^2, [\bar{\lambda}]^2, [3^*][\lambda][\bar{\lambda}], [5^*][\lambda][\bar{\lambda}]\rangle ,$$

$$C_F(K')=C_F(K)+C_F(K)[5^*] .$$

Let r be a rational integer with $r^2\equiv 2 \bmod p$ and $\mu=x+y\sqrt{2}$ be a totally positive element of $\mathfrak{O}_F$ such that $(2p, \mu)=1$. Then we have

$$[\mu]\in C_F(K')\Leftrightarrow x\text{: odd, } y\text{: even, } ((x^2-2y^2)/p)=1 .$$

Further

$$[\mu]\in C_F(K)\Leftrightarrow(\operatorname{sgn}x)((ry-x)/p)(2/x)=1 .$$

We put

$$\begin{cases} E^+=\{\varepsilon\in\mathfrak{O}_F^\times \mid \varepsilon\text{: totally positive}\} , \\ E^0=\{\varepsilon\in E^+ \mid \varepsilon-1\in\mathfrak{f}(K/F)\} , \end{cases}$$

and $e=[E^+ : E^0]$. Then, the right hand side of (2) has the following expression for $M=F$.

$$\Theta(\tau; K)=e^{-1}\sum_{\substack{\mu=x+2y\sqrt{2} \\ x\equiv 1 \bmod 4 \\ N_{F/\mathbf{Q}}(\mu)>0 \\ \mu \bmod E^0}}(\operatorname{sgn}x)((2ry-x)/p)(2/x)q^{x^2-8y^2} . \tag{6}$$

Case 3. $M=E\ (=\mathbf{Q}(\sqrt{-2p}))$.

By a similar calculation of Case 2, we have the following:

(7) $$\Theta(\tau;K)=\sum_{\mathfrak{a}}\sum_{\overline{4x+1+2y\sqrt{-2p}\in\mathfrak{a}}}(-1)^{x+y}\cdot q^{\{(4x+1)^2+8py^2\}/N_{E/\mathbf{Q}}(\mathfrak{a})},$$

where $\{\mathfrak{a}\}$ 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 $p\equiv 7 \bmod 8$. Then, the notation and the assumption being kept as above, we have the three expressions of $\Theta(\tau;K)$*:

$$\begin{aligned}\Theta(\tau;K)&=\sum_{\mathfrak{a}}\sum_{\overline{4x+1+2y\sqrt{-2p}\in\mathfrak{a}}}(-1)^{x+y}\cdot q^{\{(4x+1)^2+8py^2\}/N_{E/\mathbf{Q}}(\mathfrak{a})} &&\text{(via } E)\\ &=\sum_{\mathfrak{b}}\sum_{\overline{4x+1+4y\sqrt{-p}\in\mathfrak{b}^4}}(-1)^{y}\cdot q^{\{(4x+1)^2+16py^2\}/N_{k/\mathbf{Q}}(\mathfrak{b})^4} &&\text{(via } k)\\ &=e^{-1}\sum_{\substack{\mu=x+2y\sqrt{2}\\ x\equiv 1 \bmod 4\\ N_{F/\mathbf{Q}}(\mu)>0\\ \mu \bmod E^0}}(\mathrm{sgn}x)((2ry-x)/p)(2/x)q^{x^2-8y^2}. &&\text{(via } F)\end{aligned}$$

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

$$\begin{aligned}&l=\{(4a+1)^2+8pb^2\}/N_{E/\mathbf{Q}}(\mathfrak{a}),\\ &l=\{(4\alpha+1)^2+16p\beta^2\}/N_{k/\mathbf{Q}}(\mathfrak{b})^4,\\ &l=x^2-8y^2, \qquad x\equiv 1 \bmod 4, \qquad ((x^2-8y^2)/p)=1;\\ a(l)&=\pm 2.\end{aligned}$$

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

$$\begin{aligned}(\varepsilon_p/l)_4=1 &\Leftrightarrow a+b\text{: even}\\ &\Leftrightarrow \beta\text{: even}\\ &\Leftrightarrow (\mathrm{sgn}x)((2ry-x)/p)(2/x)=1\\ &\Leftrightarrow a(l)=2.\end{aligned}$$

For prime p with $p\equiv 3 \bmod 8$, we shall only state the result as a remark.

Remark 1. Let $p\equiv 3 \bmod 8$ and $p\neq 3$. Then, the following may be obtained in a way similar to the proof of the above theorem.

$$\begin{aligned}
\Theta(\tau; K) &= \sum_{\substack{x,\, y \in \mathbf{Z} \\ x \equiv 1 \bmod 4}} (-1)^{(x-1)/4}((x-2ry)/p)q^{x^2+8y^2} \\
&= \sum_{\mathfrak{b}} \left\{ \sum_{\substack{\nu=(\alpha+\beta\sqrt{-p})/2 \in \mathfrak{b}^4 \\ N_{k/\mathbf{Q}}(\nu) \equiv 1 \bmod 8 \\ \alpha \equiv 1 \bmod 4}} (-1)^{(\alpha-1)/4+(N_{k/\mathbf{Q}}(\nu)-1)/8} \cdot q^{(\alpha^2+p\beta^2)/4N_{k/\mathbf{Q}}(\mathfrak{b})^4} \right. \\
&\qquad \left. + \sum_{4x+1+4y\sqrt{-p} \in \mathfrak{b}^4} (-1)^y \cdot q^{\{(4x+1)^2+16py^2\}/N_{k/\mathbf{Q}}(\mathfrak{b})^4} \right\} \\
&= e^{-1} \sum_{\mathfrak{a}} \sum_{\substack{\mu=4x+1+2y\sqrt{2p} \in \mathfrak{a} \\ N_{F/\mathbf{Q}}(\mu) > 0 \\ \mu \bmod E^0}} (\operatorname{sgn} x)(-1)^{x+y} \cdot q^{\{(4x+1)^2+8py^2\}/N_{F/\mathbf{Q}}(\mathfrak{a})} .
\end{aligned}$$

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

References

[1] Halter-Koch, F., Kaplan, P. and Williams, K. S.; An Artin character and representations of primes by binary quadratic forms II, *Manuscripta Math.*, **35** (1982), 357–381.

[2] Hiramatsu, T.; Higher reciprocity law and modular forms of weight one, *Comment Math. Univ. St. Pauli*, **31** (1982), 75–85.

[3] Hiramatsu, T., Ishii, N. and Mimura, Y.; On indefinite modular forms of weight one, preprint.

[4] Ishii, N.; Cusp forms of weight one, quartic reciprocity and elliptic curves, to appear in Nagoya Math. J.

[5] Leonard, P. A. and Williams, K. S.; The quadratic and quartic character of certain quadratic units II, *Rocky Mountain J. Math.* (4), **9** (1979), 683–692.

Department of Mathematics
Kobe University
Rokko, Kobe 657
Japan

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