TOKYO J. MATH.
VOL. 9, No. 1, 1986

# On the Quartic Residue Symbol of Totally Positive Quadratic Units

Noburo ISHII

*University of Osaka Prefecture*
(Communicated by Y. Kawada)

## Introduction

Let $m$ be a square free positive integer and $\varepsilon_m$ the fundamental unit of the quadratic field $\boldsymbol{Q}(\sqrt{m})$. If $\varepsilon_m$ is totally positive, then we define the biquadratic symbol $(\varepsilon_m/p)_4$ for the rational prime number $p$ with the condition,

$$(*) \qquad (-1/p)=(m/p)=(\varepsilon_m/p)=1 .$$

We refer to [3] for the definitions of the symbols $(\varepsilon_m/p)$ and $(\varepsilon_m/p)_4$. Let $K$ (resp. $K'$) be the Galois extension over the rational number field $\boldsymbol{Q}$ generated by $\sqrt{-1}$ and $\sqrt[4]{\varepsilon_m}$ (resp. $\sqrt{-1}$ and $\sqrt{\varepsilon_m}$). Then the condition $(*)$ is equivalent to say that $p$ splits completely in $K'$. Further the symbol $(\varepsilon_m/p)_4$ expresses the decompition law of this prime $p$ between $K$ and $K'$. Let $T_m$ be the trace of $\varepsilon_m$ over $\boldsymbol{Q}$ and denote by $f_m$ (resp. $e_m$) the square free part of $T_m+2$ (resp. $m(T_m+2)$). Consider the following three quadratic fields;

$$(1) \qquad F=\boldsymbol{Q}(\sqrt{f_m}) , \qquad E=\boldsymbol{Q}(\sqrt{-e_m}) , \qquad k=\boldsymbol{Q}(\sqrt{-m}) .$$

Then $K$ contains all these quadratic fields and is abelian over each of them. If the ideal class groups corresponding to $K$ and $K'$ in each field of (1) are determined explicitly, then we obtain three sorts of expressions of $(\varepsilon_m/p)_4$ in view of the representation of a power of $p$ by the norm form of each quadratic field. In the present paper, we offer explicit expressions of this symbol for the integers $m$ of following types:

$$(2) \qquad \begin{aligned} &m=qq': \quad q\equiv 5, 3 \bmod 8 , \quad q'\equiv 3 \bmod 4 , \quad (q/q')=-1 ; \\ &m=2q: \quad q\equiv 3 \bmod 8 ; \\ &m=q: \quad q\equiv 3, 7, 11 \bmod 16 . \quad (q, q': \text{prime numbers.}) \end{aligned}$$

Received October 24, 1984

This restriction imposed on $m$ assures us that the narrow class number of each field in (1) is not divided by 8. The case $m$ is prime is treated, in our previous paper [2], in a different point of view. Therefore we shall state only the results for this case. Finally it is remarked that the results for the values of the symbol $(\varepsilon_m/p)_4$ in [1] and [3] correspond to ours obtained from the field $k$.

## § 1. Preliminaries.

Let $m$ be any positive square free integer and let the notation be as above. If $p$ is a prime number such that $(-1/p)=(m/p)=1$, then it is easy to see

$$(\varepsilon_m/p)=1 \Longleftrightarrow p \text{ splits completely in } K' .$$

Let $\mathfrak{p}$ be a prime ideal of $K'$ lying over $p$. Then

$$(\varepsilon_m/p)_4=\begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits in } K , \\ -1 & \text{if } \mathfrak{p} \text{ remains prime in } K . \end{cases}$$

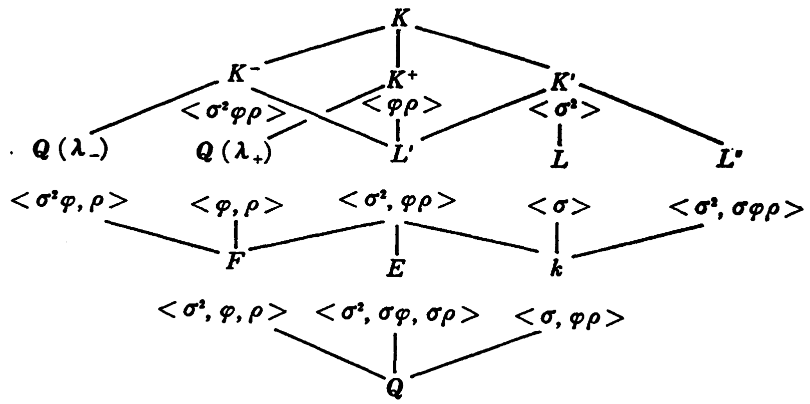
Let $G=G(K/\boldsymbol{Q})$ be the Galois group of $K$ over $\boldsymbol{Q}$. Then $G$ is of order 16 and is generated by three elements $\sigma$, $\varphi$ and $\rho$ defined by

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

Let $\lambda_\pm=\sqrt[4]{\varepsilon_m}\pm\sqrt[4]{\varepsilon_m}^{-1}$ and put

$$K^+=\boldsymbol{Q}(\sqrt{-e_m}, \lambda_+) , \qquad K^-=\boldsymbol{Q}(\sqrt{-e_m}, \lambda_-) ,$$
$$L=\boldsymbol{Q}(\sqrt{-1}, \sqrt{-m}) , \qquad L'=\boldsymbol{Q}(\sqrt{-m}, \sqrt{f_m}) , \qquad L''=\boldsymbol{Q}(\sqrt{-m}, \sqrt{e_m}) .$$

Then we have the following diagram:



From this diagram we obtain

(3) *a prime number $p$ splits completely in $K'$*

$$\Longleftrightarrow (-1/p)=(m/p)=(f_m/p)=1 .$$

In particular this shows, for a prime $p$ such that $(-1/p)=(m/p)=1$,

$$(\varepsilon_m/p)=(f_m/p) .$$

Further we have:

LEMMA 1. *Let $p$ be an odd prime divisor of $m$ and $P$ the prime ideal of $k$ over $p$. Assume that $P$ splits in $L'$. Then we obtain*

$$P \textit{ splits completely in } K' \Longleftrightarrow p\equiv 1 \bmod 4 ;$$

$$P \textit{ splits completely in } K^+ \Longleftrightarrow p\,|\,e_m \textit{ or } (2/p)=1 ;$$

$$P \textit{ splits completely in } K^- \Longleftrightarrow \begin{cases}(-2/p)=1 & \textit{if} \quad p\,|\,f_m ,\\ (-1/p)=1 & \textit{if} \quad p\,|\,e_m .\end{cases}$$

*Furthermore*

$$P \textit{ splits completely in } K \Longleftrightarrow \begin{cases}p\equiv 1 \bmod 8 & \textit{if} \quad p\,|\,f_m ,\\ p\equiv 1 \bmod 4 & \textit{if} \quad p\,|\,e_m .\end{cases}$$

PROOF. It is easy to see that

$$P \text{ splits in } L' \Longleftrightarrow (f_m/p)=1 \text{ or } (-e_m/p)=1 .$$

Therefore

$$P \text{ splits completely in } K' \Longleftrightarrow P \text{ splits in each of } L,\ L' \text{ and } L''$$

$$\Longleftrightarrow (f_m/p)=(-f_m/p)=1 \text{ or } (e_m/p)=(-e_m/p)=1 \Longleftrightarrow p\equiv 1 \bmod 4 .$$

Let $P=P_1P_2$ be the prime ideal decomposition of $P$ in $L'$. We can take a defining equation $f^+(x)$ (resp. $f^-(x)$) of $K^+$ (resp. $K^-$) over $L'$ as

$$f^{\pm}(x)=x^2-\lambda_{\pm}^2=x^2-(u_m\sqrt{f_m}\pm 2) ,$$

where $u_m$ is the positive integer such that $u_m^2 f_m=T_m+2$. Let $p\,|\,f_m$. Then

$$f^{\pm}(x)\equiv x^2\mp 2 \mod P_i .$$

This shows

$$P \text{ splits completely in } K^+ \text{ (resp. } K^-) \Longleftrightarrow (2/p)=1 \text{ (resp. } (-2/p)=1) .$$

Let $p\,|\,e_m$. Then we know only one of $P_1$ and $P_2$ divides $\lambda_+^2$. Assume that $P_1$ divides $\lambda_+^2$ and $P_2$ divides $\lambda_-^2$. Then

$$f^+(x)=x^2-4-\lambda_-^2\equiv x^2-4 \mod P_2 .$$

Therefore $P$ splits completely in $K^+$. Similarly we obtain

$$P \text{ splits completely in } K^- \Longleftrightarrow (-1/p)=1 .$$

By the way

$$P \text{ splits completely in } K \Longleftrightarrow P \text{ splits completely in } K',\ K^+,\ K^-$$

respectively. Therefore we have our assertions. Q.E.D.

LEMMA 2. *Let $m=qq'$ be the integers given by* (2). *Then the integers $e_m$ and $f_m$ are as follows.*

$$(e_m, f_m)=\begin{cases}(2q', 2q) & \textit{if} \quad q\equiv 5 \mod 8 \quad \textit{and} \quad q'\equiv 3 \mod 8 ,\\ (2q, 2q') & \textit{if} \quad q\equiv 5 \mod 8 \quad \textit{and} \quad q'\equiv 7 \mod 8 ,\\ (q, q') & \textit{if} \quad q\equiv 3 \mod 8 \quad \textit{and} \quad q'\equiv 3 \mod 4 ,\\ (2, q) & \textit{if} \quad q\equiv 3 \mod 8 \quad \textit{and} \quad q'=2 .\end{cases}$$

PROOF. Let $q\equiv 5 \mod 8$, $q'\equiv 3 \mod 4$ and $(q/q')=-1$. Put $\varepsilon_m=A+B\sqrt{m}$. First of all we shall show that $A$ is even. Let $C+D\sqrt{m}$ be the smallest positive unit of $Q(\sqrt{m})$ such that $C$ is odd and $D$ is positive. Since $C^2-D^2m=1$, we can put

$$C-1=2r^2u , \qquad C+1=2s^2v ,$$

where $u$, $v$, $r$ and $s$ are positive integers such that $uv=m$, $2rs=D$ and $(ru, sv)=1$. From this we have

$$1=s^2v-r^2u .$$

Since $(-1/q')=-1$ and $(q/q')=-1$, it follows that $u=m$ and $v=1$. This shows that $s+r\sqrt{m}$ is a positive unit of $Q(\sqrt{m})$ smaller than $C+D\sqrt{m}$. Therefore $s$ is even and $A$ is even. Put

$$A-1=R^2U , \qquad A+1=S^2V ,$$

where $R$, $S$, $U$ and $V$ are positive integers and $UV=m$. Then

$$2=S^2V-R^2U\equiv V-U \mod 8 .$$

From this we have $(U, V)=(q', q)$ (resp. $(q, q')$) if $q'\equiv 3 \mod 8$ (resp. if $q'\equiv 7 \mod 8$). Since $e_m=2U$ and $f_m=2V$ we have our assertion in the case $q\equiv 5 \mod 8$. Other assertions can be similarly proved. Q.E.D.

In the following for an abelian extension $\Omega$ over a field $\Lambda$, we denote by $f(\Omega/\Lambda)$ the finite part of conductor of $\Omega/\Lambda$. Let $\mathscr{K}$, $\mathscr{L}$ and $\mathscr{F}$ be fields such that $\mathscr{K}\supset\mathscr{L}\supset\mathscr{F}$ and $[\mathscr{L}:\mathscr{F}]=2$. Assume that $\mathscr{K}$ is abelian over $\mathscr{F}$. Let $P$ be a prime ideal of $\mathscr{L}$. Denote by $f(P)$ and $g(P)$ the $P$-exponent of $f(\mathscr{K}/\mathscr{L})$ and that of the difference $D(\mathscr{L}/\mathscr{F})$ of $\mathscr{L}$ over $\mathscr{F}$ respectively. We define the integer $e(P)$ by

$$e(P)=\max(0,\ g(P)-f(P)) .$$

Then we know by Lemma 1 of [2]

$$f(\mathscr{K}/\mathscr{F})=f(\mathscr{K}/\mathscr{L})D(\mathscr{L}/\mathscr{F})\prod_P P^{e(P)} . \tag{4}$$

Furthermore assume that $\mathscr{K}$ and $\mathscr{L}$ are normal over $\boldsymbol{Q}$. Then the $P$-exponent $f(P)$ is the same for all prime ideals $P$ of $\mathscr{L}$ dividing a prime number $p$, which we denote by $f(p)$. In particular, if $[\mathscr{K}:\mathscr{L}]=2$, then $f(2)$ is calculated as follows. Let $\alpha$ be an integer of $\mathscr{L}$ such that $\mathscr{K}=\mathscr{L}(\sqrt{\alpha})$. Fix a prime ideal $Q$ of $\mathscr{L}$ dividing 2. Let $\hat{\mathfrak{o}}$ the completion of the ring of integers of $\mathscr{L}$ with respect to $Q$ and $\Pi$ a prime element of $\hat{\mathfrak{o}}$. Put

$$\alpha=\Pi^{\delta}\beta ,$$

where $\beta$ is a unit of $\hat{\mathfrak{o}}$. We denote by $S_Q(\beta)$ the greatest positive integer $t$ such that $\beta\equiv\gamma^2 \bmod \Pi^t$ for some unit $\gamma\in\hat{\mathfrak{o}}$ (cf. § 63A of [4]). We define the integer $S_{\mathscr{L}}(\alpha)$ by

$$S_{\mathscr{L}}(\alpha)=\begin{cases} S_Q(\beta) & \text{if } \delta \text{ is even ,} \\ 0 & \text{otherwise .}\end{cases}$$

It is obvious that $S_{\mathscr{L}}(\alpha)$ is determined only by $\alpha$ and is independent of the choice of $Q$ and $\Pi$. Let $e_{\mathscr{L}}$ denote the ramification exponent of $Q$. Then we have by Lemma 4 of [2] and Lemma 2 of [1],

$$f(2)=\begin{cases} 2e_{\mathscr{L}}+1-S_{\mathscr{L}}(\alpha) & \text{if } S_{\mathscr{L}}(\alpha)<2e_{\mathscr{L}} , \\ 0 & \text{otherwise .}\end{cases} \tag{5}$$

Let $M$ be one of the fields (1). By (4) and (5), we can get the conductors $f(K/M)$, $f(K'/M)$ and $f(L'/M)$ from calculating $S_L(\varepsilon_m)$ and $S_{K'}(\sqrt{\varepsilon_m})$. (cf. § 3 of [2].) If $m$ are integers in (2), then the values of $S_L(\varepsilon_m)$ and $S_{K'}(\sqrt{\varepsilon_m})$ are as follows.

| $m=qq'$ | $q\equiv 5 \bmod 8$ $q'\equiv 3 \bmod 4$ | $q\equiv 3 \bmod 8$ $q'\equiv 3 \bmod 4$ | $q\equiv 3 \bmod 8$ $q'=2$ |
|---|---|---|---|
| $e_L$ | 2 | 2 | 4 |
| $S_L(\varepsilon_m)$ | 1 | $\geq 4$ | 8 |
| $e_{K'}$ | 4 | 2 | 4 |
| $S_{K'}(\sqrt{\varepsilon_m})$ | 1 | 1 | 3 |

## § 2. Criterions.

Let the notation be as in the previous sections. Furthermore we shall use the following notation. Let $M$ be one of the quadratic fields $k$, $F$ and $E$. Let $\mathfrak{a}$ be an integral ideal of $M$. 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 $M$ and $P_M(\mathfrak{a})$ denotes the subgroup of $H_M(\mathfrak{a})$ generated by principal classes (resp. principal classes represented by totally positive elements). We denote by $h(M)$ the class number (resp. narrow class number) of $M$. Hereafter we put $H_M=H_M(f(K/M))$ and $P_M=P_M(f(K/M))$. If $\mathfrak{b}$ is an ideal prime to $f(K/M)$, then $[\mathfrak{b}]$ denotes the class of $H_M$ represented by $\mathfrak{b}$. If $b$ is an element of $M$ and $(b)$ is the principal ideal generated by $b$, then $[(b)]$ is abbreviated as $[b]$. If $\Omega$ is a subfield of $K$ over $M$, then $C_M(\Omega)$ denotes the subgroup of $H_M$ corresponding to $\Omega$. We put $C_M(\Omega)^*=C_M(\Omega)\cap P_M$. If $\mathfrak{c}$ is an integral ideal of $M$ dividing $f(K/M)$, then $K_M(\mathfrak{c})$ denotes the kernel of the canonical homomorphism of $P_M$ to $P_M(\mathfrak{c})$.

Let $m$ be one of integers given by (2) and $p$ a prime number such that $(-1/p)=(f_m/p)=(e_m/p)=1$. Now we shall evaluate the character $(\varepsilon_m/p)_4$. Because the way of our discussion is very similar for each case of $m$, we shall give the details only for the case $m=qq'$, $q\equiv 5 \bmod 8$, $q'\equiv 7 \bmod 8$ and $(q'/q)=-1$.

(I) *The criterion by* $k=\boldsymbol{Q}(\sqrt{-m})$.

LEMMA 3. *Let* $\omega=(1+\sqrt{-m})/2$ *and let* $\nu$ *be an integer of* $k$ *prime to* 2. *If* $\nu\equiv 1 \bmod 2$, *then we can put* $\nu=x+y\omega$; $x, y\in \boldsymbol{Z}$ *and we have*

$$[\nu]\in C_k(K') \Longleftrightarrow x\colon odd\ ,\quad y\equiv 0 \bmod 8\ ;$$
$$[\nu]\in C_k(K) \Longleftrightarrow x\colon odd\ ,\quad y\equiv 0 \bmod 16\ .$$

*If* $\nu\not\equiv 1 \bmod 2$, *then we can put* $\nu=(X+Y\sqrt{-m})/2$, *where* $X$ *and* $Y$ *are integers. Assume* $X\equiv 1 \bmod 4$, *if necessarily, replacing* $\nu$ *by* $-\nu$. *Then*

$$[\nu]\in C_k(K') \Longleftrightarrow N(\nu)\equiv 1 \mod 8\ ;$$
$$[\nu]\in C_k(K) \Longleftrightarrow (N(\nu)-1)/8+(X-1)/4\equiv 0 \mod 2\ ,$$

*where $N(\nu)$ denotes the norm of $\nu$ over $\boldsymbol{Q}$.*

PROOF. By the argument in the last part of § 1, we know that $f(K/k)=16$, $f(K'/k)=8$ and $f(L/k)=4$. From this we see

$$[P_k: C_k(L)^*]=[C_k(L)^*: C_k(K')^*]=[C_k(K')^*: C_k(K)^*]=2\ ,$$
$$C_k(L)^*\supset K_k((4))\ ,\quad C_k(K')^*\supset K_k((8))\ ,\quad C_k(K)^*\not\supset K_k((8))\ .$$

Let $\zeta$ be an integer such that $\zeta^3\equiv 1 \mod 16$. Then

$$P_k=\langle[1+4\omega],\ [1+2\omega],\ [\zeta]\rangle\ ,\qquad K_k((4))=\langle[1+4\omega],\ [1+2\omega]^2\rangle\ ,$$
$$K_k((8))=\langle[1+4\omega]^2,\ [1+2\omega]^4\rangle\ .$$

Therefore

$$C_k(L)^*=\langle[\zeta]\rangle\times K_k((4))\ ,$$
$$C_k(K')^*=\langle[\zeta],\ [1+4\omega]^2,\ [1+2\omega]^2\rangle\ .$$

Since the factor group $P_k/C_k(K)^*$ is of exponent 4 and $G(K/\boldsymbol{Q})$ is non-abel, we have

$$C_k(K)^*=\langle[\zeta],\ [1+2\omega]^2\cdot[1+4\omega]^2\rangle\ .$$

Let $\nu\equiv 1 \mod 2$. Then

$$[\nu]\in C_k(K') \Longleftrightarrow [\nu]\in\langle[1+8\omega],\ [5+8\omega]\rangle \Longleftrightarrow x\text{: odd}\ ,\quad y\equiv 0 \mod 8\ ;$$
$$[\nu]\in C_k(K) \Longleftrightarrow [\nu]\in\langle[5]\rangle \Longleftrightarrow x\text{: odd}\ ,\quad y\equiv 0 \mod 16\ .$$

Let $\nu\not\equiv 1 \mod 2$. Choose $a=1$ or $2$ such that $\nu\zeta^a=u+v\omega\equiv 1 \mod 2$. Since $N(\zeta)\equiv 1 \mod 16$,

$$N(\nu)\equiv u^2+v(u+vN(\omega)) \mod 16\ .$$

Therefore we know that

$$[\nu]\in C_k(K') \Longleftrightarrow v\equiv 0 \mod 8 \Longleftrightarrow N(\nu)\equiv 1 \mod 8\ .$$

Let $v\equiv 0 \mod 8$. Then noting $X^2\equiv u^2 \mod 16$ we have

$$N(\nu)-1\equiv X^2-1+v \mod 16\ .$$

Thus

$$v/8\equiv (N(\nu)-1)/8+(X^2-1)/8\equiv (N(\nu)-1)/8+(X-1)/4 \mod 2.$$

Hence for $[\nu] \in C_k(K')$,

$$[\nu] \in C_k(K) \Longleftrightarrow (N(\nu)-1)/8+(X-1)/4 \equiv 0 \mod 2\,. \qquad \text{Q.E.D.}$$

Since $h(k) \equiv 2 \mod 4$, we can put $h(k)=2h$, where $h$ is an odd number. Let $p$ be a prime number such that $p$ splits in $k$ and $P$ one of the prime ideals of $k$ lying above $p$. By (3) we have

$$(-1/p)=(2q/p)=(2q'/p)=1 \Longleftrightarrow [P] \in C_k(K')\,.$$

Assume that $[P] \in C_k(K')$, Let $Q$ be the prime ideal of $k$ lying above $q$. Let $r$ be any odd multiple of $h$. Then we have

$$[P]^r \in C_k(K')^* \quad \text{or} \quad [P]^r[Q] \in C_k(K')^*\,.$$

If $[P]^r \in C_k(K')^*$, then by Lemma 3 we can put $P^r=(\eta)$, where

$$\eta=\begin{cases} x+4y\sqrt{-m} & \text{if} \quad \eta \equiv 1 \mod 2\,, \\ (X+Y\sqrt{-m})/2\,, \quad X \equiv 1 \mod 4 & \text{otherwise}\,. \end{cases}$$

Further

$$\begin{aligned} [P] \in C_k(K) &\Longleftrightarrow [\eta] \in C_k(K) \\ &\Longleftrightarrow \begin{cases} y \equiv 0 \mod 2 & \text{if} \quad \eta \equiv 1 \mod 2\,, \\ (p-1)/8+(X-1)/4 \equiv 0 \mod 2 & \text{otherwise}\,. \end{cases} \end{aligned}$$

If $[P]^r \cdot [Q] \in C_k(K')^*$, then we can put $P^r=Q^{-1}(\eta)$, where

$$\eta=\begin{cases} qu+4v\sqrt{-m} & \text{if} \quad \eta \equiv 1 \mod 2\,, \\ (qU+V\sqrt{-m})/2\,, \quad U \equiv 1 \mod 4 & \text{otherwise}\,. \end{cases}$$

By Lemmas 1 and 3 we obtain

$$\begin{aligned} [P] \in C_k(K) &\Longleftrightarrow [\eta] \in C_k(K) \\ &\Longleftrightarrow \begin{cases} v \equiv 0 \mod 2 & \text{if} \quad \eta \equiv 1 \mod 2\,, \\ (qp-1)/8+(U-1)/4+(r+1)/2 \equiv 0 \mod 2 & \text{otherwise}\,. \end{cases} \end{aligned}$$

Therefore we have the following statements:

(6) *If $p$ is a prime such that $(-1/p)=(2q/p)=(2q'/p)=1$, then $p^r$ can be written in one of the following forms;*

$$x^2+16my^2\,, \qquad (X^2+mY^2)/4\,,$$
$$qu^2+16q'v^2\,, \qquad (qU^2+q'V^2)/4\,,$$

*where $x$, $y$, $X$, $Y$, $u$, $v$, $U$ and $V$ are all integers and $X \equiv U \equiv 1 \mod 4$.*

*Further we have*

$$(\varepsilon_m/p)_4=\begin{cases}(-1)^y & \text{if } p^r=x^2+16my^2\ ,\\ (-1)^{(p-1)/8+(X-1)/4} & \text{if } p^r=(X^2+mY^2)/4\ ,\\ (-1)^v & \text{if } p^r=qu^2+16q'v^2\ ,\\ (-1)^{(qp-1)/8+(U-1)/4+(r+1)/2} & \text{if } p^r=(qU^2+q'V^2)/4\ .\end{cases}$$

(II) *The criterions by* $F=\boldsymbol{Q}(\sqrt{2q'})$ *and* $E=\boldsymbol{Q}(\sqrt{-2q})$.

LEMMA 4. *Put* $\omega=\sqrt{2q'}$. *Let* $\mu=x+y\omega$ *be a totally positive integer of* $F$ *prime to* $2q$. *Then*

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

*Further*

$$[\mu]\in C_F(K) \Longleftrightarrow (-2/x)(-1)^{y/2}(x+sy/q)=1\ ,$$

*where* $s\in\boldsymbol{Z}$ *such that* $s^2\equiv-2q' \bmod q$.

PROOF. Let $\alpha$, $\beta$, $\gamma$ and $\lambda$ be totally positive integers of $F$ satisfying the following properties:

$$\begin{cases}\alpha\equiv1+\omega & \bmod 4p_2\ ,\\ \alpha\equiv1 & \bmod q\ ;\end{cases}\qquad \begin{cases}\beta\equiv1+2\omega & \bmod 4p_2\ ,\\ \beta\equiv1 & \bmod q\ ;\end{cases}$$

$$\begin{cases}\gamma\equiv3 & \bmod 4p_2\ ,\\ \gamma\equiv1 & \bmod q\ ;\end{cases}\qquad \begin{cases}\lambda\equiv1 & \bmod 4p_2\ ,\\ \lambda\equiv r(Q) & \bmod Q\ ,\\ \lambda\equiv1 & \bmod \bar{Q}\ ,\end{cases}$$

where $Q$ is a prime ideal of $F$ lying above $q$, $r(Q)$ is a primitive root mod $Q$ and $\bar{Q}$ denotes the conjugate of $Q$. We see that

$$\begin{aligned}P_F&=\langle[\alpha],[\beta],[\gamma],[\lambda],[\bar\lambda]\rangle\ ,\\ K_F((q))&=\langle[\alpha],[\beta],[\gamma]\rangle\ ,\\ K_F((2q))&=\langle[\beta],[\gamma],[\alpha]^2\rangle\ ,\\ K_F((4q))&=\langle[\beta][\alpha]^2\rangle\ ,\end{aligned}$$

where $\bar\lambda$ denotes the conjugate of $\lambda$. By the values of conductors $f(k/F)=4p_2q$, $f(k'/F)=2q$, $f(L'/F)=q$, we know

$$\begin{aligned}C_F(L')^*&=\langle[\alpha],[\beta],[\gamma],[\lambda]^2,[\bar\lambda]^2,[\lambda][\bar\lambda]\rangle\ ,\\ C_F(K')^*&=\langle[\alpha]^2,[\beta],[\gamma],[\lambda]^2,[\bar\lambda]^2,[\lambda][\bar\lambda]\rangle\ ,\\ C_F(K)^*&\supset\langle[\beta][\lambda][\bar\lambda],[\lambda]^2,[\bar\lambda]^2,[\alpha]^2\rangle\ .\end{aligned}$$

Let $\ell$ be a prime number such that $\ell \equiv 3 \bmod 8$ and $(2q'/\ell)=-1$. Then $[\ell]=[\gamma]([\lambda][\bar{\lambda}]) \bmod C_F(K)$ and $\ell$ remains prime in $k$. By Lemma 3 we know that $\ell$ splits completely between $K$ and $k$. Therefore

$$[\ell] \in C_F(K)^* .$$

Thus

$$C_F(K)^* = \langle [\alpha]^2, [\beta][\lambda][\bar{\lambda}], [\gamma][\lambda][\bar{\lambda}], [\lambda]^2, [\bar{\lambda}]^2 \rangle .$$

From this we easily deduce our statements. Q.E.D.

LEMMA 5. *Let $Q'$ be the prime ideal of $F$ lying over $q'$. Let $\alpha$ and $\beta$ be the elements appeared in the proof of Lemma 4. Then*

$$[Q'][\alpha][\beta] \in C_F(K) .$$

PROOF. By Lemma 1, the Frobenius substitution associated with the class $[Q']$ is $\varphi\rho$. Consider an element $\mu$ of $\boldsymbol{Q}(\lambda_+)$ such that

$$\mu = a + q(\omega + \lambda_+) ,$$

where $a$ is a rational integer with properties:

$$(a, 2q)=1 , \quad a > 4qq'u_m .$$

Let $\nu$ be the norm of $\mu$ over $F$. Then $\nu$ is totally posivive and

$$[\nu] \equiv [\alpha][\beta] \quad \bmod C_F(K) .$$

Since $[\nu] \in C_F(L')$ and $K^+$ is the composite field of $L'$ and $\boldsymbol{Q}(\lambda_+)$, we know that $\varphi\rho$ is also the Frobenius substitution associated with the class $[\nu]$. Therefore we obtain $[Q'][\alpha][\beta] \in C_F(K)$. Q.E.D.

Since $h(F) \equiv 2 \bmod 4$, we can put $h(F)=2h'$, where $h'$ is odd. Let $p$ be a prime number such that $(-1/p)=(2q/p)=(2q'/p)=1$ and $P$ one of the prime ideal of $F$ lying above $p$. Let $\ell$ be any odd multiple of $h'$. Then we have by Lemma 6,

$$[P]^\ell \in C_F(K')^* \quad \text{or} \quad [P]^\ell \in [Q'][\alpha][\beta]C_F(K')^* .$$

By the similar argument in (I) and by Lemmas 4 and 5, we have

(7) *$p^\ell$ can be written in one of the forms:*

$$p^\ell = a^2 - 8q'b^2 , \quad a>0 \quad or \quad p^\ell = q'A^2 - 2B^2 , \quad A>0 .$$

*Further*

$$(\varepsilon_m/p)_4=\begin{cases}(a+2sb/q)(2/a)(-1)^b & if \quad p^e=a^2-8q'b^2\ ,\\ -(q'A+sB/q)(2/A) & if \quad p^e=q'A^2-2B^2\ .\end{cases}$$

The criterion by $E$ is similarly obtained (see next Theorem). Consequently we obtain

THEOREM. *Let $m$ be a product of two distinct primes $q$ and $q'$ such that $q\equiv 5 \bmod 8$, $q'\equiv 7 \bmod 8$ and $(q'/q)=-1$. Denote by $H$ the product of odd parts of class numbers $h(k)$, $h(F)$ and $h(E)$. Let $p$ be a prime number such that $(-1/p)=(2q/p)=(2q'/p)=1$. Then we obtain the following table which offers representations of $p^H$ and evaluation of $(\varepsilon_m/p)_4$ according to each of them.*

| | representations of $p^H$ | evaluation of $(\varepsilon_m/p)_4$ | |
|---|---|---|---|
| $p\equiv 1$ mod 8 | $x^2+16my^2$<br>$\frac{1}{4}(X^2+mY^2)$, $X\equiv 1 \bmod 4$ | $(-1)^y$<br>$(-1)^{(p-1)/8+(X-1)/4}$ | $k$ |
| | $a^2-8q'b^2$, $a>0$ | $(a+2sb/q)(2/a)(-1)^b$ | $F$ |
| | $\alpha^2+8q\beta^2$ | $(\alpha+2t\beta/q')(-2/\alpha)(-1)^\beta$ | $E$ |
| $p\equiv 5$ mod 8 | $qu^2+16q'v^2$<br>$\frac{1}{4}(qU^2+q'V^2)$, $U\equiv 1 \bmod 4$ | $(-1)^v$<br>$(-1)^{(qp-1)/8+(U-1)/4+(H+1)/2}$ | $k$ |
| | $q'A^2-2B^2$, $A>0$ | $-(q'A+sB/q)(2/A)$ | $F$ |
| | $q\gamma^2+8\delta^2$ | $-(q\gamma+2t\delta/q')(-2/\gamma)(-1)^\delta$ | $E$ |

Here $s$ and $t$ are integers such that $s^2\equiv 2q' \bmod q$ and $t^2\equiv -2q \bmod q'$.

NUMERICAL EXAMPLE. Let $q=5$ and $q'=7$. Then $\varepsilon_{35}=6+\sqrt{35}$ and $H=1$.

(i) Take $p=13$. Then $\varepsilon_{35}\equiv 9 \bmod 13$ and $(\varepsilon_{35}/p)_4=1$. We can put $s=t=2$ and we see

$$U=-3\ ,\quad V=1\ ;\quad A=3\ ,\quad B=5\ ;\quad \gamma=1\ ,\quad \delta=1\ .$$

(ii) Take $p=281$. Then $\varepsilon_{35}\equiv 69 \bmod 281$ and $(\varepsilon_{35}/p)_4=-1$. Let $s=t=2$. We have

$$X=33\ ,\quad Y=1\ ;\quad a=41\ ,\quad b=5\ ;\quad \alpha=11\ ,\quad \beta=2\ .$$

For the integers $m$ of other type in (2), we shall only state the results. Let $H$ be the product of odd parts of narrow class numbers of $k$, $F$ and $E$. Let $p$ be a prime number such that $(-1/p)=(e_m/p)=(f_m/p)=1$. Then we have the following tables.

(T-1) $m=qq'$; $q\equiv 5 \bmod 8$, $q'\equiv 3 \bmod 8$, $(q'/q)=-1$. ($e_m=2q'$, $f_m=2q$.)

| | representations of $p^H$ | evaluation of $(\varepsilon_m/p)_4$ | |
|---|---|---|---|
| $p\equiv 1$ mod 8 | $x^2+16my^2$ | $(-1)^y$ | $k$ |
| | $a^2-8qb^2$, $a>0$ | $(a+2sb/q')(2/a)(-1)^b$ | $F$ |
| | $\alpha^2+8q'\beta^2$ | $(\alpha+2t\beta/q)(2/\alpha)(-1)^\beta$ | $E$ |
| $p\equiv 5$ mod 8 | $qX^2+16q'Y^2$ | $(-1)^{Y+1}$ | $k$ |
| | $qA^2-8B^2$, $A>0$ | $(qA+2sB/q')(2/A)(-1)^B$ | $F$ |
| | $q'\gamma^2+2\delta^2$ | $-(q'\gamma+t\delta/q)(2/\gamma)$ | $E$ |

Here $s$ and $t$ are integers such that $s^2\equiv 2q \bmod q'$ and $t^2\equiv -2q' \bmod q$.

(T-2) $m=qq'$; $q\equiv 3 \bmod 8$, $q'\equiv 3 \bmod 4$, $(q/q')=-1$. ($e_m=q$, $f_m=q'$.)

| representations of $p^H$ | evaluation of $(\varepsilon_m/p)_4$ | |
|---|---|---|
| $x^2+4my^2$<br>$4X^2+mY^2$ | $(-1)^y$<br>$(-2/q')(-1)^{X+1}$ | $k$ |
| $a^2-4q'b^2$, $a>0$ | $(-1)^b(a+2sb/q)$ | $F$ |
| $\alpha^2+4q\beta^2$<br>$\frac{1}{4}(\gamma^2+q\delta^2)$, $\delta$: odd $\gamma\equiv\delta \bmod 4$ | $(\alpha+2t\beta/q')(-1)^{(\alpha-1)/2}$<br>$(2(\gamma+t\delta)/q')(-1)^{(p-1)/4+(\gamma+1)/2}$ | $E$ |

Here $s, t\in \boldsymbol{Z}$ such that $s^2\equiv q' \bmod q$ and $t^2\equiv -q \bmod q'$.

(T-3) $m=2q$; $q\equiv 3 \bmod 8$. ($e_m=2$, $f_m=q$.)

| representations of $p^H$ | evaluation of $(\varepsilon_m/p)_4$ | |
|---|---|---|
| $x^2+8qy^2$ | $(-1)^y$ | $k$ |
| $(4a+1)^2-16qb^2$<br>$a>0$ | $(-1)^{a-b}$ | $F$ |
| $\alpha^2+8\beta^2$ | $(-1)^\beta(\alpha+2t\beta/q)$ | $E$ |

Here $t\in \boldsymbol{Z}$ such that $t^2\equiv -2 \bmod q$.

(T-4) $m=q$; $q\equiv 3, 11 \bmod 16$. ($e_m=2$, $f_m=2q$.)

| representations of $p^H$ | evaluation of $(\varepsilon_m/p)_4$ | |
|---|---|---|
| $x^2+16qy^2$<br>$\frac{1}{4}(X^2+qY^2)$, $X\equiv 1 \bmod 4$ | $(-1)^y$<br>$(-1)^{(X-1)/4+(p-1)/8}$ | $k$ |
| $a^2-8qb^2$, $a\equiv 1 \bmod 4$ | $(\operatorname{sgn} a)(-1)^{b+(a-1)/4}$ | $F$ |
| $\alpha^2+8\beta^2$, $\alpha\equiv 1 \bmod 4$ | $(-1)^{\beta+(\alpha-1)/4}(\alpha-2r\beta/q)$ | $E$ |

Here $r\in \boldsymbol{Z}$ such that $r^2\equiv -2 \bmod q$.

(T-5) $m=q$; $q\equiv 7 \bmod 16$. ($e_m=2q$, $f_m=2$.)

| representations of $p^H$ | evaluation of $(\varepsilon_m/p)_4$ | |
|---|---|---|
| $x^2+16qy^2$ | $(-1)^y$ | $k$ |
| $a^2-8b^2$, $a\equiv 1 \bmod 4$ | $(\operatorname{sgn} a)(2rb+a/q)(2/a)(-1)^b$ | $F$ |
| $\alpha^2+8q\beta^2$, $\alpha\equiv 1 \bmod 4$<br>$q\gamma^2+2\delta^2$, $\gamma\equiv 3 \bmod 4$ | $(-1)^{\beta+(\alpha-1)/4}$<br>$(-1)^{(\gamma+1)/4}$ | $E$ |

Here $r\in \boldsymbol{Z}$ such that $r^2\equiv 2 \bmod q$.

REMARK. It is known in [2] that there exists a cusp form of weight one whose $p$-th Fourier coefficient equals to $(\varepsilon_m/p)_4$ for every prime number $p$ such that $(-1/p)=(m/p)=(f_m/p)=1$.

## References


[1] F. HALTER-KOCH, P. KAPLAN and K. S. WILLIAMS, An Artin character and representations of primes by binary quadratic forms II, Manuscripta Math., **37** (1982), 357–381.

[2] T. HIRAMATSU and N. ISHII, Quartic residuacity and cusp forms of weight one, Comment Math. Univ. St. Paul., **34** (1985), 91–103.

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

[4] O. T. O'MERA, Introduction to Quadratic Forms, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.



*Present Address*:
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF OSAKA PREFECTURE
MOZU-UMEMACHI, SAKAI 591