Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 261–275

Quadratic Units and Congruences between Hilbert Modular Forms

Noburo Ishii

Introduction

Let F be a real quadratic field which has the totally positive fundamental unit. We put $F=\boldsymbol{Q}(\sqrt{m})$ with a positive square free integer m. We denote by $[1, \sqrt{m}]$ the order of F generated by 1 and $\sqrt{m}$ over the ring of integers $\boldsymbol{Z}$. Let ε_m be the smallest unit of F such that $\varepsilon_m>1$ and $\varepsilon_m \in [1, \sqrt{m}]$. We denote by K the number field generated by $\sqrt{-1}$ and $\sqrt[4]{\varepsilon_m}$ over the rational number field $\boldsymbol{Q}$ and by E the elliptic curve over F defined by the Weierstrass equation;

$$y^2=x^3+4\varepsilon_m x.$$

We can attach to K (resp. to E) Hilbert modular forms over F of weight one (resp. of weight two) in a natural way.

The aim of the present paper is to show that the "quartic residuacity" of ε_m provides congruences between these Hilbert modular forms. Further we calculate their Fourier coefficients and express the decomposition law between K and F by them.

§ 1. Hilbert modular forms

Let the notation be as in introduction. Denote by G the galois group of the normal extension K of $\boldsymbol{Q}$. Then G is of order 16 and is generated by the following three isomorphisms σ, φ and ρ:

$$\begin{aligned} &\sigma(\sqrt[4]{\varepsilon_m})=\sqrt{-1}\,\sqrt[4]{\varepsilon_m}, && \sigma(\sqrt{-1})=\sqrt{-1}\,; \\ &\varphi(\sqrt[4]{\varepsilon_m})=1/\sqrt[4]{\varepsilon_m}, && \varphi(\sqrt{-1})=\sqrt{-1}\,; \\ &\rho(\sqrt[4]{\varepsilon_m})=\sqrt[4]{\varepsilon_m}, && \rho(\sqrt{-1})=-\sqrt{-1}. \end{aligned}$$

It is easy to see that they satisfy the relation;

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

Received June, 9, 1986.

Now we shall explain how to attach to K Hilbert modular forms. For a subfield M of K, we denote by $G(M)$ the Galois group of K over M. Set $k=\boldsymbol{Q}(\sqrt{-m})$. Then we see

$$G(F)=\langle\sigma, \rho\rangle, \qquad G(k)=\langle\sigma, \varphi\rho\rangle.$$

Therefore $G(F)$ is isomorphic to the dihedral group D_4 of order 8 and $G(k)$ is an abelian group. Let μ be the representation of $G(F)$ corresponding to the unique two-dimensional irreducible complex representation of D_4. From now on we assume that

$$\mu(\sigma)=\begin{pmatrix}\sqrt{-1} & 0 \\ 0 & -\sqrt{-1}\end{pmatrix}, \qquad \mu(\rho)=\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}.$$

The induced representation of μ to G decomposes into two distinct irreducible representations ψ_0 and ψ_1 of dimension 2. Let χ_F be the linear representation of G whose kernel coincides with $G(F)$. Then

$$\psi_1=\psi_0\otimes\chi_F. \tag{1}$$

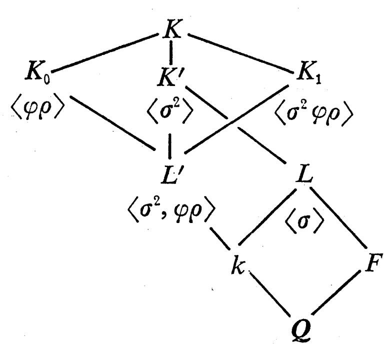
Let us assume that

$$\psi_0(\sigma)=\begin{pmatrix}\sqrt{-1} & 0 \\ 0 & -\sqrt{-1}\end{pmatrix}, \quad \psi_0(\rho)=\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}, \quad \psi_0(\varphi)=\begin{pmatrix}0 & 1 \\ 1 & 0\end{pmatrix}.$$

Since $G(k)$ is abelian, the restriction ψ_i $(i=0, 1)$ to $G(k)$ decomposes into two distinct linear representations ξ_i and ξ_i'. It is easy to see kernel of ξ_i=kernel of ξ_i' for each i. Put

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

Let K_i be the field of invariants of the kernel of ξ_i. Let L' be the intersection of K_0 and K_1. Then the following diagram is obtained.



Let us denote by the same notation ξ_i the ideal character of k induced by the representation ξ_i in view of Artin reciprocity law. Let f_i be the conductor of the abelian extension K_i/k. Then f_i coincides with the conductor of the character ξ_i and is self-conjugate. Further the support of f_i consists of all prime ideals of k lying over 2, if f_i is non-trivial. The above diagram shows

(2) *neither* f_0 *nor* f_1 *is trivial* $\Longleftrightarrow$ *K is ramified over L.*

For each i let $L(s, \psi_i)$ and $L(s, \xi_i)$ be the Artin L-function of ψ_i and Hecke L-function of ξ_i respectively. If ξ_i is ramified, then $L(s, \xi_i)$ coincides with the Hecke L-function of the primitive character associated with ξ_i. Therefore under the assumption ξ_i is ramified, we have

(3) $$L(s, \psi_i)=L(s, \xi_i).$$

In the below we assume the following.

Hypothesis. *The field K is ramified over L.*

It is known that $L(s, \xi_i)$ is the Mellin transform of a cusp form $\theta_i(z)$ of the modular group of $\Gamma_0(|D(k/\boldsymbol{Q})|N_{k/\boldsymbol{Q}}(f_i))$ of weight one (of neben type), where $D(k/\boldsymbol{Q})$ denotes the discriminant of k over $\boldsymbol{Q}$. If we denote by χ the ideal character of k determined by the extension L over k, then by (1) we have $\xi_0=\chi\xi_1$. Therefore in view of an analogy of *Doi-Naganuma correspondence* [2], we put

$$L(s, K)=L(s, \xi_0)L(s, \xi_1).$$

It is easily seen that

$$L(s, K)=L(s, \xi_0\cdot N_{L/k}).$$

Therefore we write

$$L(s, K)=\prod_{\mathfrak{p}} L_{\mathfrak{p}}(s, K),$$

where the product is taken over all prime ideals of F not lying over 2 and

$$L_{\mathfrak{p}}(s, K)=\prod_{\substack{\mathfrak{P}\mid\mathfrak{p}\\ \mathfrak{P}:\text{ prime ideal of } L}} (1-\xi_0 N_{L/k}(\mathfrak{P})N_{L/\boldsymbol{Q}}(\mathfrak{P})^{-s})^{-1}.$$

Let us write

(4) $$L(s, K)=\sum_{\mathfrak{m}} a(\mathfrak{m})N_{F/\boldsymbol{Q}}(\mathfrak{m})^{-s},$$

where the sum is taken over all integral ideals of F. Let h be the narrow class number of F and let $\mathfrak{a}_j$ ($j=1, 2, \cdots, h$) be the integral ideals of F representing all narrow classes of F. We define h functions $g_j(z, z')$ on the direct product of two complex upper half planes $\mathfrak{H}$ by

$$(5) \qquad g_j(z, z') = \sum_{\substack{\xi \in \mathfrak{a}_j \\ \xi \gg 0}} a(\xi \mathfrak{a}_j^{-1}) \exp(2\pi\sqrt{-1}(\xi z + \xi^{\varphi} z')),$$

where $\xi \gg 0$ means that ξ is totally positive. Since $L(s, K)$ is a L-function associated with the character $\xi_0 N_{L/k}$ of the totally imaginary quadratic extension L of F, $g_j(z, z')$ are Hilbert modular forms of weight one (cf. Sections 2 and 5 of [10]). Let E be the elliptic curve defined over F by the equation:

$$y^2 = x^3 + 4\varepsilon_m x.$$

If we denote by $c(m)$ the conductor of E, then $c(m)$ is always nontrivial and the support of $c(m)$ consists of all prime ideals of F lying over 2 (see Section 3 of this note). Denote by $L(s, E)$ the L-function of E over F. For a prime ideal $\mathfrak{p}$ of F prime to 2, let $E_{\mathfrak{p}}$ the reduction of E defined over the residue field $F_{\mathfrak{p}}$. Let $N(\mathfrak{p})$ be the number of $F_{\mathfrak{p}}$-rational points on $E_{\mathfrak{p}}$ and put

$$b(\mathfrak{p}) = N_{F/Q}(\mathfrak{p}) + 1 - N(\mathfrak{p}),$$
$$L_{\mathfrak{p}}(s, E) = (1 - b(\mathfrak{p}) N_{F/Q}(\mathfrak{p})^{-s} + N_{F/Q}(\mathfrak{p})^{1-2s})^{-1}.$$

Then $L(s, E)$ has the following Euler product expansion:

$$L(s, E) = \prod_{(\mathfrak{p}, 2)=1} L_{\mathfrak{p}}(s, E).$$

Let us write

$$(6) \qquad L(s, E) = \sum b(\mathfrak{m}) N_{F/Q}(\mathfrak{m})^{-s},$$

where $\mathfrak{m}$ runs over all integral ideals of F. We shall define h functions f_j ($j=1, \cdots, h$) on $\mathfrak{H} \times \mathfrak{H}$ by

$$(7) \qquad f_j(z, z') = \sum_{\substack{\xi \in \mathfrak{a}_j \\ \xi \gg 0}} b(\xi \mathfrak{a}_j^{-1}) \exp(2\pi\sqrt{-1}(\xi z + \xi^{\varphi} z')).$$

Since E has complex multiplications, E determines a Grössen character ψ of L and $L(s, E)$ coincides with the L-function of the ideal character ψ^* of L associated with ψ ([1], [9]). If we denote by c^* the conductor of ψ^*, we see easily, by Section 1 of [9],

$$\psi^*((x)) = x \cdot x^{\varphi} \qquad \text{for } x \in L,\ x \equiv 1 \bmod^{\times} c^*.$$

This shows $f_j(z, z')$ are Hilbert modular forms of weight 2. Further we know that c^* is associated with $c(m)$ in the following relation.

Lemma 1.

$$c(m)=N_{L/F}(c^*)D(L/F).$$

Proof. Let $\tilde{c}$ be the conductor of E over L. Then Theorem 12 of [8] shows $c^{*2}=\tilde{c}$. Further by Corollary of Theorem 4 of [8] and Proposition 4 of Section 2, VI of [7], we see

$$\tilde{c}\cdot D(L/F)=c(m).$$

Thus we have

$$N_{L/F}(c^*)^2 D(L/F)^2=c(m)^2. \qquad \text{Q.E.D.}$$

Let $f^*(m)$ be the conductor of K over L. Put

$$f(m)=N_{L/F}(f^*(m))D(L/F).$$

Under the notation in Section 2 of [10], we may state our results for g_j and f_j more precisely. Thus using Lemma 1 we have

Proposition 1. *Let η_1 (resp. η_2) be the Hecke character of the idele group of F such that the associated ideal character η_1^* (resp. η_2^*) is given by*

$$\eta_1^*=\chi_{L/F}\circ\xi_0^2 \ (\textit{resp. } \eta_2^*=\chi_{L/F}\circ\psi^*\circ N_{F/Q}^{-1}),$$

where $\chi_{L/F}$ denotes the ideal character of F attached to the extension L. Then, under the notation in [10], *we obtain*

$$(g_1, \cdots, g_h)\in\mathfrak{M}_{(1,1)}(f(m), \eta_1),$$
$$(f_1, \cdots, f_h)\in\mathfrak{M}_{(2,2)}(c(m), \eta_2).$$

Proof. See [10].

§ 2. Congruences

In this section we show a congruence between Hilbert modular forms $g_j(z, z')$ and $f_j(z, z')$. The way of argument is similar to that of our proof [4] for the congruence between cusp forms by quartic residue of rational integers. We preserve the notation and the hypothesis in Section 1. Let p be an odd prime number and $\mathfrak{p}$ a prime ideal of F lying over p. For an integer α of F prime to $\mathfrak{p}$, we define the symbol $(\alpha/\mathfrak{p})$ by

$$(\alpha/\mathfrak{p})=\begin{cases} 1 & \text{if } \alpha \text{ is square modulo } \mathfrak{p}, \\ -1 & \text{otherwise.} \end{cases}$$

Let J be the automorphism of the reduction $E_{\mathfrak{p}}$ defined by

$$J\colon (x, y) \longmapsto (-x, Iy), \tag{8}$$

for any point (x, y) on $E_{\mathfrak{p}}$. Here the letter I denotes an element of algebraic closure of $F_{\mathfrak{p}}$ such that $I^2=-1$. For a positive integer i we denote by R_i the set of $F_{\mathfrak{p}}$-rational $(1+J)^i$-division points on $E_{\mathfrak{p}}$. Easy calculation shows

$$\begin{cases} R_2=\{(x, 0)\,|\,x^3+4\bar{\varepsilon}_m x=0,\ x \in F_{\mathfrak{p}}\} \cup \{\bar{0}\}, \\ R_3\backslash R_2=\{(x, y)\,|\,x^2-4\bar{\varepsilon}_m=0,\ y^2=x^3+4\bar{\varepsilon}_m x,\ x, y \in F_{\mathfrak{p}}\}, \end{cases} \tag{9}$$

where $\bar{\varepsilon}_m$ denotes the residue class of ε_m mod $\mathfrak{p}$, $\bar{0}$ denotes the identity element of the group structure on $E_{\mathfrak{p}}$ and $R_3\backslash R_2$ means the set of elements of R_3 not belonging to R_2. Denote by $S(\mathfrak{p})$ the set of $F_{\mathfrak{p}}$-rational solutions of the equation $x^4-\bar{\varepsilon}_m=0$. Then we have

Lemma 2.

$$N(\mathfrak{p})=|S(\mathfrak{p})|+3+(-\varepsilon_m/\mathfrak{p})+\omega(\mathfrak{p}) \bmod 8,$$

where

$$\omega(\mathfrak{p})=\begin{cases} 4 & \textit{if } p\equiv 7 \bmod 8 \textit{ and } (-1/\mathfrak{p})=-1, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. We define a mapping φ of $S(\mathfrak{p})$ to $R_3\backslash R_2$ by

$$\varphi\colon x \in S(\mathfrak{p}) \longmapsto (2x^2, 4x^3).$$

It is easy to see φ is a bijection. Therefore we obtain by (9)

$$|R_3|=|S(\mathfrak{p})|+3+(-\varepsilon_m/\mathfrak{p}). \tag{10}$$

To prove our assertion it is sufficient to show the congruence:

$$N(\mathfrak{p})\equiv|R_3|+\omega(\mathfrak{p}) \bmod 8. \tag{11}$$

Assume $(-1/\mathfrak{p})=-1$. Then we see $p\equiv 3 \bmod 4$ and $N_{F/Q}(\mathfrak{p})=p$. Therefore we have, by (10),

$$N(\mathfrak{p})=p+1, \qquad |R_3|=4.$$

This shows (11). Let $(-1/\mathfrak{p})=1$. Then the automorphism J is $F_{\mathfrak{p}}$-rational.

Denote by R the group of $F_{\mathfrak{p}}$-rational points on $E_{\mathfrak{p}}$ and by R_+ the 2-primary subgroup of R. Let R_- be the subgroup of R consisting of all elements of odd order. Then R has a following direct decomposition;

$$R = R_+ \oplus R_- .$$

Since J is $F_{\mathfrak{p}}$-rational, J operates on R_+ and R_- respectively. Let U be the cyclic group of order 4 generated by J. For any $x \in R$ we denote by $U(x)$ the U-orbit of x. We see easily

$$\text{(12)} \qquad |U(x)| = \begin{cases} 1 & \text{if } x \in R_1, \\ 2 & \text{if } x \in R_2 \backslash R_1, \\ 4 & \text{otherwise.} \end{cases}$$

This shows especially

$$R_3 \backslash R_2 \text{ is non-empty} \Rightarrow |R_3| = 8.$$

Therefore we obtain

$$|R_+| \equiv |R_3| \bmod 8.$$

Since $|R_3|$ is even and $|R_-| \equiv 1 \bmod 4$ (by (12)), we see

$$N(\mathfrak{p}) = |R_+| \cdot |R_-| \equiv |R_3| \bmod 8.$$

This establishes (11). Q.E.D.

Proposition 2. *Let the notation be as above. Then we have the following congruence;*

$$b(\mathfrak{p}) \equiv a(\mathfrak{p}) + \gamma(\mathfrak{p}) \bmod 8,$$

where

$$\gamma(\mathfrak{p}) = \begin{cases} 4 & \text{if } p \equiv 5 \bmod 8 \text{ and } p \text{ is not inert in } F, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\sigma_{\mathfrak{p}}$ be a Frobenius substitution of $\mathfrak{p}$ in the extension K/F and ν the character of μ. Let δ be the character of $G(F)$ induced by the identity character of $G(F(\sqrt[4]{\varepsilon_m}))$. Then it is known that

$$|S(\mathfrak{p})| = \delta(\sigma_{\mathfrak{p}}).$$

Since $a(\mathfrak{p}) = \nu(\sigma_{\mathfrak{p}})$, by decomposing δ to the sum of irreducible characters of $G(F)$, we have

(13) $$|S(\mathfrak{p})|=1+(\varepsilon_m/\mathfrak{p})+\nu(\sigma_\mathfrak{p})=1+(\varepsilon_m/\mathfrak{p})+a(\mathfrak{p}).$$

By the definition of $b(\mathfrak{p})$, Lemma 2 and (13), we obtain

$$b(\mathfrak{p})\equiv N_{F/Q}(\mathfrak{p})-(\varepsilon_m/\mathfrak{p})-(-\varepsilon_m/\mathfrak{p})+\omega(\mathfrak{p})-a(\mathfrak{p})-3 \bmod 8.$$

From the regular character of $G(F)$ we deduce the congruence:

$$1+2a(\mathfrak{p})+(-1/\mathfrak{p})+(-\varepsilon_m/\mathfrak{p})+(\varepsilon_m/\mathfrak{p})\equiv 0 \bmod 8.$$

Therefore we have

$$b(\mathfrak{p})\equiv a(\mathfrak{p})+(-1/\mathfrak{p})+N_{F/Q}(\mathfrak{p})+\omega(\mathfrak{p})-2 \bmod 8.$$

By the way, easy argument shows

$$(-1/\mathfrak{p})+N_{F/Q}(\mathfrak{p})+\omega(\mathfrak{p})-2\equiv\gamma(\mathfrak{p}) \bmod 8.$$

Use the following facts:

If $(-1/\mathfrak{p})=-1$, then $N_{F/Q}(\mathfrak{p})=p$ and $p\equiv 3 \bmod 4$.
If $(-1/\mathfrak{p})=1$ and p is not inert in F, then $p\equiv 1 \bmod 4$. Q.E.D.

Corollary. *For any integral ideal* $\mathfrak{m}$ *of* F *prime to* 2, *we have*

$$a(\mathfrak{m})\equiv b(\mathfrak{m}) \bmod 4.$$

Proof. By the definition, we may write

$$L_\mathfrak{p}(s, K)=\{1-a(\mathfrak{p})N_{F/Q}(\mathfrak{p})^{-s}+\chi_{L/F}(\mathfrak{p})N_{F/Q}(\mathfrak{p})^{-2s}\}^{-1}.$$

Comparing $L_\mathfrak{p}(s, K)$ with $L_\mathfrak{p}(s, E)$, we have only to prove the congruence:

$$\chi_{L/F}(\mathfrak{p})\equiv N_{F/Q}(\mathfrak{p}) \bmod 4.$$

But this is easily obtained. Q.E.D.

This Corollary shows

Theorem 1. *Let the notation and hypothesis be as above. Then for every* j, *we obtain*

$$g_j(z, z')\equiv f_j(z, z') \bmod 4.$$

§ 3. Conductors

In this section we calculate the conductor $c(m)$ of the elliptic curve E (=level of Hilbert modular forms $f_j(z, z')$) and level $f(m)$ of Hilbert modular forms $g_j(z, z')$. Further we determine the condition of ε_m to satisfy our hypothesis. Put

$$\varepsilon_m = A + B\sqrt{m}, \quad \text{with} \quad A, B \in Z.$$

Then it is easy to see that A and B satisfy the following congruences.

$$\begin{cases} A \equiv \pm 1 \bmod 8,\ B \equiv 0 \bmod 4 & \text{if } m \equiv 1 \bmod 4, \\ A \equiv \pm 1 \bmod 8,\ B \equiv 0 \bmod 4 \text{ or } A \equiv 2 \bmod 4,\ B\text{: odd} & \text{if } m \equiv 3 \bmod 4, \\ A \equiv \pm 1 \bmod 4,\ B\text{: even} & \text{if } m \equiv 2 \bmod 4. \end{cases}$$

By the algorithm of Tate [11], the conductors $c(m)$ is given in the following Proposition.

Proposition 3. *Let* $m \equiv 1 \bmod 4$. *Then*

$$c(m) = \begin{cases} 2^5 & \textit{if } A \equiv 1 \bmod 8, \\ 2^6 & \textit{otherwise.} \end{cases}$$

Let $m \equiv 3 \bmod 4$. *Then*

$$c(m) = \begin{cases} 2^3 & \textit{if } A \equiv 1 \bmod 8, \\ 2^4 & \textit{if } A \equiv -1 \bmod 8, \\ 2^6 & \textit{if } A \equiv 2 \bmod 4. \end{cases}$$

Let $m \equiv 2 \bmod 4$. *Then*

$$c(m) = \begin{cases} 2^4 & \textit{if } B \equiv 2 \bmod 4, \\ \mathfrak{q}^5 & \textit{otherwise,} \end{cases}$$

where $\mathfrak{q}$ *is the prime ideal of* F *lying over* 2.

Next we determine the condition that K is ramified over L in the following Proposition.

Proposition 4.

$$K \textit{ is unramified over } L \Leftrightarrow \begin{cases} A \equiv 1 \bmod 8,\ B \equiv 0 \bmod 8 & \textit{if } m \equiv 1 \bmod 4, \\ A \equiv 1 \bmod 8,\ B \equiv 0 \bmod 4 & \textit{if } m \equiv 3 \bmod 4, \\ B \equiv 0 \bmod 4 & \textit{if } m \equiv 2 \bmod 4. \end{cases}$$

Proof. By (2) we see

$$\xi_0 \text{ or } \xi_1 \text{ is unramified} \Leftrightarrow K \text{ is unramified over } L$$
$$\Rightarrow L' \text{ is unramified over } k.$$

Let us write

$$A+1=2^{\varepsilon}f_0u^2, \qquad A-1=2^{\varepsilon}e_0v^2.$$

Here f_0, e_0, u, v are positive integers such that f_0 and e_0 are square free and $(f_0u, e_0v)=1$. Further

$$\varepsilon=\begin{cases}0 & \text{if } A \text{ is even,}\\ 1 & \text{otherwise.}\end{cases}$$

Put $f=2^{-\varepsilon+1}f_0$ and $e=2^{-\varepsilon+1}e_0$. Then we know $L'=\boldsymbol{Q}(\sqrt{f}, \sqrt{-e})$ (see [2]). Therefore it follows

$$L' \text{ is unramified over } k \Leftrightarrow 2 \text{ is unramified at } \boldsymbol{Q}(\sqrt{f}) \text{ or at}$$
$$\boldsymbol{Q}(\sqrt{-e}) \Leftrightarrow A \equiv \pm 1 \bmod 8,\ B \equiv 0 \bmod 4.$$

Now we shall recall the definition of "*quadratic defect*". Let $\mathfrak{F}$ be a number field which is normal over $\boldsymbol{Q}$ and $\mathfrak{P}$ a prime ideal of $\mathfrak{F}$ lying over 2. We denote by $e_{\mathfrak{F}}$ the ramification exponent of $\mathfrak{P}$. Let $\hat{o}$ be the completion of the ring of integers of $\mathfrak{F}$ at $\mathfrak{P}$ and take a prime element π of $\hat{o}$. For an integer α of F prime to 2, we denote by $S_{\mathfrak{P}}(\alpha)$ the maximal positive integer t such that α is congruent to a square of an element of $\hat{o}$ mod π^t. The ideal $\mathfrak{P}^{S_{\mathfrak{P}}(\alpha)}$ is called the quadratic defect of α at $\mathfrak{P}$. Assume that the field $\mathfrak{F}(\sqrt{\alpha})$ is normal over $\boldsymbol{Q}$. Then the integer $S_{\mathfrak{P}}(\alpha)$ is independent of the choice of $\mathfrak{P}$ and π. Therefore we can put $S_{\mathfrak{P}}(\alpha)=S_{\mathfrak{F}}(\alpha)$. By Section 63:3 of [6], we see

$$\text{every prime ideal of } \mathfrak{F} \text{ lying over 2 is ramified at } \mathfrak{F}(\sqrt{\alpha})$$
$$\Leftrightarrow S_{\mathfrak{F}}(\alpha) < 2e_{\mathfrak{F}}.$$

Hereafter we may assume that $A \equiv \pm 1 \bmod 8$ and $B \equiv 0 \bmod 4$. Let us put $\mathfrak{F}=L$ and $\alpha=\varepsilon_m$ in the above notation. Since $\varepsilon_m \equiv \pm 1 \bmod 4$, we have that $S_L(\varepsilon_m) \geqq 2e_L$. Thus K' is unramified over L. Next let $\mathfrak{F}=K'$ and $\alpha=\sqrt{\varepsilon_m}$. Then $\mathfrak{F}(\sqrt{\alpha})=K$. Since K' is unramified over L, we can choose $\mathfrak{P}$ such that a prime element π of $\hat{o}$ is given by

$$\pi=\begin{cases}1+\sqrt{-1} & \text{if } e_{K'}=2\ (\Leftrightarrow m \equiv 1, 3 \bmod 4),\\ 1-\sqrt{m}/(1+\sqrt{-1}) & \text{if } e_{K'}=4\ (\Leftrightarrow m \equiv 2 \bmod 4).\end{cases}$$

Let $m \equiv 1, 3 \bmod 4$ and $A \equiv -1 \bmod 8$. Since

$$\varepsilon_m \equiv (1-\pi)^2 \bmod 4,$$

we see easily

$$\sqrt{\varepsilon_m} \equiv 1-\pi \bmod \pi^2.$$

This shows that $S_{K'}(\sqrt{\varepsilon_m})=1$ and K is ramified over K'.

Let $m\equiv 1, 3 \bmod 4$ and $A\equiv 1 \bmod 8$. Then we can write

$$\sqrt{\varepsilon_m}=1+\beta\pi^2+\gamma\pi^3, \qquad \sqrt{m}=1+\delta\pi+\eta\pi^2, \tag{14}$$

where β is a unit of $\hat{o}$ or 0, γ, $\eta \in \hat{o}$ and

$$\delta=\begin{cases}0 & \text{if } m\equiv 1 \bmod 4,\\ 1 & \text{otherwise.}\end{cases}$$

Put $b=B/4$. Then we have by (14)

$$\varepsilon_m\equiv 1+(\beta+\beta^2)\pi^4+(\gamma-\beta)\pi^5\equiv 1+b\pi^4\sqrt{m} \bmod \pi^6.$$

Thus

$$\beta+\beta^2+(\gamma-\beta)\pi\equiv b\sqrt{m} \bmod \pi^2.$$

This shows

$$\sqrt{\varepsilon_m}\equiv(1+\beta\pi)^2+b\sqrt{m}\,\pi^2 \bmod \pi^4.$$

If b is even, then $S_{K'}(\sqrt{\varepsilon_m})\geqq 4$. Let b be odd. Then by (14)

$$\sqrt{\varepsilon_m}\equiv(1+(1+\beta)\pi)^2+(1+\delta)\pi^3 \bmod \pi^4.$$

From this it follows

$$S_{K'}(\sqrt{\varepsilon_m})\geqq 4 \Leftrightarrow m\equiv 3 \bmod 4.$$

Therefore we have our assertions for the cases $m\equiv 1, 3 \bmod 4$. Let $m\equiv 2 \bmod 4$. Then we see easily

$$2\equiv\pi^4-\pi^6 \bmod \pi^8, \qquad \sqrt{m}\equiv\pi^2-\pi^3 \bmod \pi^4.$$

Put $\alpha=1$ or $\sqrt{-1}$ according to $A\equiv 1$ or $-1 \bmod 8$. Then it is noted that α is a square mod π^8. Let us write

$$\sqrt{\varepsilon_m}=\alpha+\beta\pi^4+\gamma\pi^5+\delta\pi^6+\eta\pi^7,$$

where β, γ, δ are 0 or units of $\hat{o}$ and $\eta\in\hat{o}$. From this

$$\begin{aligned}\varepsilon_m&\equiv\alpha^2+(\beta^2+\alpha\beta)\pi^8+\alpha\gamma\pi^9+(\gamma^2-\alpha\beta+\alpha\delta)\pi^{10}+(-\alpha\gamma+\alpha\eta)\pi^{11}\\&\equiv\alpha^2+B\sqrt{m} \bmod \pi^{12}.\end{aligned}$$

Put $b=B/4$. Then it follows

$$\beta^2+\alpha\beta+\alpha\gamma\pi+(\gamma^2-\alpha\beta+\alpha\delta)\pi^2+(-\alpha\gamma+\alpha\eta)\pi^3\equiv b\sqrt{m} \bmod \pi^4.$$

Therefore

$$\begin{aligned}\alpha\sqrt{\varepsilon_m}&\equiv(\alpha+\beta\pi^2+\gamma\pi^3)^2+b\sqrt{m}\,\pi^4\\&\equiv(\alpha+\beta\pi^2+(\gamma+b)\pi^3)^2 \bmod \pi^8.\end{aligned}$$

Since α is square mod π^8, $S_{K'}(\sqrt{\varepsilon_m})\geqq 8$. Q.E.D.

Proposition 5. *Let the notation be as in Section* 1. *Then our hypothesis is satisfied with the integers m of the following types*:

$m=p$ (p: *prime*, $p\equiv 3 \bmod 4$),
$m=qq'$ (q, q': *primes*, $q\equiv 3, 5 \bmod 8$, $q'\equiv 3 \bmod 4$, $(q/q')=-1$),
$m=2q$ (q: *prime*, $q\equiv 3 \bmod 8$).

Further for these m the levels $c(m)$ *and* $f(m)$ *of Hilbert modular forms in Proposition* 1 *are given by*

$$c(m)=f(m)=\begin{cases}2^4 & \textit{if } m=2q,\\ 2^6 & \textit{otherwise}.\end{cases}$$

Proof. Let m be one of the integers given as above. Put

$$\varepsilon_m=A+B\sqrt{m}.$$

Then by "infinite decent" of Fermat, we know the followings. If $m\equiv 1 \bmod 4$, then $A\equiv 7 \bmod 8$. If $m\equiv 3 \bmod 4$, then A is even. If $m\equiv 2 \bmod 4$, then $A\equiv 5 \bmod 8$ and $B\equiv 2 \bmod 4$. Hence our first assertions follow from Proposition 4. (For details see [3] and [5].) By the results obtained in [3] and [5], we know

$$f^*(m)=\begin{cases}(8) & \text{if } m\equiv 3 \bmod 4,\\ (4) & \text{if } m\equiv 1 \bmod 4,\\ 2\mathfrak{q}^2 & \text{if } m\equiv 2 \bmod 4,\end{cases}$$

where $\mathfrak{q}$ is the prime ideal of L lying over 2. Since

$$D(L/F)=\begin{cases}(1) & \text{if } m\equiv 3 \bmod 4,\\ (4) & \text{if } m\equiv 1 \bmod 4,\\ (2) & \text{if } m\equiv 2 \bmod 4,\end{cases}$$

the definition of $f(m)$ and Proposition 3 show our last statements. Q.E.D.

§ 4. Fourier coefficients and decomposition law

In this section we discuss the relation between the decomposition in K of the prime ideals $\mathfrak{p}$ of F and the $\mathfrak{p}$-th Fourier coefficients $a(\mathfrak{p})$ and $b(\mathfrak{p})$. Firstly we have the following.

Theorem 2. *Let $\mathfrak{p}$ be a prime ideal of F prime to 2. Then we have the following equivalences:*

$$a(\mathfrak{p})\neq 0 \Leftrightarrow a(\mathfrak{p})=\pm 2 \Leftrightarrow \mathfrak{p} \text{ splits completely in } K',$$
$$a(\mathfrak{p})=2 \Leftrightarrow \mathfrak{p} \text{ splits completely in } K.$$

Proof. By the definition of μ, we know

$$\nu(\sigma_{\mathfrak{p}})=\begin{cases} 2 & \text{if } \sigma_{\mathfrak{p}}=1 \\ -2 & \text{if } \sigma_{\mathfrak{p}}=\sigma^2, \\ 0 & \text{otherwise.}\end{cases}$$

Since $G(K')=\langle\sigma^2\rangle$ and $a(\mathfrak{p})=\nu(\sigma_{\mathfrak{p}})$ we have our assertions. Q.E.D.

Corollary. *Let $\gamma(\mathfrak{p})$ be the symbol defined in Proposition 2. Then*

$$b(\mathfrak{p})\equiv \pm 2 \bmod 8 \Leftrightarrow \mathfrak{p} \text{ splits completely in } K',$$
$$b(\mathfrak{p})\equiv 2+\gamma(\mathfrak{p}) \bmod 8 \Leftrightarrow \mathfrak{p} \text{ splits completely in } K.$$

Proof. This is deduced from Theorem 2 and Proposition 2. Q.E.D.

Let $(\varepsilon_m/\mathfrak{p})_4$ be the fourth power residue symbol of ε_m modulo $\mathfrak{p}$. Then

Proposition 6. *Let $\mathfrak{p}$ be a prime ideal of F such that $a(\mathfrak{p})\neq 0$. Then*

$$a(\mathfrak{p})=2(\varepsilon_m/\mathfrak{p})_4.$$

Proof. By Theorem 2 our assumption $a(\mathfrak{p})\neq 0$ implies $(\varepsilon_m/\mathfrak{p})=1$ and $(-1/\mathfrak{p})=1$. Thus

$$(\varepsilon_m/\mathfrak{p})_4=1 \text{ (resp. } -1) \Leftrightarrow |S(\mathfrak{p})|=4 \text{ (resp. } 0).$$

By (13) we obtain

$$|S(\mathfrak{p})|=2+a(\mathfrak{p}).$$

This shows our assertions. Q.E.D.

Proposition 7. *Let p be an odd prime number which is inert in F and $\mathfrak{p}$ the unique prime ideal of F lying over p. Then $a(\mathfrak{p})\neq 0$. Further denote* *by $T(m)$ the positive square free part of the trace of $1+\varepsilon_m$. Then we have*

$$a(\mathfrak{p})=-2\Leftrightarrow(-1/p)=(T(m)/p)=-1.$$

Proof. The first assertion is deduced from that the group $G(K'/Q)$ is an abelian group of type (2, 2, 2) and from Theorem 2. Denote by C_p the conjugate class of Frobenius substitution of p in G. Then it is easy to see

$$a(\mathfrak{p})=-2\Leftrightarrow C_p=\{\sigma\varphi\rho, \sigma^3\varphi\rho\}\Leftrightarrow p \text{ splits completely in } L^*,$$

where L^* is the field of invariants of the group $\langle\sigma\varphi\rho\rangle$. Since $L^*=Q(\sqrt{-m}, \sqrt{-T(m)})$, we have second assertion. Q.E.D.

In the reminder of this section we consider the case m is a prime number q. We give an explicit expression of $a(\mathfrak{p})$ for the prime p not inert in F.

Theorem 3. *Let p be odd prime number which is not inert in F and $\mathfrak{p}$ a prime ideal of F dividing p. Let h be the class number of k. Then we have*

$a(\mathfrak{p})\neq 0\Leftrightarrow$ *there exists uniquely determined integers*
a and b such that $a\equiv 1 \bmod 4$, $(a, p)=1$, $b>0$ *and*
$p^{3h}=a^2+16qb^2$.

Further in this case we see

$$a(\mathfrak{p})=2(-1)^b.$$

Proof. This is proved by determining the class groups in k corresponding to K and K'. See [3] and [5] for details. Q.E.D.

Furthermore if p is split in F, we have other expression.

Theorem 4. *Let p be an odd prime number which is split in F. Then we have*

$$a(\mathfrak{p})\neq 0\Leftrightarrow p\equiv 1 \bmod 8.$$

In this case p has a following representation in the binary quadratic form:

$$p=\begin{cases} x^2+8y^2 \ (x\equiv 1 \bmod 4, y>0) & \text{if } q\equiv 3 \bmod 8,\\ x^2-8y^2 \ (x>0, y>0) & \text{if } q\equiv 7 \bmod 8,\end{cases}$$

where x and y are uniquely determined integers prime to p. Let r be an *integer such that*

$$r^2 \equiv (-1)^{(1/4)(q+1)} 2 \bmod q.$$

Then we have

$$a(\mathfrak{p}) = 2(-1)^{(p-1)/8} \left(\frac{x+2ry}{q} \right).$$

Proof. Our statement follows from Proposition 6 and from the results in [3] and [5]. Q.E.D.

Remark. Let $\theta_i(z)$ ($i=0, 1$) be the cusp forms of weight one defined in Section 1. Then the decomposition law of the extension $K/\boldsymbol{Q}$ is also expressed in Fourier coefficients of the form $\theta_0(z)+\theta_1(z)$. For details we refer to [3].

The author thanks to Professor J. Evans for pointing out that our results in Theorem 4 can be collected in the above simple form.

References

[1] M. Deuring, Die zetafunktionen einer algebraischen Kurven von geshlechte eins IV, Nachr. Akad. Wiss. Göttingen (1957), 55–80.
[2] K. Doi and H. Naganuma, On the functional equation of certain Dirichlet series, Invent. Math., **9** (1969), 1–14.
[3] T. Hiramatsu and N. Ishii, Quartic residuacity and cusp forms of weight one, Comment Math. Univ. St. Pauli, **34** (1985), 91–103.
[4] N. Ishii, Cusp forms of weight one, quartic reciprocity and elliptic curves, Nagoya Math. J., **98** (1985), 117–137.
[5] ——, On the quartic residue symbol of totally positive quadratic units, Tokyo J. Math., **9** (1986), 53–65.
[6] O. T. O'Mera, Introduction to quadratic forms, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.
[7] J. P. Serre, Corps locaux, Hermann, 1963.
[8] J. P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math., **88** (1968), 492–517.
[9] G. Shimura, On the zeta function of an abelian variety with complex multiplication, Ann. of Math., **94** (1971), 504–533.
[10] ——, The special values of the zeta functions associated with Hilbert modular forms, Duke Math. J., **45** (1978), 637–679.
[11] J. Tate, Algorithm for determining the type of a singular fibre in an elliptic pencil, Lecture notes in Math., **476** (1975), 33–52.

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