Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 413–431

On the Eighth Power Residue of Totally Positive Quadratic Units

Noburo Ishii

§ 0. Introduction

Let p be a prime number which is congruent to 3 modulo 4 and ε_p the totally positive fundamental unit of the real quadratic field $F=\boldsymbol{Q}(\sqrt{p})$. Let q be a prime number which is split in F and is congruent to 1 modulo 2^n. Then we may define 2^n-th power residue symbol $(\varepsilon_p/q)_{2^n}$ of ε_p modulo q as follows. For a prime factor $\mathfrak{Q}$ of q in F, we choose an integer A such that

$$\varepsilon_p \equiv A \qquad \bmod \mathfrak{Q}.$$

The integer A is uniquely determined modulo q. The symbol $(\varepsilon_p/q)_{2^n}$ is defined only when A is a 2^{n-1}-th power residue modulo q and given by

$$(\varepsilon_p/q)_{2^n}=\begin{cases} 1 & \text{if } A \text{ is a } 2^n\text{-th power residue modulo } q, \\ -1 & \text{otherwise.} \end{cases}$$

This definition is independent of the choice of the prime ideal $\mathfrak{Q}$ and the assumption imposed on q implies the following equivalence:

$$(\varepsilon_p/q)_{2^n}=1 \Longleftrightarrow \text{the polynomial } x^{2^n}-A \text{ factors into a product of distinct } 2^n \text{ linear polynomials modulo } q.$$

The symbol $(\varepsilon_p/q)_2$ (resp. $(\varepsilon_p/q)_4$) is usually called the quadratic symbol (resp. biquadratic symbol or quartic symbol) of ε_p modulo q. For the given q, it is comparatively easy to determine the sign of the quadratic symbol. Thus we have

$$(\varepsilon_p/q)_2=1 \Longleftrightarrow q\equiv 1 \bmod 8.$$

The evaluation of the quartic residue symbol $(\varepsilon_p/q)_4$ are studied by many authors ([1], [2], [3], [4], [5], [7]). Here we shall quote one of their results. Let r be any positive odd multiples of the class number of the imaginary

Received July 14, 1986.

quadratic field $k=\boldsymbol{Q}(\sqrt{-p})$ and q a prime number of the properties: $(p/q)=(2/q)=1$. Then a condition on q to be $(\varepsilon_p/q)_4=1$ is given as follows. (cf. [2], [3].)

$$(1)\quad\begin{cases} \textit{If } p\equiv 7 \bmod 8, \textit{ then} \\ (\varepsilon_p/q)_4=1 \Longleftrightarrow \textit{there exists two integers } x \textit{ and } y \textit{ such that} \\ \qquad q^r=x^2+64py^2, \quad x\equiv 1 \bmod 4, \quad (x, q)=1. \\ \textit{If } p\equiv 3 \bmod 8, \textit{ then} \\ (\varepsilon_p/q)_4=1 \Longleftrightarrow \textit{there exists two integers } \xi \textit{ and } \eta \textit{ such that} \\ \qquad q^r=\xi^2+64p\eta^2, \quad \xi\equiv 1 \bmod 4, \quad (\xi, q)=1 \\ \qquad \textit{or there exists two integers } \xi_0 \textit{ and } \eta_0 \textit{ such that} \\ \qquad q^r=(\xi_0^2+p\eta_0^2)/4, \quad \xi_0\equiv 1 \bmod 4, \quad (\xi_0, q)=1. \end{cases}$$

The purpose of this note is to determine when $(\varepsilon_p/q)_8=1$ for the prime q given by the type in the right hand side of (1). We obtain the following results:

Let $p\equiv 7 \bmod 8$. Then under the notation in (1) we have

$$(2)\qquad (\varepsilon_p/q)_8=(-1)^{y+(1/4)(x-1)}.$$

Let $p\equiv 3 \bmod 8$. Put H the class number of the biquadratic field $L=\boldsymbol{Q}(\sqrt{-1}, \sqrt{-p})$. Since H is odd, by (1) for $r=H$, the number q^H is expressed in

$$q^H=\xi^2+64p\eta^2 \quad \text{or} \quad q^H=(\xi_0^2+p\eta_0^2)/4, \quad \xi\equiv\xi_0\equiv 1 \bmod 4, \quad (\xi\xi_0, q)=1.$$

Further we can write

$$q^H=a^2+b^2, \quad a\equiv 1 \bmod 4, \quad (a, q)=1.$$

We have

$$(3)\qquad (\varepsilon_p/q)_8=\begin{cases}(-1)^{\eta+(\xi+a-2)/8} & \textit{if } q^H=\xi^2+64p\eta^2, \\ (-1)^{(\xi_0+a-2)/8} & \textit{if } q^H=(\xi_0^2+p\eta_0^2)/4.\end{cases}$$

We shall explain the way of proof of our results. Consider the fields

$$K_3=\boldsymbol{Q}(\sqrt{-1}, \sqrt[8]{\varepsilon_p})\supset K_2=\boldsymbol{Q}(\sqrt{-1}, \sqrt[4]{\varepsilon_p})\supset K_1=\boldsymbol{Q}(\sqrt{-1}, \sqrt{\varepsilon_p}).$$

For a prime number q such that $q\equiv 1 \bmod 8$ and $(p/q)=1$, we know

$$(\varepsilon_p/q)_4=1 \Longleftrightarrow \textit{the prime } q \textit{ decomposes completely in } K_2$$

(cf. [3]). The 8-th power residue symbol represents the decomposition between K_3 and K_2 of q. If $p\equiv 7 \bmod 8$, then K_3 is an abelian extension over $k=Q(\sqrt{-p})$. By determining the class groups attached to K_3 and K_2 in k, the result (2) is obtained. In the case $p\equiv 3 \bmod 8$, K_3 has no quadratic subfields over which K_3 is abelian. However K_3 is a cyclic extension of degree 8 over L. By adapting the class field theory for K_3/L, the result (3) is obtained. This is the reason why some congruence conditions in the fields $Q(\sqrt{-1})$ and $Q(\sqrt{-p})$ appear at the same time in the formula (3). The results (2) and (3) are given in Theorem 1 of Section 2 and in Theorem 2 of Section 3 respectively. In Section 3, we shall also prove the strengthend form of the conjecture 1 of E. Lehmer in [6]. The author would like to express his hearty thanks to Dr. Y. Mimura for helpful discussions.

§ 1. The Galois group of $Q(\sqrt{-1}, \sqrt[8]{\varepsilon_p})/Q$

Let p and ε_p be as in Section 0. Put $F=Q(\sqrt{p})$ and

$$\eta=\sqrt[8]{\varepsilon_p} \quad \text{and} \quad \zeta=\exp(2\pi\sqrt{-1}/8)=(1+\sqrt{-1})/\sqrt{2}.$$

By Fermat's method, we know there exists an integer $s\gneqq 0$ such that

$$2^{-1}\operatorname{tr}_{F/Q}(\varepsilon_p)=s^2+(-1)^{(1/4)(p-3)}.$$

(cf. p. 97 of [3], Lemma 3 of this note.) Since

$$\eta^8+\eta^{-8}=\operatorname{tr}_{F/Q}(\varepsilon_p),$$

we have the relation

$$s^{-1}(\eta^4+(-1)^{(1/4)(p-7)}\eta^{-4})=\sqrt{2}=\zeta+\zeta^{-1}. \tag{4}$$

Let $K_3=Q(\sqrt{-1}, \eta)$, Then K_3 contains ζ. Therefore K_3 is a Galois extension over Q generated by η and ζ. We denote by G the Galois group $G(K_3/Q)$ of K_3 over Q. We have

Proposition 1. *Let the notation be as above. Then*

(i) *The group G is a group of degree* 32 *generated by the following three elements defined by*

$$\sigma(\eta)=\zeta\eta\ ;\ \sigma(\zeta)=-\zeta,$$
$$\rho(\eta)=\eta\ ;\ \rho(\zeta)=\zeta^7,$$
$$\varphi(\eta)=\eta^{-1};\ \varphi(\zeta)=\zeta^{-p}.$$

Furthermore σ, φ and ρ satisfy the fundamental relations

(5) $$\sigma^8=\rho^2=\varphi^2=1,\ \rho\sigma\rho^{-1}=\sigma^3,\ \varphi\sigma\varphi^{-1}=\sigma^{4+p},\ \varphi\rho=\rho\varphi.$$

(ii) *If* $p\equiv 7$ mod 8, *then* G *contains one and only one commutative subgroup of index* 2. *This subgroup is generated by* σ *and* $\varphi\rho$. *If* $p\equiv 3$ mod 8, *then* G *has no commutative subgroups of index* 2.

Proof. Let $G(F)$ be the Galois group of K_3 over F. If μ is an element of $G(F)$, then μ is determined uniquely by the actions on η and ζ. Let

$$\mu(\eta)=\zeta^m\eta, \qquad \mu(\zeta)=\zeta^n,$$

where m and n are integers such that $0\leqq m,\ n<8$, $(n, 2)=1$. By acting μ on the both sides of (4), we have

$$\zeta^n+\zeta^{-n}=(-1)^m(\zeta+\zeta^{-1}).$$

This shows

$$n=1, 7 \text{ (resp. } 3, 5) \Longleftrightarrow m\text{: even (resp. odd)}.$$

Therefore we define σ and ρ by

$$\sigma(\eta)=\zeta\eta;\ \sigma(\zeta)=\zeta^5=-\zeta,$$
$$\rho(\eta)=\eta\ ;\ \rho(\zeta)=\zeta^7.$$

We see easily

$$\sigma^8=\rho^2=1, \quad \rho\sigma=\sigma^3\rho, \quad G(F)=\langle\rho, \sigma\rangle.$$

Let λ be an element of G not belonging to $G(F)$. Then

$$\lambda(\eta^8)=\lambda(\varepsilon_p)=\varepsilon_p^{-1}=\eta^{-8}.$$

Thus we may put

$$\lambda(\eta)=\zeta^u/\eta, \qquad \lambda(\zeta)=\zeta^v,$$

where u and v are integers. By acting λ on (4) we obtain

$$\zeta^v+\zeta^{-v}=(-1)^{u+(1/4)(p-7)}(\zeta+\zeta^{-1}).$$

From this we can take an element φ not belonging to $G(F)$ as

$$\varphi(\eta)=\eta^{-1}; \qquad \varphi(\zeta)=\zeta^{-p}.$$

Immediately we have

$$\varphi^2=1, \quad \varphi\rho=\rho\varphi, \quad \varphi\sigma=\sigma^{4+p}\varphi, \quad G=\langle\sigma, \rho, \varphi\rangle.$$

Next we shall prove (ii). Suppose that H is a commutative subgroup of G of index 2. Then H contains $\langle\sigma^4\rangle$. The factor group $\bar{H}=H/\langle\sigma^4\rangle$ is the commutative subgroup of the Galois group $G(K_2/Q)$ where K_2 is a subfield of K_3 generated by $\sqrt[4]{\varepsilon_p}$ and $\sqrt{-1}$. In Section 2 of [3], we know that there are only three commutative subgroups of index 2 in $G(K_2/Q)$. They are given as follows.

$$\langle\bar{\sigma}, \bar{\varphi}\bar{\rho}\rangle, \quad \langle\bar{\sigma}^2, \bar{\varphi}, \bar{\rho}\rangle, \quad \langle\bar{\sigma}^2, \bar{\sigma}\bar{\varphi}, \bar{\sigma}\bar{\rho}\rangle,$$

where for the element α of G, $\bar{\alpha}$ denotes the restriction of α to K_2. Thus H coincides with one of the three subgroups

$$\langle\sigma, \varphi\rho\rangle, \quad \langle\sigma^2, \varphi, \rho\rangle, \quad \langle\sigma^2, \sigma\varphi, \sigma\rho\rangle.$$

By (5) we see

$$\sigma\varphi\rho=\varphi\rho\sigma^{4+3p}, \quad \sigma^2\rho=\rho\sigma^6, \quad \sigma^2(\sigma\rho)=(\sigma\rho)\sigma^6.$$

This shows that $\langle\sigma^2, \varphi, \rho\rangle$ and $\langle\sigma^2, \sigma\varphi, \sigma\rho\rangle$ are non-commutative and that $\langle\sigma, \varphi\rho\rangle$ is commutative only when $p\equiv 7 \bmod 8$. Q.E.D.

Corollary 1.

(i) *If* $p\equiv 7 \bmod 8$, K_3 *contains one and only one quadratic subfield over which* K_3 *is abelian. This quadratic subfield is* $Q(\sqrt{-p})$.

(ii) *If* $p\equiv 3 \bmod 8$, *then* K_3 *contains no quadratic subfields over which* K_3 *is abelian.* K_3 *is a cyclic extension of degree* 8 *over* L.

Proof. In Section 2 of [3], we obtained the field of invariants of the group $\langle\bar{\sigma}, \bar{\varphi}\bar{\rho}\rangle$ is $Q(\sqrt{-p})$. Therefore our statements follow from (ii) of Proposition 1. Q.E.D.

We shall explain the notation to be used in the following. Let $\mathscr{K}$ be a finite abelian extension over the number field $\mathscr{F}$. Then we denote by $f(\mathscr{K}/\mathscr{F})$ the conductor of $\mathscr{K}$ over $\mathscr{F}$. For an integral ideal $\mathfrak{a}$ of $\mathscr{F}$, we denote by $H_{\mathscr{F}}(\mathfrak{a})$ the maximal ray class group defined mod $\mathfrak{a}$ and by $P_{\mathscr{F}}(\mathfrak{a})$ the subgroup of $H_{\mathscr{F}}(\mathfrak{a})$ generated by the principal classes. For an integral ideal $\mathfrak{b}$ prime to $\mathfrak{a}$, we denote by $[\mathfrak{b}]$ the class of $H_{\mathscr{F}}(\mathfrak{a})$ represented by $\mathfrak{b}$. If $\mathfrak{b}$ is principal, i.e. $\mathfrak{b}=(b)$, then we write [b] instead of [(b)]. For an intermediate field $\mathscr{L}$ of $\mathscr{K}$ over $\mathscr{F}$, we denote by $C_{\mathscr{F}}(\mathscr{L})$ the subgroup of $H_{\mathscr{F}}(f(\mathscr{K}/\mathscr{F}))$ corresponding to $\mathscr{L}$ by Artin reciprocity law. Further we put

$$C^*_{\mathscr{F}}(\mathscr{L})=C_{\mathscr{F}}(\mathscr{L})\cap P_{\mathscr{F}}(f(\mathscr{K}/\mathscr{F})).$$

Consider the following sequence of subfields of K_3,

$$K_3 \supset K_2 = \boldsymbol{Q}(\sqrt{-1}, \sqrt[4]{\varepsilon_p}) \supset K_1 = \boldsymbol{Q}(\sqrt{-1}, \sqrt{\varepsilon_p}) \supset L$$
$$= \boldsymbol{Q}(\sqrt{-1}, \sqrt{-p}) \supset k = \boldsymbol{Q}(\sqrt{-p}).$$

Proposition 2. *Let the notation be as above. Then*

(i) *If* $p \equiv 7 \bmod 8$, *then* K_3 *is abelian over* k *and the conductors of intermediate fields over* k *are given as follows.*

$$f(L/k) = (4),\ f(K_i/k) = (2^{i+2}) \qquad \textit{for } i = 1, 2, 3.$$

(ii) *If* $p \equiv 3 \bmod 8$, *then* K_3 *is abelian over* L *and the conductors of the intermediate fields over* L *are given as follows.*

$$f(K_i/L) = (2^{i+1}) \qquad \textit{for } i = 1, 2, 3.$$

Proof. We know the exponent of quadratic defect $S_L(\varepsilon_p)$ of ε_p at L equals to 1. Thus we see immediately $S_{K_1}(\sqrt{\varepsilon_p}) = S_{K_2}(\sqrt[4]{\varepsilon_p}) = 1$. By Lemmas 1 and 4 of [3], we have our results. Q.E.D.

§ 2. The case $p \equiv 7 \bmod 8$

Put $K_0 = L$. For brevity's sake, we will write C_i instead of $C_k^*(K_i)$ for every $i \geqq 0$. Let h be the class number of k. Since h is odd, we have the following isomorphisms between groups;

$$G(K_3/k) \xrightarrow[\text{Artin map}]{\sim} H_k((32))/C_k(K_3) \xrightarrow{\sim} P_k((32))/C_3.$$
$$[\mathfrak{a}] \longrightarrow [\mathfrak{a}]^h$$

Let $(2) = \mathscr{P}\mathscr{P}'$ be the decomposition of the ideal (2) in k. Take two integers A and B of k such that

$$A \equiv 5 \bmod \mathscr{P}^5; \qquad A \equiv 1 \bmod \mathscr{P}'^5,$$
$$B \equiv -1 \bmod \mathscr{P}^5; \qquad B \equiv 1 \bmod \mathscr{P}'^5.$$

Then it is easy to see

$$(6) \qquad \begin{cases} P_k((32)) = \langle [A], [A^\rho], [B] \rangle, \\ [A][A^\rho] = [5],\ [A]^8 = [A^\rho]^8 = 1, \\ [B] = [B^\rho],\ [B]^2 = 1. \end{cases}$$

Lemma 1. *The class groups* C_2 *and* C_3 *are given by*

$$C_2=\langle [A]^4,\ [A^\rho]^4,\ [A]\cdot[A^\rho]\rangle,$$
$$C_3=\langle [A]^5\cdot[A^\rho]\rangle.$$

Proof. For an integer a dividing 32, put

$$K(a)=\mathrm{Ker}\,(P_k((32))\xrightarrow{\text{can.}}P_k((a))).$$

Then it is easy to see

$$K(2)=P_k((32)),$$
$$K(2^{i+1})=\langle [A]^{2^{i-1}},\ [A^\rho]^{2^{i-1}}\rangle \qquad (i=1,\ 2,\ 3 \text{ and } 4).$$

By (i) of Proposition 2, we know

$$C_i\supset K(2^{i+2}),\ \not\supset K(2^{i+1}), \qquad \text{for every } i.$$

This shows

$$C_0=K(4)=\langle [A],\ [A^\rho]\rangle,$$
$$C_i\ni [A]^{2^i},\quad [A^\rho]^{2^i},\quad \not\ni [A]^{2^{i-1}},\quad [A^\rho]^{2^{i-1}},\quad \text{for } i\geqq 1.$$

Further $G(K_2/Q)$ is non-commutative. Therefore we have

$$C_2\not\ni [A]\cdot[A^\rho]^{-1}.$$

Since C_{i+1} is a subgroup of C_i of index 2 for every i, we see

$$C_1=\langle [A]^2,\ [A^\rho]^2,\ [A]\cdot[A^\rho]\rangle,$$
$$C_2=\langle [A]^4,\ [A^\rho]^4,\ [A]\cdot[A^\rho]\rangle=\langle [A]^4,\ [A]\cdot[A^\rho]\rangle.$$

From the relation $\rho\sigma\rho^{-1}=\sigma^3$ in G it follows

$$[A^\rho]\cdot[A]^{-3}\in C_3.$$

Hence we have

$$C_3=\langle [A]^5\cdot[A^\rho]\rangle. \qquad \text{Q.E.D.}$$

Lemma 2. *Put* $\omega=\frac{1}{2}(1+\sqrt{-p})$. *Let* $S=x+y\omega$ *be an integer of* k. *Then*

$$[S]\in C_2 \Longleftrightarrow x\colon \textit{odd},\ y\equiv 0 \bmod 16.$$

Let $[S]\in C_2$ *and suppose* $x\equiv 1 \bmod 4$. *Then*

$$[S]\in C_3 \Longleftrightarrow \tfrac{1}{4}(x-1)+y/16\equiv 0 \bmod 2.$$

Proof. By easy calculation we know

$$AA^{\rho}\equiv 5 \bmod 32, \quad A^4\equiv 17+16\omega \bmod 32,$$
$$A^5A^{\rho}\equiv 21+16\omega \bmod 32.$$

By Lemma 1, we have

$$C_2=\langle[5], [17+16\omega]\rangle=\{[x+y\omega]\,|\,x\equiv 1 \bmod 4,\ y\equiv 0 \bmod 16\},$$
$$C_3=\langle[21+16\omega]\rangle$$
$$=\left\{[x+y\omega]\,\middle|\,\begin{array}{l}x\equiv 1 \bmod 4,\ y\equiv 0 \bmod 16,\\ x \text{ is square mod } 32 \text{ if and only if } y\equiv 0 \bmod 32\end{array}\right\}.$$

If $x\equiv 1 \bmod 4$, then

$$x \text{ is square mod } 32 \Longleftrightarrow x\equiv 1 \bmod 8.$$

Hence

$$[S]\in C_3 \Longleftrightarrow \tfrac{1}{4}(x-1)\equiv y/16 \bmod 2. \qquad \text{Q.E.D.}$$

Theorem 1. *Let h be the class number of k and q a prime number such that $q\equiv 1 \bmod 4$ and $(p/q)=1$. Then we have*

$$(\varepsilon_p/q)_4=1 \Longleftrightarrow \left\{\begin{array}{l}\textit{there exists uniquely determined integers } a \textit{ and } b \textit{ such that}\\ q^h=a^2+64pb^2, \quad a\equiv 1 \bmod 4, \quad (a, q)=1, \quad b>0.\end{array}\right.$$

Further, in the above case, we have

$$(\varepsilon_p/q)_8=(-1)^{(1/4)(a-1)+b}.$$

Proof. Let $\mathfrak{Q}$ be a prime factor of q in k and put

$$\mathfrak{Q}^h=(x+y\omega), \qquad x\equiv 1 \bmod 4.$$

Then we see

$$(\varepsilon_p/q)_4=1 \Longleftrightarrow \mathfrak{Q} \text{ decomposes completely in } K_2$$
$$\Longleftrightarrow [x+y\omega]\in C_2.$$

By Lemma 2 we have $y=16b$ for an integer b. Further we have

$$x+y\omega=(x+8b)+8b\sqrt{-p}.$$

Put $a=x+8b$. Then $a\equiv 1 \bmod 4$ and $q^h=a^2+64pb^2$. Again by Lemma 2,

$$(\varepsilon_p/q)_8=1 \Longleftrightarrow \mathscr{Q} \text{ decomposes completely in } K_3$$
$$\Longleftrightarrow [a+8b\sqrt{-p}] \in C_3$$
$$\Longleftrightarrow \tfrac{1}{4}(a-1)+b\equiv 0 \bmod 2. \qquad \text{Q.E.D.}$$

Remark. In [6], E. Lehmer conjectured

$$(\varepsilon_7/q)_8=(-1)^{b+d}$$

for the prime numbers q such that $q\equiv 1 \bmod 16$ and $(\varepsilon_7/q)_4=1$, where b and d are integers given by $q=a^2+16b^2=c^2+448d^2$. This conjecture does not hold for $q=449$, since in this case we have $b=5$, $d=1$ and $(\varepsilon_7/q)_8=-1$. See the next numerical examples.

Numerical examples. Let $p=7$.

(a) $q=449=1^2+448\cdot 1^2$: $(\varepsilon_7/q)_8=-1$.

$$\varepsilon_7=8+3\sqrt{7}\equiv 8+3\cdot 160\equiv 39\equiv 200^2\equiv 149^4\equiv \text{NO} \bmod 449.$$

Here the notation "NO" implies that 149 is not square mod 449.

(b) $q=617=13^2+448\cdot 1^2$: $(\varepsilon_7/q)_8=1$.

$$\varepsilon_7\equiv 8+3\cdot 161\equiv 491\equiv 209^2\equiv 120^4\equiv 103^8 \bmod 617.$$

(c) $q=1801=(-3)^2+448\cdot 2^2$: $(\varepsilon_7/q)_8=-1$.

$$\varepsilon_7\equiv 8+3\cdot 746\equiv 445\equiv 801^2\equiv 314^4\equiv \text{NO} \bmod 1801.$$

§ 3. The case $p\equiv 3 \bmod 8$

Let R be the maximal order of L. Then R is a free module of rank 4 over $\boldsymbol{Z}$ generated by $1, \omega, \sqrt{-1}, \sqrt{-1}\omega$, where $\omega=\frac{1}{2}(1+\sqrt{-p})$.

The prime number 2 has unique prime divisor $\mathscr{P}$ in L and decomposes in $(2)=\mathscr{P}^2$. The prime ideal $\mathscr{P}$ is a free module over $\boldsymbol{Z}$ generated by 2, $1+\sqrt{-1}$, $1+\sqrt{p}$, $1+\sqrt{-p}$. Therefore we have,

for an integer $\alpha=X+\sqrt{-1}\,Y+(Z+\sqrt{-1}\,W)\omega$ of L $(X, Y, Z, W\in \boldsymbol{Z})$,

$$(7) \qquad \begin{aligned} \alpha \in (2^e) &\Longleftrightarrow X\equiv Y\equiv Z\equiv W\equiv 0 \bmod 2^e,\\ \alpha \in (2^e)\mathscr{P} &\Longleftrightarrow X\equiv Y\equiv Z\equiv W\equiv 0 \bmod 2^e,\\ & \qquad X-Y\equiv Z-W\equiv 0 \bmod 2^{e+1}. \end{aligned}$$

Since L has two archimedean places, the rank of the unit group $R^\times$ of L equals to 1. The fundamental unit E of L is given in the following

Lemma 3. *Let p be a prime number such that $p\equiv 3 \bmod 4$. Let ε_p be the totally positive fundamental unit of $F=Q(\sqrt{p})$. Then there exists two positive odd integers s and t such that*

$$\varepsilon_p=s^2+(-1)^{(1/4)(p-3)}+st\sqrt{p}.$$

Further a fundamental unit E of L is given by

$$E=\tfrac{1}{2}(s-t)+\tfrac{1}{2}(s+t)\sqrt{-1}+t(1-\sqrt{-1})\omega.$$

Proof. Write

$$\varepsilon_p=uE^l, \qquad N_{L/F}(E)=\varepsilon_p^k,$$

where u is a root of unity contained in L and l and k are rational integers. Then we have $kl=2$ and we can assume $k>0$. Let H, h, h' be the class number of L, k and F respectively. It is well-known that

$$Hk=hh'.$$

Since h and h' are odd integers, we have $k=1$ and $l=2$. If $p=3$, then we may take $s=t=1$. Therefore we may assume $p>3$. Put

$$E=\tfrac{1}{2}(X+\sqrt{-1}\,Y)+\tfrac{1}{2}(Z+\sqrt{-1}\,W)\sqrt{-p},$$

where X, Y, Z and W are integers with properties:

$$X-Z\equiv Y-W\equiv 0 \bmod 2.$$

If $Y=Z=0$ or $X=W=0$, then E is written in the product of a power of ε_p and a root of unity. Thus these cases are outside of our consideration. Since

$$N_{L/Q(\sqrt{-1})}(E)=\tfrac{1}{4}(X^2-Y^2+p(Z^2-W^2))+\tfrac{1}{2}(XY+pZW)\sqrt{-1}\in\langle\sqrt{-1}\rangle,$$

we have one of the next relations (8) and (9);

$$(8)\qquad X^2-Y^2+p(Z^2-W^2)=\pm 4:\ XY+pZW=0,$$

$$(9)\qquad X^2-Y^2+p(Z^2-W^2)=0:\ XY+pZW=\pm 2.$$

Furthermore we have

$$\begin{aligned}E^2=&\tfrac{1}{4}(X^2-Y^2-p(Z^2-W^2))-\tfrac{1}{2}(XW+YZ)\sqrt{p}\\&+\sqrt{-1}(\tfrac{1}{2}(XY-pZW)+\tfrac{1}{2}(XZ-WY)\sqrt{p}).\end{aligned}$$

Since $E^2 = u\varepsilon_p$, where u is a 4-th root of unity, one of the following relations (10) and (11) holds true.

$$(10) \qquad X^2 - Y^2 - p(Z^2 - W^2) = 0: \quad XW + YZ = 0,$$

$$(11) \qquad XY - pZW = 0: \quad XZ - WY = 0.$$

Therefore we have four possibilities. By easy arguments, we know only the combination of (9) and (10) holds true. In this case we obtain

$$\begin{gathered} X = -Y: \ Z = W \quad \text{or} \quad X = Y: \ Z = -W, \\ Y^2 - pW^2 = 2(-1)^{(1/4)(p-7)}. \end{gathered}$$

Since

$$\varepsilon_p = N_{L/F}(E) = \tfrac{1}{2}(Y^2 + pW^2) + YW\sqrt{p} = Y^2 + (-1)^{(1/4)(p-3)} + YW\sqrt{p},$$

we may take $s = |Y|$ and $t = |W|$. Q.E.D.

In the following, for $i = 1, 2$ and 3, put $C_i = C_L^*(K_i)$. Since H is odd, we have the following isomorphisms between cyclic groups of order 8.

$$\begin{gathered} G(K_3/L) \xrightarrow[\text{Artin map}]{\sim} H_L((16))/C_L(K_3) \xrightarrow{\sim} P_L((16))/C_3. \\ [\alpha] \longmapsto [\alpha]^H \end{gathered}$$

Let $\hat{R}$ be the completion of R at $\mathscr{P}$ and $\hat{\mathscr{P}}$ the unique prime ideal of $\hat{R}$. Then $\pi = 1 + \sqrt{-1}$ is a prime element of $\hat{R}$. For every integer $n > 0$, put

$$U_n = 1 + \hat{\mathscr{P}}^n.$$

Let A be an integer of k such that $A^3 \equiv 1 \bmod 16$. For example we can take A as

$$(12) \qquad A = \begin{cases} 2u - (1 + 4u)\omega & \text{if } p = 3 + 8u \equiv 3 \bmod 16, \\ 2(u+2) + (7 - 4u)\omega & \text{if } p = 3 + 8u \equiv 11 \bmod 16. \end{cases}$$

Since $R^\times$ is contained in U_1, We have the following isomorphism:

$$(13) \qquad P_L((16)) \xrightarrow{\sim} \langle \bar{A} \rangle \otimes (U_1/U_8)/V,$$

where $\bar{A}$ denotes the class of $\hat{R}^\times/U_8$ represented by A and V denotes the subgroup of U_1/U_8 generated by the classes represented by the elements of $R^\times$.

Lemma 4. *Let E be the unit of L given in Lemma 3. Consider the* *following five integers of L such that*

$$B=1+A\pi^4,\quad D_1=1+\pi^3,\quad D_2=1+A\pi^3,$$
$$S=1+\pi^2,\qquad T=1-\pi=-\sqrt{-1}.$$

Then these six elements E, B, D_1, D_2, S and T generate U_1 mod U_8. *Further we have the following congruences;*

$$\text{(14)}\qquad \begin{aligned} &ST^2\equiv BD_2^2\cdot(BD_2^2)^{\varphi} \bmod U_8,\\ &D_2^{\varphi}D_1\equiv D_2^7 \bmod U_8,\\ &D_2^{\varphi\rho}\equiv D_2^5\cdot(BD_2^2)^3\cdot S^2\cdot D_1^{-2}\cdot(D_1D_2)^4 \bmod U_8. \end{aligned}$$

Proof. By (12) we know

$$\omega\equiv A \bmod \pi^2.$$

Therefore from the Lemma 3 it follows

$$E\equiv 1+A_0\pi \bmod \pi^2,$$

where A_0 is A or A^2. From this we have

$$E^2\equiv 1+A_0^2\pi^2 \bmod \pi^4,\qquad E^4\equiv 1+\pi^4 \bmod \pi^5.$$

Let $\alpha=1+a\pi^i\in U_i$ with $a\in\hat{R}^{\times}$. Then we note for $i\geqq 3$,

$$\alpha^2\equiv 1+a\pi^{i+2} \bmod \pi^{i+3}.$$

Since the group U_i/U_{i+1} is isomorphic to $Z/(2)\oplus Z/(2)$ for $i\geqq 1$, we have

E and T generate U_1 mod U_2,
E^2 and S generate U_2 mod U_3,
D_1 and D_2 generate U_3 mod U_4,
E^4 and B generate U_4 mod U_5,
D_1^2 and D_2^2 generate U_5 mod U_6,
E^8 and B^2 generate U_6 mod U_7,
D_1^4 and D_2^4 generate U_7 mod U_8.

Hence we have inductively

$$\text{(15)}\qquad \begin{cases} U_7/U_8=\langle \bar{D}_1^4, \bar{D}_2^4\rangle, \quad U_6/U_8=\langle \bar{E}^8, \bar{B}^2, \bar{D}_1^4, \bar{D}_2^4\rangle,\\ U_5/U_8=\langle \bar{E}^8, \bar{B}^2, \bar{D}_1^2, \bar{D}_2^2\rangle, \quad U_4/U_8=\langle \bar{E}^4, \bar{B}, \bar{D}_1^2, \bar{D}_2^2\rangle,\\ U_3/U_8=\langle \bar{E}^4, \bar{B}, \bar{D}_1, \bar{D}_2\rangle, \quad U_2/U_8=\langle \bar{E}^2, \bar{S}, \bar{B}, \bar{D}_1, \bar{D}_2\rangle,\\ U_1/U_8=\langle \bar{E}, \bar{T}, \bar{S}, \bar{B}, \bar{D}_1, \bar{D}_2\rangle, \end{cases}$$

where $\bar{E}, \bar{B}, \cdots, \bar{S}$ and $\bar{T}$ denote the classes of U_1/U_8 represented by $E, \cdots, S$ and T respectively. The relation (14) is obtained from the direct calculation. Q.E.D.

Corollary 2. *The degree of the class group* $P_L((16))$ *is* $3\cdot 4^5$ *and we have the following isomorphism*:

$$P_L((16)) \xrightarrow{\sim} \langle [B], [D_1], [D_2], [S]\rangle \otimes \langle [A]\rangle.$$

Proof. This is obvious from (13) and Lemma 4. Q.E.D.

Lemma 5. *Let the notation be as above. Then*

$$C_2 = \langle [B][D_2]^2, [D_1], [D_2]^4, [S]\rangle \otimes \langle [A]\rangle,$$
$$C_3 = \langle [B][D_2]^6, [D_1], [S]\rangle \otimes \langle [A]\rangle.$$

Proof. For $1 \leqq n \leqq 8$, put

$$K(\mathscr{P}^n) = \ker (P_L((16)) \xrightarrow{\text{can.}} P_L(\mathscr{P}^n)).$$

Then obviously we see

$$K(\mathscr{P}^n) = \langle [x] \mid x \in R,\ x \in U_n/U_8\rangle.$$

By (15) we know $K(\mathscr{P}^n)$ explicitly. By (ii) of Proposition 2, we have

(16) $$C_i \supset K(\mathscr{P}^{2i+2}), \quad \not\supset K(\mathscr{P}^{2i+1}) \quad (i=1, 2, 3).$$

We note that C_i is G-invariant and C_{i+1} is a subgroup of C_i of index 2 for every i. First of all we shall determine the group C_1. By (16) we know

$$C_1 \supset \langle [B], [D_1]^2, [D_2]^2\rangle.$$

Since $G(K_1/Q)$ is commutative, we see

$$[D_2]^\varphi \cdot [D_2]^{-1} \in C_1.$$

Thus, it follows from (14)

$$[S] = ([B]\cdot [D_2]^2)([B]\cdot [D_2]^2)^\varphi \in C_1,$$
$$[D_1] = ([D_2]^\varphi \cdot [D_2]^{-1})^{-1} \cdot [D_2]^6 \in C_1.$$

By Corollary 2, we have

$$C_1 = \langle [B], [D_1], [S], [D_2]^2\rangle \otimes \langle [A]\rangle.$$

Next we shall calculate C_2. Since $[D_1]^2 \in C_2$, we deduce from (16)

$$C_2 \not\ni [D_2]^2.$$

This shows that $[D_2]$ generates $P_L((16))$ mod C_2. The relation (5) implies

$$[D_2]^{\varphi} \cdot [D_2]^{-3}, \qquad [D_2]^{\varphi\rho} \cdot [D_2]^{-1} \in C_2.$$

This shows

$$[D_1],\ [B] \cdot [D_2]^2,\ [S] \in C_2.$$

Therefore we have

$$C_2 = \langle [S],\ [D_1],\ [B] \cdot [D_2]^2,\ [D_2]^4 \rangle \otimes \langle [A] \rangle.$$

Consider the group C_3. Since $[D_1]^2 \in C_3$, we see by (16)

$$[D_2]^4 \notin C_3.$$

Thus the class $[D_2]$ generates $P_L((16))$ mod C_3. By (5) we obtain

$$[D_2]^{\varphi} \cdot [D_2]^{-7},\ [D_2]^{\varphi\rho} \cdot [D_2]^{-5} \in C_3.$$

By the result for C_2 and (14) we have

$$[D_1] = ([D_2]^{\varphi} \cdot [D_2]^{-7})^{-1},\ [S]^2,\ ([B] \cdot [D_2]^2)^2 \in C_3.$$

Thus

$$[B] \cdot [D_2]^6 = ([D_2]^{\varphi\rho} \cdot [D_2]^{-5}) \cdot [D_1]^{-2} \cdot [S]^{-2} \cdot ([B] \cdot [D_2]^2)^{-2} \in C_3.$$

From this especially we have, because of $[D_2]^4 \notin C_3$,

$$[B] \cdot [D_2]^2,\ ([B] \cdot [D_2]^2)^{\varphi} \notin C_3.$$

Therefore

$$[S] \in C_3.$$

Hence

$$C_3 = \langle [B] \cdot [D_2]^6,\ [D_1],\ [S] \rangle \otimes \langle [A] \rangle. \qquad \text{Q.E.D.}$$

Lemma 6. *Let* (α) *be the principal integral ideal of* L *whose generator* α *satisfies the condition* $\alpha \equiv 1 \bmod \mathscr{P}$. *Then we have*

$[\alpha] \in C_2 \Longleftrightarrow$ *The ideal* (α) *has the generator* β *of the following type*:
$$\beta = x + 2y\sqrt{-1} + (8z + 4\sqrt{-1}w)\,\omega,\ x, y, z, w \in \boldsymbol{Z},\ x \equiv 1 \bmod 4.$$

Further suppose $[\alpha] \in C_2$ *and* (α) *has the generator of the above type. Then*

$$[\alpha] \in C_3 \Longleftrightarrow z \equiv yw \bmod 2.$$

Proof. By (7), we know that (α) has a generator of the form:

$$X+Y\sqrt{-1}+(Z+\sqrt{-1}\,W)\omega, \quad X\equiv 1 \bmod 4, \quad Y\equiv Z-W\equiv 0 \bmod 2.$$

By the definitions of S and D_1, we see

$$\langle [S], [D_1]\rangle = \{[X+\sqrt{-1}\,Y] \mid X\equiv 1 \bmod 4,\ Y\equiv 0 \bmod 2\}.$$

Since

$$\begin{aligned} BD_2^2 &\equiv 1+8\sqrt{-1}+(8+4\sqrt{-1})\omega \bmod 16,\\ D_2^4 &\equiv 1+(8+8\sqrt{-1})\omega \qquad\qquad \bmod 16, \end{aligned}$$

we have

$$\begin{aligned} C_2 = \{[X+\sqrt{-1}\,Y+(Z+\sqrt{-1}\,W)\omega] \mid \\ X\equiv 1 \bmod 4,\ Y\equiv 0 \bmod 2,\ Z\equiv 0 \bmod 8,\ W\equiv 0 \bmod 4\}. \end{aligned}$$

It is easy to see the group C_3 is generated by $[S]$, $[D_1]$ and $[1-4\sqrt{-1}\,\omega]$. Obviously we have

$$\langle [1-4\sqrt{-1}\,\omega]\rangle = \{[1+4b\sqrt{-1}\,\omega] \mid b \in \boldsymbol{Z}\}.$$

Since any element ν of C_3 is a product of an element $[X+\sqrt{-1}\,Y] \in \langle [S], [D_1]\rangle$ and an element $[1+4b\sqrt{-1}\,\omega] \in \langle [1-4\sqrt{-1}\,\omega]\rangle$, the class ν has a generator ν_0 such that

$$\begin{aligned} \nu_0 &\equiv (X+Y\sqrt{-1})(1+4b\sqrt{-1}\,\omega)\\ &\equiv X+Y\sqrt{-1}+4b(-Y+\sqrt{-1})\omega \bmod 16. \end{aligned}$$

If we put $\nu_0 = x+2y\sqrt{-1}+(8z+4\sqrt{-1}\,w)\omega$, $x, y, z, w \in \boldsymbol{Z}$, then the above congruence shows

$$z+yw\equiv 0 \bmod 2.$$

Converse part is obvious. Q.E.D.

Theorem 2. *Let H be the class number of L. Let q be a prime number such that* $q\equiv 1 \bmod 8$ *and* $(p/q)=1$. *Then we have*

$$(\varepsilon_p/q)_4=1 \Longleftrightarrow \begin{cases} \textit{there exists uniquely determined integers } \xi \textit{ and } \eta \textit{ such} \\ \textit{that } \xi\equiv 1 \bmod 4,\ (\xi, q)=1,\ \eta>0 \textit{ and they satisfy one of} \\ \textit{the following relations:} \\ q^H=\xi^2+64p\eta^2,\ q^H=\frac{1}{4}(\xi^2+p\eta^2). \end{cases}$$

Let a and b be the uniquely determined integers such that

$$a\equiv 1 \bmod 4, \quad (a, q)=1, \quad b>0 \quad \textit{and} \quad q^H=a^2+16b^2.$$

Suppose $(\varepsilon_p/q)_4=1$ *and take* ξ *and* η *as above. Then we have*

$$(\varepsilon_p/q)_8=\begin{cases}(-1)^{\eta+(\xi+a-2)/8} & \textit{if } q^H=\xi^2+64p\eta^2, \\ (-1)^{(\xi+a-2)/8} & \textit{if } q^H=\frac{1}{4}(\xi^2+p\eta^2).\end{cases}$$

Proof. The condition on q implies that q decomposes completely in L. Let $\mathcal{Q}$ be one of the prime factors of q in L. Since H is odd, we know

$$(\varepsilon_p/q)_4=1 \Longleftrightarrow [\mathcal{Q}]^H \in C_2, \qquad (\varepsilon_p/q)_8=1 \Longleftrightarrow [\mathcal{Q}]^H \in C_3.$$

Assume $[\mathcal{Q}]^H \in C_2$. Then by Lemma 6, there exists five integers x, y, z, w and u such that

$$\mathcal{Q}^H=(x+2y\sqrt{-1}+(8z+4w\sqrt{-1})\omega)\cdot(A^u),$$
$$x\equiv 1 \bmod 4, \qquad u \in \{0, 1, 2\}.$$

Further, we know

$$[\mathcal{Q}]^H \in C_3 \Longleftrightarrow z\equiv yw \bmod 2.$$

Firstly assume $u=0$. Then we have

$$N_{L/k}(\mathcal{Q}^H)=(\xi+8\eta\sqrt{-p}),$$

where

$$\text{(17)} \qquad \begin{cases}\xi=x^2+4y^2+8(xz+yw)+4(1-p)(4z^2+w^2), \\ \eta=xz+yw+4z^2+w^2.\end{cases}$$

Further we have

$$N_{L/k'}(\mathcal{Q}^H)=(a+4b\sqrt{-1}),$$

where k' denotes the field $\boldsymbol{Q}(\sqrt{-1})$ and

$$\text{(18)} \qquad \begin{cases}a=x^2-4y^2+8(xz-yw)+4(p+1)(4z^2-w^2), \\ b=(x+4z)(y+w)+4pzw.\end{cases}$$

We note $\xi\equiv\alpha\equiv 1 \bmod 4$. By easy calculation, we see

$$(\xi+\alpha-2)/8+\eta\equiv z+yw \bmod 2,$$
$$q^H=\xi^2+64p\eta^2=a^2+16pb^2.$$

Next consider the case $u\neq 0$. The we have

$$N_{L/k}(\mathcal{Q}^H)=(A^{2u}(\xi+8\eta\sqrt{-p})),$$
$$N_{L/k'}(\mathcal{Q}^H)=(N_{L/k'}(A)^u(a+4b\sqrt{-1})),$$

where ξ, η, a and b are integers given by (17) and (18) respectively. Put

$$A^{2u}(\xi+8\eta\sqrt{-p})=\tfrac{1}{2}(\xi'+\eta'\sqrt{-p}),$$
$$N_{L/k'}(A^u)(a+4b\sqrt{-1})=a'+b'\sqrt{-1}.$$

Since $N_{L/k'}(A)\equiv 1 \bmod 16$, we have

$$a'\equiv a \bmod 16, \qquad b'\equiv 4b \bmod 16.$$

Put

$$A^{2u}=\tfrac{1}{2}(c+d\sqrt{-p})\ (c,\ d\in Z,\ c\equiv d\equiv\ 1 \bmod 2).$$

Then

$$\xi'\equiv\xi\ \mathrm{tr}_{k/Q}(A^{2u})+8\eta(A^{2u}-A^{4u})\sqrt{-p}$$
$$\equiv-\xi+8\eta pd\equiv-\xi+8\eta \bmod 16.$$

Hence

$$[\mathcal{Q}]^H\in C_3\Longleftrightarrow(\xi+a-2)/8+\eta\equiv 0 \bmod 2\Longleftrightarrow(-\xi'+a-2)/8\equiv 0 \bmod 2,$$
$$q^H=\tfrac{1}{4}((-\xi')^2+p\eta'^2)=a'^2+16(b'/4)^2. \qquad \text{Q.E.D.}$$

Corollary 3. (*The proof for the strengthened form of the conjecture* 1 *of Lehmer* [6].) *Let q be a prime number such that* $q\equiv 1 \bmod 16$ *and* $(\varepsilon_p/q)_4=1$. *Suppose q has the expressions of the type*:

$$q^H=a^2+16b^2=c^2+64pd^2,$$

where a, b, c and d are integers satisfying $a\equiv c\equiv 1 \bmod 4$, $(ac,q)=1$. *Then we have*

$$(\varepsilon_p/q)_8=(-1)^{b+d}.$$

Proof. By (17) and (18) there exists four integers x, y, z and w such that

$$a=x^2-4y^2+8(xz-yw)+4(p+1)(4z^2-w^2),$$
$$b=\pm\{(x+4z)(y+w)+4pzw\},$$
$$d=xz+yw+4z^2+w^2,$$
$$x\equiv 1 \bmod 4.$$

From this we see

$$b+d\equiv z+yw+y \bmod 2.$$

The condition $q\equiv 1 \bmod 16$ implies $a\equiv 1 \bmod 8$. This shows $y\equiv 0 \bmod 2$. Therefore

$$b+d\equiv z+yw \bmod 2.$$

Lemma 6 shows our assertion. Q.E.D.

Numerical examples. In the below, put

$$F(\xi, \eta, a)=(\xi+a-2)/8+\eta,$$
$$G(\xi, a)=(\xi+a-2)/8.$$

The class number H is 1 in all cases treated here.

(i) $p=11$: $\varepsilon_{11}=10+3\sqrt{11}$.

a) $q=97$. $q=\frac{1}{4}(17^2+11\cdot 3^2)=9^2+16\cdot 1^2$: $G(17, 9)=3$.

$$\varepsilon_{11}\equiv 10+3\cdot 37\equiv 121\equiv 11^2\equiv 37^4\equiv \text{NO} \bmod 97.$$

Here "NO" means that the number 37 is not square mod 97.

b) $q=929$. $q=(-15)^2+704\cdot 1^2=(-23)^2+16\cdot 5^2$: $F(-15, 1, -23)=-4$.

$$\varepsilon_{11}\equiv 10+3\cdot 143\equiv 439\equiv 131^2\equiv 246^4\equiv 181^8 \bmod 929.$$

(ii) $p=19$: $\varepsilon_{19}=170+39\sqrt{19}$.

a) $q=73$. $q=\frac{1}{4}((-11)^2+19\cdot 3^2)=(-3)^2+16\cdot 2^2$: $G(-11, -3)=-2$.

$$\varepsilon_{19}\equiv 170+39\cdot 26\equiv 16\equiv 4^2\equiv 2^4\equiv 32^8 \bmod 73.$$

(iii) $p=43$. $\varepsilon_{43}=3482+531\sqrt{43}$.

a) $q=2833$. $q=9^2+64\cdot 43\cdot 1^2=(-23)^2+16\cdot 12^2$: $F(9, 1, -23)=-1$.

$$\varepsilon_{43}\equiv 649+531\cdot 244\equiv 2728\equiv 784^2\equiv 28^4\equiv \text{NO} \bmod 2833.$$

(iv) $p=163$. $\varepsilon_{163}=64080026+5019135\sqrt{163}$.

a) $q=97$. $q=\frac{1}{4}((-15)^2+163\cdot 1^2)=9^2+16\cdot 1^2$: $G(-15, 9)=-1$.

$$\varepsilon_{163}\equiv 80+64\cdot 39\equiv 54\equiv 32^2\equiv 41^4\equiv \text{NO} \bmod 97.$$

b) $q=1601$. $q=\frac{1}{4}((-79)^2+163\cdot 1^2)=1+16\cdot 10^2$: $G(-79, 1)=-10$.

$$\varepsilon_{163}\equiv 1+0\cdot 42\equiv 1 \bmod 1601.$$

c) $q=2753$. $q=\frac{1}{4}((-55)^2+163\cdot 7^2)=(-7)^2+16\cdot 13^2$: $G(-55, -7)$ $=-8$.

$$\varepsilon_{163}\equiv 1198+416\cdot 54\equiv 1638\equiv 1288^2\equiv 1290^4\equiv 679^8 \bmod 2753.$$

References

[1] Y. Furuta and P. Kaplan, On quadratic and quartic characters of quadratic units, Sci. Rep. Kanazawa Univ., **26** (1981), 27–30.

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

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

[4] N. Ishii, On the quartic residue symbol of totally positive quadratic units, Tokyo J. Math., **9** (1986), 53–65.

[5] K. Kramer, Residue properties of certain quadratic units, J. Number theory, **21** (1985), 204–213.

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

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

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