N. Ishii
Nagoya Math. J.
Vol. 98 (1985) 117-137

CUSP FORMS OF WEIGHT ONE, QUARTIC RECIPROCITY AND ELLIPTIC CURVES

NOBURO ISHII

§1. Introduction

Let m be a non-square positive integer. Let K be the Galois extension over the rational number field $\boldsymbol{Q}$ generated by $\sqrt{-1}$ and $\sqrt[4]{m}$. Then its Galois group over $\boldsymbol{Q}$ is the dihedral group D_4 of order 8 and has the unique two-dimensional irreducible complex representation ψ. In view of the theory of Hecke-Weil-Langlands, we know that ψ defines a cusp form of weight one (cf. Serre [6]). This cusp form is denoted by $\theta(\tau, K)$. The present paper consists of two parts. In the first part (§ 2 and § 3), we shall study the number theoretic properties of $\theta(\tau, K)$ deduced from K. We show firstly that $\theta(\tau, K)$ has three expressions by definite or indefinite theta series. We may consider these expressions of $\theta(\tau, K)$ as the identities between cusp forms of weight one. This point of view gives a number theoretic explanation for the identities between cusp forms ([3]). Further we show that the Fourier coefficients of the cusp form $\theta(\tau, K)$ determine the decomposition law of the extension $K/\boldsymbol{Q}$ and especially the quartic residuacity of m. These results are obtained from that K has three quadratic subfields over which K is abelian. In particular, for the case m is prime, we write down the above expressions of $\theta(\tau, K)$ explicitly by determining the class group corresponding to K in each quadratic subfield. We deduce from this a special case of quartic reciprocity law. In this part we also establish the "higher reciprocity law" of the defining equation of K.

Let E be the elliptic curve defined by the equation: $y^2=x^3+4mx$. Then K is generated over $\boldsymbol{Q}$ by certain torsion points of E. The purpose of the second part is to study the property of $\theta(\tau, K)$ related to E through K. Let $\vartheta(\tau, E)$ denote the inverse Mellin transform of the L-function of E. Then $\vartheta(\tau, E)$ is a cusp form of weight two (cf. Shimura [8]). In

Received April 13, 1984.

Section 4, we shall show, under certain assumption on m, the following congruence:

$$\theta(\tau, K) \equiv \vartheta(\tau, E) \bmod 4 .$$

We remark that this result provides an answer for the problem proposed by Koike (cf. Koike [4]).

The author would like to express his hearty gratitude to Professor T. Hiramatsu for encouraging him to consider these problems and Dr. Y. Mimura for very helpful discussions.

§ 2. Quartic residuacity and cusp forms of weight one

Let m be a non-square positive integer such that m has the following decomposition in prime numbers p:

$$(1) \qquad m = \prod_p p^{e(p)}, \qquad 0 \leqq e(p) \leqq 3 .$$

Let $K = \boldsymbol{Q}(\sqrt{-1}, \sqrt[4]{m})$ be the field generated by $\sqrt{-1}$ and $\sqrt[4]{m}$ over the rational number field $\boldsymbol{Q}$. Then K is a Galois extension over $\boldsymbol{Q}$ of degree 8 and its Galois group $G = G(K/\boldsymbol{Q})$ is isomorphic to the dihedral group D_4 of order 8. Let σ and ρ be the two generators of G defined by

$$\sigma(\sqrt[4]{m}) = \sqrt{-1}\,\sqrt[4]{m}, \qquad \sigma(\sqrt{-1}) = \sqrt{-1} ;$$
$$\rho(\sqrt[4]{m}) = \sqrt[4]{m}, \qquad \rho(\sqrt{-1}) = -\sqrt{-1} .$$

Then the following Diagram 1 of subfields of K is obtained:

$$\begin{tikzcd}
& K \arrow[d, dash] & \\
& L = \boldsymbol{Q}(\sqrt{-1}, \sqrt{m}) \arrow[dl, dash] \arrow[d, dash, "\langle\sigma^2\rangle"] \arrow[dr, dash] & \\
\langle\sigma^2, \rho\rangle\ F = \boldsymbol{Q}(\sqrt{m}) \arrow[dr, dash] & k = \boldsymbol{Q}(\sqrt{-1}) \arrow[d, dash, "\langle\sigma\rangle"] & E = \boldsymbol{Q}(\sqrt{-m})\ \langle\sigma^2, \sigma\rho\rangle \arrow[dl, dash] \\
& \boldsymbol{Q} &
\end{tikzcd}$$

Diagram 1.

To the field K we shall define a cusp form $\theta(\tau, K)$ of weight one. Let ψ be the two-dimensional complex irreducible representation of G defined by

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

Then the representation $\det \psi$ of G defined by $(\det \psi)(g) = \deg \psi(g)$ induces a Dirichlet character ε such that

$$\varepsilon(n) = (-1/n) .$$

Denote the Artin L-function associated with ψ by

$$L(s, K/\boldsymbol{Q}, \psi) = \sum_{n=1}^{\infty} a(n) n^{-s} .$$

Then $L(s, K/\boldsymbol{Q}, \psi)$ has the Euler product:

$$(2) \quad L(s, K/\boldsymbol{Q}, \psi) = \prod_{p \mid N} (1 - a(p)p^{-s})^{-1} \prod_{p \nmid N} (1 - a(p)p^{-s} + \varepsilon(p)p^{-2s})^{-1} ,$$

where N denotes the conductor of ψ. Now we define the function $\theta(\tau, K)$ by

$$\theta(\tau, K) = \sum_{n=1}^{\infty} a(n) q^n , \qquad q = \exp(2\pi\sqrt{-1}\tau) .$$

It follows from the well-known theory of Hecke-Weil-Langlands that $\theta(\tau, K)$ is a cusp form (new form) of weight one with character ε on the Hecke group $\Gamma_0(N)$[1].

We are going to give explicit form of $\theta(\tau, K)$. At first we explain the notation used below. Let Ω and Λ be fields such that Ω is abelian over Λ. Then $F(\Omega/\Lambda)$ (resp. $f(\Omega/\Lambda)$) denotes the conductor (resp. the finite part of conductor) of Ω over Λ. Let M be one of the quadratic fields appeared in Diagram 1. Then $\mathcal{O}_M$ denotes the ring of integers of M and $N_{M/\boldsymbol{Q}}$ denotes the norm of M over $\boldsymbol{Q}$. 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. Furthermore $P_M(\mathfrak{a})$ denotes the subgroup of $H_M(\mathfrak{a})$ generated by principal classes (resp. principal classes represented by totally positive elements). If $\mathfrak{b}$ is an ideal prime to $\mathfrak{a}$, then $[\mathfrak{b}]$ denotes the class of $H_M(\mathfrak{a})$ represented by $\mathfrak{b}$. If b is an element of M and (b) is the principal ideal generated by b, then $[b]$ denotes $[(b)]$. Finally let $C_M(K)$ (resp. $C_M(L)$) denote the subgroup of $H_M(f(K/M))$ corresponding to the field K (resp. L).

Let ψ and M be as above. Then the restriction of ψ to the abelian group $G(K/M)$ decomposes into two distinct linear representations ξ_M and ξ'_M of $G(K/M)$. Via Artin reciprocity law, we can identify ξ_M and ξ'_M with

1) See Serre [6], for example.

characters of $H_M(f(K/M))$ trivial on $C_M(K)$. We denote these characters by the same notation. If c_M and c'_M are the finite part of conductors of ξ_M and ξ'_M respectively, then c_M is conjugate to c'_M over $\boldsymbol{Q}$. Let $\tilde{\xi}_M$ (resp. $\tilde{\xi}'_M$) be the primitive character of ξ_M (resp. ξ'_M) and $L(s, \tilde{\xi}_M)$ (resp. $L(s, \tilde{\xi}'_M)$) the Hecke L-function associated with $\tilde{\xi}_M$ (resp. $\tilde{\xi}'_M$). Then it is well-known that

$$L(s, K/\boldsymbol{Q}, \psi) = L(s, \tilde{\xi}_M) = L(s, \tilde{\xi}'_M).^{2)} \tag{3}$$

Let $\tilde{C}_M(K)$ and $\tilde{C}_M(L)$ be the images of $C_M(K)$ and $C_M(L)$ by the canonical homomorphism of $H_M(f(K/M))$ to $H_M(c_M)$ respectively. Then, as shown in [3],

$$L(s, \tilde{\xi}_M) = \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_M \\ [\mathfrak{a}] \in \tilde{C}_M(L)}} \chi_M(\mathfrak{a}) N_{M/Q}(\mathfrak{a})^{-s},$$

where

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

Applying the inverse Mellin transformation on the both sides of (3), we obtain

$$\theta(\tau, K) = \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_M \\ [\mathfrak{a}] \in \tilde{C}_M(L)}} \chi_M(\mathfrak{a}) q^{N_{M/Q}(\mathfrak{a})}. \tag{4}$$

Therefore $\theta(\tau, K)$ has three expressions according to quadratic fields F, E and k. To determine $C_M(K)$ and $C_M(L)$, it is necessary to know the conductors of K/M and L/M. 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 $\mathscr{K}$ is abelian over $\mathscr{F}$. Then $f(\mathscr{K}/\mathscr{F})$ is determined by $f(\mathscr{K}/\mathscr{L})$ and the different $D(\mathscr{L}/\mathscr{F})$ of $\mathscr{L}$ over $\mathscr{F}$. Thus we have

LEMMA 1. *For a prime ideal $\mathfrak{P}$ of $\mathscr{L}$, let $f(\mathfrak{P})$ (resp. $g(\mathfrak{P})$) denotes the $\mathfrak{P}$-exponent of $f(\mathscr{K}/\mathscr{L})$ (resp. $D(\mathscr{L}/\mathscr{F})$). Put*

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

Then

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

2) See [3].

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

It follows from $[L:M]=2$ that $f(L/M)=D(L/M)^2$. And $D(L/M)$ is deduced from the following equalities:

$$D(L/\boldsymbol{Q})^2 = D(F/\boldsymbol{Q})D(E/\boldsymbol{Q})D(k/\boldsymbol{Q})\,;$$
$$D(L/\boldsymbol{Q}) = D(L/M)D(M/\boldsymbol{Q})\,.$$

In view of Lemma 1, to obtain $F(K/M)$ it is sufficient to determine $F(K/L)$. Write

$$m = 2^{e(2)}m_1\,, \qquad 0 \leqq e(2) \leqq 3\,, \quad (m_1, 2) = 1\,.$$

Let

$$n_1 = \prod_{\substack{p\mid m_1 \\ e(p):\ \text{even}}} p\,, \qquad n_2 = \prod_{\substack{p\mid m_1 \\ e(p):\ \text{odd}}} p\,.$$

Furthermore put $n = n_1\sqrt{n_2}$. Then the conductor $F(K/L)$ is as follows.

$e(2)$	1, 3	0			2		
$m_1 \bmod 8$		1	5	3, 7	1, 5	3	7
$F(K/L)$	$4n$	n	$2n$	$4n$	$4n$	$2n$	n

Table 1.

In the next Table 2, we give $F(K/M)$, $F(L/M)$ and c_M in only the cases needed below, thus, the cases where m are prime numbers $p \geqq 5$.

$p \bmod 8$	$F(K/E)$	$F(L/E)$	c_E	$F(K/k)$	$F(L/k)$	c_k	$F(K/F)$	$F(L/F)$	c_F
1	$\sqrt{-p}$	1	$\sqrt{-p}$	p	p	p	$4\sqrt{p}\,\infty_1\infty_2$	$4\infty_1\infty_2$	$\mathfrak{p}_2^2\sqrt{p}$
5	$2\sqrt{-p}$		$2\sqrt{-p}$	$2p$		$2p$			$4\sqrt{p}$
3, 7	$8\sqrt{-p}$	4	$8\sqrt{-p}$	$4p$	p	$4p$	$4\sqrt{p}\,\infty_1\infty_2$	$\infty_1\infty_2$	$4\sqrt{p}$

Table 2.

In the above Table 2, $\mathfrak{p}_2$ denotes a prime ideal of F dividing 2 and ∞_i $(i=1,2)$ denote infinite places of F. From this we know that $\tilde{C}_M(L) = C_M(L)$ and $\tilde{C}_M(K) = C_M(K)$ except the case $p \equiv 1 \bmod 8$ and $M = F$.

Assume that m is a prime p congruent to $5 \bmod 8$. Denote by $\theta(\tau, M)$ the right side of (4). In (I) through (III) below, we shall determine $\theta(\tau, M)$ explicitly for $M = E, k$ and F respectively. In the following we write simply H_M and P_M in place of $H_M(f(K/M))$ and $P_M(f(K/M))$ respectively.

Further for a prime ideal $\mathfrak{P}$ of M denote by $r(\mathfrak{P})$ a generator of the group $(\mathcal{O}_M/\mathfrak{P})^{\times}$. And, for an integral ideal $\mathfrak{a}$ dividing $f(K/M)$, denote by $K(\mathfrak{a})$ the kernel of the canonical homomorphism of P_M to $P_M(\mathfrak{a})$.

(I) The case $M = E(= \boldsymbol{Q}(\sqrt{-p}))$. Put $\mathfrak{P} = (\sqrt{-p})$. Let ω and λ be integers of E satisfying the following properties:

$$\begin{cases} \omega \equiv \sqrt{-p} \bmod 2\,, \\ \omega \equiv 1 \qquad \bmod \mathfrak{P}\,; \end{cases} \qquad \begin{cases} \lambda \equiv 1 \bmod 2,\ \lambda \in \boldsymbol{Z}^{+} \\ \lambda \equiv r(\mathfrak{P}) \bmod \mathfrak{P}\,. \end{cases}$$

Then it is easy to see

$$P_E = \langle [\omega], [\lambda] \rangle\,, \qquad K(\mathfrak{P}) = \langle [\omega] \rangle\,,$$
$$K((2)) = \langle [\lambda] \rangle\,.$$

Since $F(K/E) = 2\mathfrak{P}$ and $F(L/E) = 1$, we see

$$C_E(L) \supset P_E\,; \quad C_E(K) \not\supset P_E\,, \quad K(\mathfrak{P})\,, K((2))\,.$$

This implies

$$[P_E : P_E \cap C_E(K)] = 2\,, \qquad C_E(K) \not\ni [\omega], [\lambda]\,.$$

From this, noting that $[\lambda]^2 \in C_E(K)$, we have

$$P_E \cap C_E(K) = \langle [\omega] \cdot [\lambda] \rangle\,.$$

It follows from the genus theory that the class number $h(E)$ of E is even and that the number of square classes in H_E/P_E equals to $\frac{1}{2}h(E)$. Let $\mathfrak{a}_i$ $(i = 1, \cdots, \frac{1}{2}h(E))$ be integral ideals of E such that $[\mathfrak{a}_i]^2$ represent all square classes in H_E/P_E. Since $G(K/E)$ is a Klein four group, $[\mathfrak{a}_i]^2 \in C_E(K)$ and the following coset decompositions are obtained:

$$C_E(L) = C_E(K) + C_E(K)[\omega]\,,$$
$$C_E(K) = \sum_i [\mathfrak{a}_i]^{-2}(P_E \cap C_E(K))\,.$$

If $\mathfrak{a}$ is an integral ideal of E prime to $2\mathfrak{P}$ and $[\mathfrak{a}] \in C_E(L)$, then there exist unique $\mathfrak{a}_i$ and an element $a + b\sqrt{-p}$ of $\mathfrak{a}_i^2$ such that

$$\mathfrak{a} = \mathfrak{a}_i^{-2}(a + b\sqrt{-p})\,,$$
$$(a, p) = 1\,,$$
$$a \not\equiv b \bmod 2\,.$$

Furthermore

$$[\mathfrak{a}] \in C_E(K) \Longleftrightarrow (a/p)(-1)^b = 1\,.$$

Hence we obtain

$$\theta(\tau, E) = \frac{1}{2} \sum_{i=1}^{h(E)/2} \{ \sum_{\substack{a \not\equiv b \bmod 2 \\ a+b\sqrt{-p} \in \mathfrak{a}_i^2}} (-1)^b (a/p) q^{(a^2+pb^2)/A_i^2} \},$$

where $A_i = N_{E/Q}(\mathfrak{a}_i)$.

(II) The case $M = k (= \boldsymbol{Q}(\sqrt{-1}))$. Let $p = \mathfrak{P}\mathfrak{P}'$ be the decomposition in prime ideals of p in k. Choose integral elements η and λ of k satisfying the congruent relations:

$$\begin{cases} \eta \equiv \sqrt{-1} \bmod 2 \\ \eta \equiv 1 \qquad \bmod \mathfrak{P} \end{cases}; \quad \begin{cases} \lambda \equiv 1 \bmod 2 \\ \lambda \equiv r(\mathfrak{P}) \bmod \mathfrak{P} \\ \lambda \equiv 1 \bmod \mathfrak{P}'. \end{cases}$$

Let λ' be the conjugate of λ over $\boldsymbol{Q}$. Then it is easy to see $P_k = \langle [\lambda], [\lambda'], [\eta] \rangle$ and $K((p)) = \langle [\eta] \rangle$. It follows from the values of conductors in Table 2 that

$$[P_k : C_k(L)] = [C_k(L) : C_k(K)] = 2;$$
$$C_k(L) \supset K((p)), \quad C_k(K) \not\supset K((p)).$$

Since $G(K/k)$ is cyclic of order 4, we know

$$C_k(L) \in [\lambda]^2, \qquad C_k(K) \not\ni [\lambda]^2.$$

Further the commutativity (resp. non-commutativity) of $G(L/\boldsymbol{Q})$ (resp. $G(K/\boldsymbol{Q})$) implies that

$$C_k(L) \ni [\lambda]^{-1} \cdot [\lambda'] \quad (\text{resp. } C_k(K) \not\ni [\lambda]^{-1}[\lambda']).$$

Therefore

$$\begin{aligned} C_k(L) &= \langle [\lambda]^2, [\lambda]^{-1}[\lambda'], [\eta] \rangle, \\ C_k(K) &= \langle [\lambda]^2[\eta], [\lambda][\lambda']^{-1}[\eta] \rangle \\ &= \langle [\lambda]^4, [\lambda][\lambda']^{-1} \rangle. \end{aligned}$$

Thus for integral ideals $\mathfrak{a}$ of k prime to $2p$, we obtain

$$[\mathfrak{a}] \in C_k(L) \Longleftrightarrow \mathfrak{a} \text{ has a generator } x + \sqrt{-1}y \text{ such that } (x^2 + y^2/p) = 1,\ x \equiv 1,\ y \equiv 0 \bmod 2:$$

Furthermore

$$[\mathfrak{a}] \in C_k(K) \Longleftrightarrow (x + sy/p)(x^2 + y^2/p)_4 = 1,$$

where s is an integer such that $s^2 \equiv -1 \bmod p$.

Hence

$$\theta(\tau, k) = \frac{1}{2} \sum_{x,y} (x + sy/p)(x^2 + y^2/p)_4 q^{x^2+y^2},$$

where the summation is over all pairs of integers (x, y) such that $x \equiv 1$, $y \equiv 0 \bmod 2$ and $(x^2 + y^2/p) = 1$.

(III) The case $M = F(= \boldsymbol{Q}(\sqrt{p}))$. Let $\mathfrak{P} = (\sqrt{p})$ and $\omega = \frac{1}{2}(1 + \sqrt{p})$. For $\alpha \in \mathcal{O}_F$, take an element α^* of $\mathcal{O}_F$ such that

$$\begin{cases} \alpha^* \text{ is totally positive,} \\ \alpha^* \equiv \alpha \bmod 4\,, \\ \alpha^* \equiv 1 \bmod \mathfrak{P}\,. \end{cases}$$

Let $\xi \in \mathcal{O}_F$ such that ξ induces an element of order 3 in the group $(\mathcal{O}_F/4)^\times$. Let λ be a positive integer such that $\lambda \equiv 1 \bmod 4$ and $\lambda \equiv r(\mathfrak{P}) \bmod \mathfrak{P}$. Put $\eta = 1 + 2\omega$. Then it is easy to see

$$P_F = \langle[\xi^*], [\eta^*], [3^*], [\lambda]\rangle\,,$$
$$K((2)) = \langle[\eta^*], [3^*], [\lambda]\rangle\,, \quad K((4)) = \langle[\lambda]\rangle\,.$$

Taking account of the values of conductors, we have

$$[P_F : C_F(L) \cap P_F] = [C_F(L) \cap P_F : C_F(K) \cap P_F] = 2\,;$$
$$C_F(L) \supset K((4)),\ \not\supset K((2));\ C_F(K) \not\supset K((4))\,.$$

If $[\eta^*]'$ is the conjugate class of $[\eta^*]$, then

$$[\eta^*]' = [3^*]\cdot[\eta^*]\,.$$

Since $C_F(L)$ is closed under the conjugation, thus $C_F(L)' = C_F(L)$, and $C_F(L) \not\supset P_F$, we know

$$C_F(L) \not\ni [\eta^*],\ [\eta^*]\cdot[3^*]\,.$$

Therefore

$$C_F(L) \cap P_F = \langle[\xi^*], [3^*], [\lambda]\rangle\,. \tag{5}$$

The non-commutativity of $G(K/\boldsymbol{Q})$ shows that $C_F(K) \not\ni [3^*]$.

This implies

$$C_F(K) \cap P_F = \langle[\xi^*], [3^*][\lambda]\rangle\,. \tag{6}$$

Let $h(F)$ be the narrow class number of F. By the genus theory, $h(F)$ is odd. Let $\mathfrak{b}_i$ $(i = 1, \cdots, h(F))$ be integral ideals such that $[\mathfrak{b}_i]$ represent all classes of H_F/P_F. Then we have the coset decompositions:

$$C_F(L) = C_F(K) + C_F(K)[3^*]\,,$$
$$C_F(K) = \sum_i [\mathfrak{b}_i]^{-2}(C_F(K) \cap P_F)\,.$$

Let μ be a totally positive element of $\mathcal{O}_F$ prime to $4\mathfrak{P}$. If $\mu \equiv 1 \bmod 2$, then we can put $\mu = u + v\sqrt{p}$, $u \equiv v + 1 \bmod 2$. Further in view of (5) and (6), we obtain

$$(7)\qquad \begin{cases}[\mu] \in C_F(L) \Longleftrightarrow [\mu] \in \langle [3^*], [\lambda]\rangle \Longleftrightarrow v \equiv 0 \bmod 2,\ (p, u) = 1;\\ [\mu] \in C_F(K) \Longleftrightarrow (u/p)(-1)^{(u+v-1)/2} = 1,\ v \equiv 0 \bmod 2\,.\end{cases}$$

If $\mu \not\equiv 1 \bmod 2$, then we can put $\mu = \frac{1}{2}(s + t\sqrt{p})$, s: odd. Choose $a = 1$ or 2 such that $\mu\xi^{*a} \equiv 1 \bmod 2$. Put $\mu\xi^{*a} = u + v\sqrt{p}$, $u \equiv v + 1 \bmod 2$. Since $N_{F/Q}(\xi^*) \equiv 1 \bmod 4$, we have

$$N_{F/Q}(\mu) \equiv u^2 - v^2 \bmod 4\,.$$

Therefore

$$v \equiv 0 \bmod 2 \Longleftrightarrow N_{F/Q}(\mu) \equiv 1 \bmod 4\,.$$

Further if $v \equiv 0 \bmod 2$, then

$$\tfrac{1}{2}(u + v - 1) \equiv \tfrac{1}{2}(s + 1) \bmod 2\,.$$

Noting $s \equiv 2u \bmod p$, it follows from (7) that

$$[\mu] \in C_F(L) \Longleftrightarrow v\text{: even} \Longleftrightarrow N_{F/Q}(\mu) \equiv 1 \bmod 4\,;$$

Furthermore

$$[\mu] \in C_F(K) \Longleftrightarrow (u/p)(-1)^{(u+v-1)/2} = 1 \Longleftrightarrow (s/p)(-1)^{(s-1)/2} = 1\,.$$

To obtain $\theta(\tau, F)$, we must consider the effect of units of F. Let

$$E^+ = \{\varepsilon \in \mathcal{O}_F | \varepsilon\text{: totally positive units}\}\,,$$
$$E_0 = \{\varepsilon \in E^+ | \varepsilon \equiv 1 \bmod f(K/F)\}\,.$$

Put $e = [E^+ : E_0]$ and $B_i = N_{F/Q}(\mathfrak{b}_i)$. Then

$$\theta(\tau, F) = e^{-1} \sum_{i=1}^{h(F)} \{\sum_{\mu_1} (s/p)(-1)^{(s-1)/2+t} q^{(s^2-4pt^2)/B_i^2} + \sum_{\mu_2} (s/p)(-1)^{(s-1)/2} q^{(s^2-pt^2)/4B_i^2}\}\,,$$

where the summation with respect to μ_1 (resp. μ_2) is over all representatives mod E_0 of the set of totally positive elements of $\mathfrak{b}_i^2$ such that $\mu_1 = s + 2t\sqrt{p}$; $s, t \in Z$ and $s \equiv 1 \bmod 2$ (resp. $\mu_2 = \frac{1}{2}(s + t\sqrt{p})$; $s, t \in Z$, $s \equiv 1 \bmod 2$ and $N_{F/Q}(\mu_2) \equiv 1 \bmod 4$).

Let ℓ be a prime number. Then we have

$$\begin{aligned}(-1/\ell) = (p/\ell) = 1 &\Longleftrightarrow \ell \text{ splits completely in } L \\ &\Longleftrightarrow a(\ell) = \pm 2 ;\end{aligned}$$

Furthermore

$$\ell \text{ splits completely in } K \Longleftrightarrow a(\ell) = 2 .$$

(See Corollary 2 of Section 3 in the present paper).

Consequently we have

THEOREM 1. *Let $p \equiv 5 \bmod 8$ and keep the notation as above. Then*

(i) *$\theta(\tau, K)$ is a new form of weight one, with character $\varepsilon(n) = (-1/n)$ on the group $\Gamma_0(16p^2)$;*

(ii) *For a prime number ℓ such that $(-1/\ell) = (p/\ell) = 1$,*

$$(p/\ell)_4 = \tfrac{1}{2}a(\ell) ;$$

(iii) *$\theta(\tau, K)$ has the following three expressions:*

$$\begin{aligned}\theta(\tau, K) &= \frac{1}{2}\sum_{i=1}^{h(E)/2} \sum_{\substack{a \not\equiv b \bmod 2 \\ a + b\sqrt{-p} \in \mathfrak{a}_i^2}} (-1)^b (a/p) q^{(a^2 + pb^2)/A_i^2} \\ &= \frac{1}{2}\sum_{x, y} (x + sy/p)(x^2 + y^2/p)_4 q^{x^2 + y^2} \\ &= e^{-1} \sum_{i=1}^{h(F)} \{\sum_{\mu_1} (s/p)(-1)^{(s-1)/2 + t} q^{(s^2 - 4pt^2)/B_i^2} \\ &\qquad + \sum_{\mu_2} (s/p)(-1)^{(s-1)/2} q^{(s^2 - pt^2)/4B_i^2}\} .\end{aligned}$$

Especially from the second expression of $\theta(\tau, K)$ in (iii), we obtain a reciprocity law of quartic residue:

COROLLARY 1. *Let ℓ be a prime number such that $(-1/\ell) = (p/\ell) = 1$. Put $\ell = x^2 + y^2$ with $x \equiv 1 \bmod 2$. Then*

$$(p/\ell)_4 = (x + sy/p)(\ell/p)_4 .$$

To avoid diffuseness, for other primes, we shall state only the results corresponding to (iii) in the next Remarks.

Remark 1. Let $p = 2$ or 3. Then $\theta(\tau, K)$ is expressed as follows.

$(p=2)$

$$\begin{aligned}\theta(\tau, K) &= \tfrac{1}{2}\vartheta_4(16\tau)\vartheta_3(16\tau) = \sum_{a,b}(-1)^a q^{(4a+1)^2+8b^2} && \text{(via } E) \\ &= \tfrac{1}{2}\vartheta_2(8\tau)\vartheta_0(32\tau) = \sum_{x,y}(-1)^y q^{(4x+1)^2+16y^2} && \text{(via } k) \\ &= \vartheta_+(16\tau, 1, \mathcal{O}_F, 4\sqrt{2}) + \vartheta_+(16\tau, 3, \mathcal{O}_F, 4\sqrt{2}) \\ &= \sum_{s>6|t|}(-2/s)q^{s^2-32t^2} && \text{(via } F),\end{aligned}$$

where ϑ_0, ϑ_2, ϑ_3 and ϑ_4 are theta series defined by

$$\vartheta_0(\tau) = \sum_n (-1)^n \exp(\pi\sqrt{-1}n^2\tau),\ \vartheta_2(\tau) = \sum_{n\equiv 1 \bmod 2} \exp(\pi\sqrt{-1}n^2\tau/4),$$
$$\vartheta_3(\tau) = \sum_n \exp(\pi\sqrt{-1}n^2\tau),\ \vartheta_4(\tau) = \sum_n (2/n)\exp(\pi\sqrt{-1}n^2\tau/8)$$

and ϑ_+ denotes the Hecke indefinite theta series (see [3]).

$(p=3)$

$$\begin{aligned}\theta(\tau, K) &= \eta(24\tau)\vartheta_3(24\tau) = \sum_{a,b}(-1)^a q^{(6a+1)^2+12b^2} && \text{(via } E) \\ &= \sum_{x,y}(-1)^y q^{(6x+1)^2+12y^2} + \sum_{x,y}(-1)^{x+1} q^{4(3x+1)^2+9(2y+1)^2} && \text{(via } k) \\ &= \vartheta_+(24\tau, 1, \mathcal{O}_F, 4\sqrt{3}) - \vartheta_+(24\tau, 7+2\sqrt{3}, \mathcal{O}_F, 4\sqrt{3}) \\ &= \sum_{s>4|t|}(s/6)(-1)^t q^{s^2-12t^2} && \text{(via } F),\end{aligned}$$

where $\eta(\tau)$ is the Dedekind eta function.

Remark 2. Let $p\equiv 3 \bmod 4$ or $p \equiv 1 \bmod 8$. Keep the notation as above. Let $\{\mathfrak{a}_i\}$ (resp. $\{\mathfrak{b}_i\}$) be the set of the integral ideals of E (resp. F) such that $\{[\mathfrak{a}_i]^2\}$ (resp. $\{[\mathfrak{b}_i]^2\}$) represent all square classes in H_E/P_E (resp. H_F/P_F). Put $A_i = N_{E/Q}(\mathfrak{a}_i)$ and $B_i = N_{F/Q}(\mathfrak{b}_i)$. Then we have the following expressions of $\theta(\tau, K)$.

$(p\equiv 3 \bmod 4)$

$$\begin{aligned}\theta(\tau, K) &= \sum_{i=1}^{h(E)}\{\sum_{\omega_1}(-1)^b(a/p)q^{(a^2+4pb^2)/A_i^2}\} \\ &\quad + \begin{cases} 0 & \text{if } p\equiv 7 \bmod 8, \\ \sum_{i=1}^{h(E)}\sum_{\omega_2}(-1)^{(N_{E/Q}(\omega_2)+3)/4}(a/p)q^{(a^2+pb^2)/4A_i^2} & \text{otherwise;}\end{cases} \\ &= \sum_{\lambda}\{x+\sqrt{-1}y/p\}_4(-1)^{y/2}q^{x^2+y^2} \\ &= e^{-1}\sum_{i=1}^{h(F)/2}\{\sum_{\mu_1}(a/p)(-1)^{t/2}q^{(s^2-pt^2)/B_i^2} \\ &\qquad\qquad + \sum_{\mu_2}(s/p)(-1)^{s/2}q^{(s^2-pt^2)/B_i^2}\},\end{aligned}$$

where $\{x+\sqrt{-1}y/p\}_4$ denotes a cyclic character of $(\mathcal{O}_k/p)^\times$ of order 4 and the summations are as follows:

$\sum\limits_{\omega_1}$: $\omega_1 = a + 2b\sqrt{-p} \in \mathfrak{a}_i^2$, $a+2b \equiv 1 \bmod 4$;

$\sum\limits_{\omega_2}$: $\omega_2 = \frac{1}{2}(a + b\sqrt{-p}) \in \mathfrak{a}_i^2$, $a \equiv 3 \bmod 4$;

$\sum\limits_{\lambda}$: $\lambda = x + \sqrt{-1}y$, $x \equiv 1 \bmod 4$, $y \equiv 0 \bmod 2$, $(x^2 + y^2/p) = 1$;

$\sum\limits_{\mu_1}$ (resp. $\sum\limits_{\mu_2}$): μ_1 (resp. μ_2) runs over all representatives mod E_0 of the set of totally positive elements $s + t\sqrt{p} \in \mathfrak{b}_i^2$ such that $s \equiv 1$, $t \equiv 0$ (resp. $s \equiv 0$, $t \equiv 1$) mod 2.

($p \equiv 1 \bmod 8$)

Let $\mathfrak{p}_2$ be a prime ideal of F over 2. Put

$$E_0' = \{u \in E^+ | u \equiv 1 \bmod \mathfrak{p}_2^3(\sqrt{p})\}.$$

Let $e' = [E^+ : E_0']$. Take $s \in \boldsymbol{Z}$ such that $s^2 \equiv -1 \bmod p$. Then

$$\begin{aligned}\theta(\tau, K) &= \frac{1}{2}\sum_{i=1}^{h(F)/2}\sum_{\omega}(-1)^b(a/p)q^{(a^2+pb^2)/A_i^2}\\ &= \frac{1}{4}\sum_{\lambda}(x+sy/p)(x^2+y^2/p)_4 q^{x^2+y^2}\\ &= e'^{-1}\sum_{i=1}^{h(F)}\Big\{\sum_{\mu_1}(-1)^{(s-t-1)/2}(s/p)q^{(s^2-pt^2)/B_i^2}\\ &\qquad + \sum_{\mu_2}(-1)^{(s-t-2)/4}(-1)^{(p-1)/8}(s/p)q^{(s^2-pt^2)/4B_i^2}\Big\},\end{aligned}$$

where the summations are as follows;

$\sum\limits_{\omega}$: $\omega = a + b\sqrt{-p} \in \mathfrak{a}_i^2$, $a \not\equiv b \bmod 2$;

$\sum\limits_{\lambda}$: $\lambda = x + \sqrt{-1}y$, $(x^2 + y^2/p) = 1$;

$\sum\limits_{\mu_1}$ (resp. $\sum\limits_{\mu_2}$): μ_1 (resp. μ_2) runs over all representatives mod E_0' of the set of totally positive integers such that $\mu_1 = s + t\sqrt{p}$ (resp. $\mu_2 = \frac{1}{2}(s + t\sqrt{p})) \in \mathfrak{b}_i^2$ and $s \equiv t+1 \bmod 2$ (resp. $s \equiv 1 \bmod 2$ and $s - t - 2 \equiv 0 \bmod 4$).

§ 3. Higher reciprocity law

Let the notation be as in Section 2. Consider the polynomial $f(x) = x^4 - m$. Then the cusp form $\theta(\tau, K)$ has close relation to the decomposition law of $K/\boldsymbol{Q}$ and the "higher reciprocity law[3]" of $f(x)$. We shall

3) For the higher reciprocity law, see Hiramatsu [2] and Moreno [5].

explain these properties of $\theta(\tau, K)$. To this purpose, let us consider the expression of $\theta(\tau, K)$ in (4), for $M = k$. Since ξ_k is primitive we obtain

$$(8) \qquad \theta(\tau, K) = \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_k \\ [\mathfrak{a}] \in C_k(L)}} \chi_k(\mathfrak{a}) q^{N_{k/Q}(\mathfrak{a})}$$

Let $m = 2^{e(2)} m_1$, $(m_1, 2) = 1$. Put

$$(9) \qquad m_1^* = \prod_{p \mid m_1} p .$$

Then the conductor $F(K/k)$ of K over k is given in the next Table 3.

$e(2)$	1, 3	0			2		
$m_1 \bmod 8$		1	5	3, 7	1, 5	3	7
$F(K/k)$	$8m_1^*$	m_1^*	$2m_1^*$	$4m_1^*$	$4m_1^*$	$2m_1^*$	m_1^*

Table 3.

Let f be the positive integer such that $F(K/k) = (f)$. Then the level N of $\theta(\tau, K)$ is given by

$$(10) \qquad N = 4f^2 .$$

Now the decomposition law of $K/\boldsymbol{Q}$ is described by $\theta(\tau, K)$ as follows.

PROPOSITION 1. *Let p be a prime number not dividing f. Denote by f_p the relative degree of the prime ideals of K over p. Then the following assertions hold;*

(i) *If $p \equiv 1 \bmod 4$, then*

$$f_p = 1 \Longleftrightarrow a(p) = 2 ;$$
$$f_p = 2 \Longleftrightarrow a(p) = -2 ;$$
$$f_p = 4 \Longleftrightarrow a(p) = 0 .$$

(ii) *If $p \equiv 3 \bmod 4$, then $a(p) = 0$, $f_p = 2$ or 4. Further*

$$f_p = 2 \Longleftrightarrow a(p^2) = 1 ;$$
$$f_p = 4 \Longleftrightarrow a(p^2) = -1 .$$

(iii) *If $p = 2$, then $f_p = 1$ or 2. Further*

$$f_p = 1 \Longleftrightarrow a(p) = 1 ;$$
$$f_p = 2 \Longleftrightarrow a(p) = -1 .$$

Proof. Let $\mathfrak{P}$ be a prime ideal of k over p and $f_{\mathfrak{P}}$ the relative degree of $\mathfrak{P}$. Denote by $\mathfrak{P}'$ the conjugate ideal of $\mathfrak{P}$. Since $G(K/k)$ is cyclic, it is easy to see

$$[\mathfrak{P}] \in C_k(L) \text{ (resp. } C_k(K)) \Longleftrightarrow \mathfrak{P} \text{ splits completely in } L \text{ (resp. } K)$$
$$\Longleftrightarrow f_p/f_{\mathfrak{P}} = 1 \text{ or } 2 \text{ (resp, } f_p/f_{\mathfrak{P}} = 1) ;$$
$$[\mathfrak{P}] \notin C_k(L) \Longrightarrow [\mathfrak{P}] \neq [\mathfrak{P}'] .$$

From this, for a prime p such that $p = 2$ or $p \equiv 3 \bmod 4$ we have

$$[\mathfrak{P}] \in C_k(L) \text{ and } f_p/f_{\mathfrak{P}} = 1 \text{ or } 2 .$$

Therefore our assertions are deduced immediately from (8). q.e.d.

COROLLARY 2. *Let p be a prime number such that $(-1/p) = (m/p) = 1$. Then*

$$(m/p)_4 = \tfrac{1}{2} a(p) .$$

Next we shall treat the higher reciprocity law of $f(x)$. Consider all irreducible representations of G and they are listed below.

	σ	ρ
ψ_0	1	1
ψ_1	1	-1
ψ_2	-1	1
ψ_3	-1	-1
ψ	$\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

Table 4.

Let χ be the character of ψ. For a prime number p unramified at K ($\Longleftrightarrow p \nmid N$), denote by σ_p the Frobenius substitution of p. Then

$$\begin{aligned} &\psi_1(\sigma_p) = (-1/p) , \qquad \psi_2(\sigma_p) = (m_0/p) , \\ &\psi_3(\sigma_p) = (-m_0/p) , \qquad \chi(\sigma_p) = a(p), \end{aligned} \tag{11}$$

where m_0 is the square free part of m:

$$m_0 = \prod_{e(p):\ \mathrm{odd}} p .$$

For a prime number p, put

$$S(p) = \# \{a \in \boldsymbol{F}_p | f(a) \equiv 0 \bmod p\} .$$

Then we have

PROPOSITION 2. *Let p be a prime number not dividing N. Then*

$$\begin{aligned} S(p) &= 1 + a(p) + (m_0/p) \\ &= a(p) + a(p^2) - (-m_0/p)\,. \end{aligned}$$

Proof. Put $H = \langle \rho \rangle$. Then H is the subgroup of G corresponding to the subfield $\boldsymbol{Q}(\sqrt[4]{m})$. Let 1_H be the identity character of H and ν its induced character of G. Let $d(f)$ be the discriminant of $f(x)$. Then N and $d(f)$ have the same prime divisors. Therefore we obtain for $p \nmid N$,

$$\nu(\sigma_p) = S(p)\,.$$

Computing inner product of ν with all irreducible characters of G, we have

$$\begin{aligned} (\nu|\psi_i) &= \begin{cases} 0 & \text{if } i = 1, 3\,, \\ 1 & \text{otherwise}\,; \end{cases} \\ (\nu|\chi) &= 1\,. \end{aligned}$$

Therefore

$$\nu = \psi_0 + \psi_2 + \chi\,.$$

It follows from (11) that

$$S(p) = 1 + (m_0/p) + a(p)\,.$$

In view of (2), we obtain (§ 3.3 of Shimura [7])

$$a(p)^2 = a(p^2) + (-1/p)\,.$$

On the other hand, by (11) we see

$$a(p)^2 = \chi(\sigma_p^2) + 2(-1/p)\,.$$

Therefore

$$a(p^2) = \chi(\sigma_p^2) + (-1/p)\,.$$

Since the correspondence: $g \rightarrow \chi(g^2)$ is a class function of G, by computing inner products with irreducible characters of G, we have

$$\chi(\sigma_p^2) = 1 - (-1/p) + (m_0/p) + (-m_0/p)\,.$$

From this we have

$$a(p^2) = 1 + (m_0/p) + (-m_0/p); \quad S(p) = a(p) + a(p^2) - (-m_0/p).$$

q.e.d.

Let $\mathrm{Spl}\{f(x)\}$ be the set of all primes p such that $f(x) \bmod p$ factors into a product of distinct linear polynomials over $\boldsymbol{F}_p$. Then we have

PROPOSITION 3. (Higher Reciprocity Law of $f(x)$). *Let p be a prime number not dividing N. Then*

$$p \in \mathrm{Spl}\{f(x)\} \Longleftrightarrow a(p) = 2.$$

Proof. This is obvious from Propositions 1 and 2.

§4. Elliptic curves and cusp forms of weight one

Let the notation be as in preceding sections. Consider the elliptic curve E over $\boldsymbol{Q}$ defined by

$$E\colon y^2 = x^3 + 4mx.$$

Then E has a complex multiplication J such that

$$J(P) = (-x, -\sqrt{-1}y), \tag{12}$$

for all points $P = (x, y)$ on E.

Since $J^2 = -1_E$, the subalgebra $\mathcal{O}$ generated by J over $\boldsymbol{Z}$ is identified with the maximal order $\mathcal{O}_k$ of $k = \boldsymbol{Q}(\sqrt{-1})$. Denote the L-function of E by

$$L(s, E) = \sum_{n=1}^{\infty} c(n)n^{-s}.$$

Let $c(E)$ be the conductor of E. Further put

$$\vartheta(\tau, E) = \sum_{n=1}^{\infty} c(n)q^n.$$

Since E has complex multiplications, we know $\vartheta(\tau, E)$ is a cusp form of weight 2, with trivial character on the group $\Gamma_0(c(E))$ (Shimura [8]). In this section we shall show that the cusp form $\theta(\tau, K)$ of weight one is associated with the cusp form $\vartheta(\tau, E)$ of weight 2 under a congruent relation. At first we determine the conductor $c(E)$. Since E has complex multiplications it is easy to see that $c(E)$ takes the form

$$c(E) = 2^x 3^y m_2^2,$$

where $x, y \in Z$ and m_2 is the product of all prime divisors of m which are prime to 6. Let $e(2)$ and $e(3)$ be the 2-exponent and 3-exponent of m respectively. Then by Tate's argorithm in Tate [10], we know $y = 0$ or 2 according to $e(3) = 0$ or not. Further x are as follows.

$e(2)$	0		1	2		3
$m_1 \bmod 4$	1	3		1	3	
x	5	6	8	6	5	8

Table 5.

Let m_1^* be the integer defined by (9). Then we have from this

$$c(E) = 2^x m_1^{*2} .$$

Therefore it follows from Tables 3 and 5 that the level $c(E)$ of $\vartheta(\tau, E)$ equals to the level N of $\theta(\tau, K)$ up to a power of 2 and that $c(E) = N$ if $e(2)$ is odd. For a prime number p not dividing $c(E)$, denote by E_p the reduction of E mod p. Then E_p is again an elliptic curve with complex multiplications $\mathcal{O}_k$. Let $\mathfrak{Q} = (1 + \sqrt{-1})$ be the prime ideal of k dividing 2. Denote by $E(n)$ (resp. $E_p(n)$) the group of $\mathfrak{Q}^n$-division points of E (resp. E_p). Then

$$E(2) = \{(x, 0) | x^3 + 4mx = 0\} \cup \{0_E\} ,$$
$$E(3) = \{(x, y) | (x^2 - 4mx)(x^2 - 4m) = 0, y^2 = x^3 + 4mx\} \cup \{0_E\} ,$$

where 0_E denotes the identity element of the group structure on E. From this we obtain

(13) $$P = (x, y) \in E(3) - E(2) \Longleftrightarrow x^2 - 4m = 0 .$$

Further K is generated over $\boldsymbol{Q}$ by all $\mathfrak{Q}^3$-division points of E. Denote by N_p and $T(p)$ the number of F_p-rational points of E_p and $E_p(3)$ respectively. Then we have following Proposition.

PROPOSITION 4. *Keep the notations as above. Let*

$$\mu(p) = \{1 - (-1/p)\}\{1 + (2/p)\}.$$

Then

(i) $T(p) = S(p) + (-m_0/p) + 3$;

(ii) $N_p \equiv T(p) + \mu(p) \bmod 8$.

Proof. Let M (resp. $M(n)$) be the subset of F_p-rational points of E_p (resp. $E_p(n) - E_p(n-1)$). Let

$$\Lambda = \{a \in \boldsymbol{F}_p | f(a) \equiv 0 \bmod p\}.$$

For $p \nmid 2m$, by (13) we have a bijection φ of Λ to $M(3)$ defined by

$$\varphi(a) = (2a^2, 4a^3), \qquad a \in \Lambda.$$

Therefore

$$S(p) = |\Lambda| = |M(3)|.$$

Further it is easy to see

$$|M(2)| = 1 + (-m_0/p), \qquad |M(1)| = 2.$$

Hence

$$T(p) = |M(3)| + |M(2)| + |M(1)| = S(p) + (-m_0/p) + 3.$$

This shows (i). Next we shall prove (ii). The following is easily obtained:

$$(14) \qquad S(p) = \begin{cases} 4 & \text{if } (-1/p) = (m/p)_4 = 1, \\ 2 & \text{if } (-1/p) = -1 \text{ and } (m/p)_4 = 1, \\ 0 & \text{otherwise}. \end{cases}$$

Let $p \equiv 3 \bmod 4$. Then it follows from (14) and (i) just proved that

$$T(p) \equiv 4 \bmod 8.$$

On the other hand it is easily obtained

$$N_p = p + 1.$$

Therefore

$$N_p \equiv T(p) + \mu(p) \bmod 8.$$

Let $p \equiv 1 \bmod 4$. Then by (12), the endomorphism J_p of E_p induced by J is defined over F_p. Let U be the subgroup of $\mathrm{Aut}_{F_p}(E_p)$ generated by J_p. Then U is a cyclic group of order 4 and M becomes a U-module. Let $P \in M$ and denote by $O(p)$ the U-orbit of P. Then we have

$$(15) \qquad |O(P)| = \begin{cases} 1 & \text{if } P \in M(1), \\ 2 & \text{if } P \in M(2), \\ 4 & \text{otherwise}. \end{cases}$$

Let

$$M^* = \bigcup_{n=1}^{\infty} M(n), \qquad M^{**} = \{x \in M | \text{order of } x \text{ is odd}\}.$$

Then M^* and M^{**} become U-modules and $M = M^* \oplus M^{**}$. From (15) we know

$$|M^{**}| \equiv 1 \bmod 4. \tag{16}$$

Let t be the largest integer such that $M^* \supseteqq E_p(t)$. If there exists an element P of $M(3)$, then it follows from (15) that

$$|M(3)| = 4, \qquad |M(2)| = 2.$$

This implies that $t \geqq 3$. Therefore

$$\begin{aligned} |M^*| = 2 &\Longleftrightarrow t = 1 \Longleftrightarrow T(p) = 2; \\ |M^*| = 4 &\Longleftrightarrow t = 2 \Longleftrightarrow T(p) = 4; \\ |M^*| \equiv 0 \bmod 8 &\Longleftrightarrow t \geqq 3 \Longleftrightarrow T(p) = 8. \end{aligned}$$

Hence by (16).

$$N_p = |M^*| \cdot |M^{**}| \equiv T(p) \bmod 8. \qquad \text{q.e.d.}$$

Consider the L-function $L(s, E)$ of E. Since E has complex multiplications, the Euler product and p-th coefficient $c(p)$ of $L(s, E)$ are as follows (Tate [9]):

$$\begin{aligned} L(s, E) &= \prod_{p \nmid c(E)} (1 - c(p)p^{-s} + p^{1-2s})^{-1}, \\ c(p) &= \begin{cases} 1 + p - N_p & \text{if } p \nmid c(E), \\ 0 & \text{otherwise}. \end{cases} \end{aligned} \tag{17}$$

Furthermore we have

PROPOSITION 5. *Let p be a prime number such that $p \nmid c(E)$. Let $\gamma(p) = \{1 + (-1/p)\}\{1 - (2/p)\}$. Then*

$$c(p) \equiv a(p) + \gamma(p) \bmod 8.$$

Proof. Let ρ_G denote the character of the regular representation of G. Then

$$\rho_G = 1 + \psi_1 + \psi_2 + \psi_3 + 2\chi.$$

Since G is of order 8, for all $g \in G$ we have

$$\rho_G(g) \equiv 0 \bmod 8.$$

In this congruent equation, put $g = \sigma_p$ for $p \nmid c(E)$, then by (11),

$$2a(p) + 1 + (m_0/p) + (-m_0/p) + (-1/p) \equiv 0 \bmod 8.$$

On the other hand, Propositions 2 and 4 imply

$$c(p) \equiv -a(p) - \mu(p) + p - 2 - \{1 + (m_0/p) + (-m_0/p)\} \bmod 8 .$$

Thus

$$c(p) \equiv a(p) - \mu(p) + p - 2 + (-1/p) \bmod 8 .$$

It is easy to see

$$\gamma(p) \equiv p - 2 - \mu(p) + (-1/p) \bmod 8 .$$

Therefore

$$c(p) \equiv a(p) + \gamma(p) \bmod 8 . \qquad \text{q.e.d.}$$

Note that $a(p) = 0$ if $p|f$, $c(p) = 0$ if $p|c(E)$, and $\gamma(p) \equiv 0 \bmod 4$. Further it follows from Tables 3 and 5 that $c(E)/f$ is a power of 2. Therefore we have:

COROLLARY 3. *Let p be an odd prime. Then*

$$a(p) \equiv c(p) \bmod 4 .$$

Furthermore, if f is even, then

$$a(2) \equiv c(2) \bmod 4 .$$

It follows from (2) and (17) that Fourier coefficients $a(n)$ and $c(n)$ are both multiplicative. Therefore we know that $a(n) \equiv c(n) \bmod 4$, if n is odd and that $c(n) \equiv 0 \bmod 4$ if n is even. Let

$$\theta'(\tau, K) = \sum_{n:\ \mathrm{odd}} a(n) q^n .$$

Then $\theta'(\tau, K)$ is a cusp form of weight one, with character ε' on the group $\Gamma_0(4N)$, where ε' is a character mod $4N$ induced by ε (Lemma 2 in Shimura [8]). Consequently we obtain the next Theorem.

THEOREM 2. *Keep the notation as above. Then*

$$\theta'(\tau, K) \equiv \vartheta(\tau, E) \bmod 4 .$$

If f is even, we have further

$$\theta(\tau, K) \equiv \vartheta(\tau, E) \bmod 4 .$$

Remark 3. The number of rational points N_p is computed as follows. For $p \nmid c(E)$,

$$N_p = \begin{cases} p+1 & \text{if } p \equiv 3 \bmod 4\,, \\ p+1-\bar{\pi}(-4m/\pi)_4 - \pi(-4m/\bar{\pi})_4 & \text{otherwise}\,, \end{cases}$$

where π and $\bar{\pi}$ are prime elements of $k = \boldsymbol{Q}(\sqrt{-1})$ such that $p = \pi \cdot \bar{\pi}$ and $\pi \equiv 1 \bmod (2 + 2\sqrt{-1})$ (Davenport and Hasse [1]). From this it is comparatively easy to deduce Proposition 4 and Theorem 2. However we could attain to Theorem 2, without using this result, along the following process:

$$c(p) \longrightarrow N_p \longrightarrow T(p) \longrightarrow S(p) \longrightarrow a(p)\,.$$

REFERENCES

[1] H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, J. reine u. angew. Math., **172** (1934), 151–182.

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

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

[4] M. Koike, Higher reciprocity law, modular forms of weight 1 and elliptic curves, Nagoya Math. J., **98** (1985),

[5] C. Moreno, The higher reciprocity law: an example, J. Number Theory, **12** (1980), 57–70.

[6] J. P. Serre, Modular forms of weight one and Galois representations, Proc. Symposium on Algebraic Number Fields, Academic Press, London, 1977, 193–268.

[7] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten Publisher and Princeton Univ. Press, 1971.

[8] ——, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, Nagoya Math. J., **43** (1971), 199–208.

[9] J. Tate, The arithmetic of elliptic curves, Invent. Math., **23** (1974), 179–206.

[10] ——, Algorithm for determining the type of a singular fiber in an elliptic pencil, Lecture Notes in Math., **476** (1975), 33–52.

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