J. Math. Soc. Japan
Vol. 43, No. 3, 1991

Dedekind sums and quadratic residue symbols of imaginary quadratic fields

By Hiroshi ITO

(Received July 10, 1990)

§ 1. Introduction.

Let K be an imaginary quadratic field embedded in the complex number field $\boldsymbol{C}$ and $\mathcal{O}_K$ its ring of integers. Consider the subgroup $\Gamma(8)$ of $SL(2, \mathcal{O}_K)$ consisting of all matrices congruent to $\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$ modulo 8. As was noticed by Kubota [7], the map $\chi: \Gamma(8) \to \boldsymbol{Z}/2\boldsymbol{Z}$ defined by

$$\chi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} \frac{1}{2}\left(1-\left(\frac{c}{a}\right)\right), & c \neq 0 \\ 0, & c=0 \end{cases}$$

is a homomorphism, the homomorphic property being essentially equivalent to the reciprocity law of the quadratic residue symbol (c/a) of K. On the other hand, by a result of Sczech [10], we have homomorphisms from $\Gamma(8)$ to the additive group of $\boldsymbol{C}$ explicitly given by generalized Dedekind sums. The aim of this paper is to study the relation between these two kinds of homomorphisms. The main result is that there exists, among the linear combinations of Sczech's homomorphisms, a homomorphism Ψ with values in the ring $\boldsymbol{Z}$ of rational integers such that

$$\chi(A) \equiv \Psi(A) \pmod 2 \tag{1}$$

for every $A \in \Gamma(8)$. This was conjectured in [10].

To be more specific, let L be a lattice in $\boldsymbol{C}$ and denote by $\mathcal{O}_L$ the ring consisting of all m in $\boldsymbol{C}$ with $mL \subset L$. Let, for z in $\boldsymbol{C}$ and a non-negative integer n,

$$E_n(z) = \sum_{\substack{w \in L \\ w+z \neq 0}} (w+z)^{-n} |w+z|^{-s}|_{s=0},$$

where the value at $s=0$ is to be understood in the sense of analytic continuation. Put, for two integers a, c in $\mathcal{O}_L$ with $c \neq 0$,

$$D(a, c) = \frac{1}{c} \sum_{m \in L/cL} E_1\left(\frac{am}{c}\right) E_1\left(\frac{m}{c}\right)$$

and define the map $\Phi=\Phi_L$ from $SL(2, \mathcal{O}_L)$ to $\boldsymbol{C}$ by

$$\Phi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{cases} E_2(0)I\left(\dfrac{a+d}{c}\right)-D(a, c), & c\neq 0 \\ E_2(0)I\left(\dfrac{b}{d}\right), & c=0 \end{cases},$$

with $I(z)=z-\bar{z}$. It is proved in [**10**] that

$$\Phi(AB)=\Phi(A)+\Phi(B), \qquad A, B\in SL(2, \mathcal{O}_L),$$

i.e., Φ is a homomorphism. The following is our main theorem.

THEOREM 1. *Among the linear combinations of the homomorphisms Φ_L associated with lattices L such that $\mathcal{O}_L$ is the order of K with conductor* 8, *there exists a $\boldsymbol{Z}$-valued homomorphism Ψ which satisfies* (1) *for every A in $\Gamma(8)$.*

By a general result of Harder (cf. [**3**]), the first cohomology group $H^1(\Gamma(8), \boldsymbol{C})$ of $\Gamma(8)$, which is nothing else than the $\boldsymbol{C}$-vector space of all homomorphisms from $\Gamma(8)$ to $\boldsymbol{C}$, has a canonical decomposition

$$H^1(\Gamma(8), \boldsymbol{C}) = H^1_{\text{Eis}}(\Gamma(8), \boldsymbol{C})\oplus H^1_{\text{cusp}}(\Gamma(8), \boldsymbol{C})$$

into the Eisenstein part and the cusp part. If $\mathcal{O}_L$ is the order in K with conductor 8, the restriction of Φ_L to $\Gamma(8)$ belongs to the Eisenstein part (cf. Weselmann [**13**]). Our theorem, therefore, says that $\chi: \Gamma(8)\to \boldsymbol{Z}/2\boldsymbol{Z}$ has a 'lift' $\Psi: \Gamma(8)\to \boldsymbol{Z}$ in the Eisenstein part.

In the following we first prepare congruences for the division values of elliptic functions (§ 2). Then our result is obtained by the help of a lemma (Lemma 6) which is a version of the so-called Gauss' lemma. The case where the discriminant of K is congruent to one modulo 8 is essentially treated in [**5**]. There is a similar result for the cubic residue symbol of $\boldsymbol{Q}(\sqrt{-3})$ ([**6**]). For the relation between classical Dedekind sums and the quadratic residue symbol of the rational number field $\boldsymbol{Q}$, we refer the readers to Rademacher and Grosswald [8] and Sczech [**11**].

The author would like to thank Sonderforschungsbereich 170 at Göttingen for financial support and accommodation during the preparation of this work.

§ 2. Congruences satisfied by division values of elliptic functions.

The purpose of this section is to get two corollaries of Theorem 2. First we quote some known facts (cf. Cassou-Noguès and Taylor [**1**], Fueter [**2**]). Keeping the notation introduced in the previous section, take a 4-division point ψ of $\boldsymbol{C}/L$ with $2\psi\neq 0$ and put

$$t = t_L(\phi) = \frac{12\mathfrak{P}(2\phi)}{\mathfrak{P}(\phi)-\mathfrak{P}(2\phi)},$$

$$T(z) = T_L(z\,;\phi) = \frac{\mathfrak{P}(\phi)-\mathfrak{P}(2\phi)}{\mathfrak{P}(z)-\mathfrak{P}(2\phi)},$$

where $\mathfrak{P}(z)$ denotes the Weierstrass $\mathfrak{P}$-function with respect to L.

LEMMA 1 ([2], p. 99). *For every odd integer n greater than one, the polynomial*

$$\prod_{\alpha\in n^{-1}L/L-\{0\}}(X-T(\alpha))$$

has coefficients in $\boldsymbol{Z}[t]$ and the constant term is n^2.

The value $t_L(\phi)^2$ depends only on L and 2ϕ and hence we may put

$$s_L(2\phi) = t_L(\phi)^2-2^6. \tag{2}$$

For (u, v) in $(\boldsymbol{Z}/2\boldsymbol{Z})^2-\{(0, 0)\}$ and a variable τ in the upper half plane $\boldsymbol{H}$, let

$$s_{(u,v)}(\tau) = s_{L_\tau}\left(\frac{u\tau+v}{2}\right)$$

with $L_\tau=\boldsymbol{Z}\tau+\boldsymbol{Z}$.

LEMMA 2 (cf. [1]). *One has*

$$s_{(1,0)}(\tau) = \frac{\Delta\left(\frac{\tau}{2}\right)}{\Delta(\tau)}, \qquad s_{(1,1)}(\tau) = \frac{\Delta\left(\frac{\tau+1}{2}\right)}{\Delta(\tau)}, \tag{3}$$

$$s_{(0,1)}(\tau) = 2^{12}\frac{\Delta(2\tau)}{\Delta(\tau)}$$

with

$$\Delta(\tau) = e^{2\pi i\tau}\prod_{n=1}^{\infty}(1-e^{2\pi in\tau})^{24}$$

and

$$s_{(1,0)}(\tau)s_{(1,1)}(\tau)s_{(0,1)}(\tau) = -2^{12}. \tag{4}$$

Furthermore, for every A in $SL(2, \boldsymbol{Z})$,

$$s_{(u,v)}(A\tau) = s_{(u,v)A}(\tau). \tag{5}$$

Denote by $\mathcal{O}_f$ the order in K with conductor f $(0<f\in\boldsymbol{Z})$ and by H_m the maximal ray class field over K modulo m $(0\neq m\in\mathcal{O}_K)$. For a non-negative integer k, we put

$$r_k = \begin{cases} 0, & D_K\equiv 1 \pmod 8 \\ 2^{1-k}, & D_K\equiv 5 \pmod 8, \\ 3\cdot 2^{-1-k}, & D_K\equiv 0 \pmod 4 \end{cases}$$

where D_K is the discriminant of K. If a and b are algebraic integers in $\boldsymbol{C}$, we write $a\sim b$ when a/b is a unit.

LEMMA 3 ([2], pp. 202~204). *Suppose $\mathcal{O}_L=\mathcal{O}_K$ and let ϑ be a primitive 2-division point of $\boldsymbol{C}/L$. Then $s_L(\vartheta)$ is an algebraic integer of H_2 and*

$$s_L(\vartheta)\sim 2^{2r_0}.$$

LEMMA 4. *Let μ and a positive integer ν be such that $\tau_0:=\mu/\nu\in\boldsymbol{H}$, $\mathcal{O}_K=\boldsymbol{Z}\mu+\boldsymbol{Z}$ and $\mathfrak{A}=\boldsymbol{Z}\mu+\boldsymbol{Z}\nu$ is an ideal of K prime to 2. Then, for every positive integer k, $s_{(0,1)}(2^k\tau_0)$ and $s_{(1,1)}(2^k\tau_0)$ are algebraic integers in $H_{2^{k+1}}$ and*

$$s_{(0,1)}(2^k\tau_0)\sim s_{(1,1)}(2^k\tau_0)\sim 2^{2r_k}. \tag{6}$$

PROOF. We quote the following general facts from the theory of complex multiplication (cf. Stark [12], p. 217). Let g be a modular function of level N $(0<N\in\boldsymbol{Z})$ which is holomorphic on $\boldsymbol{H}$ and whose Fourier expansion at every cusp has coefficients in $\boldsymbol{Z}$. Let $\mathfrak{A}=\boldsymbol{Z}\mu+\boldsymbol{Z}\nu$ be a proper fractional $\mathcal{O}_f$-ideal $(0<f\in\boldsymbol{Z})$ with $\tau_0=\mu/\nu$ in $\boldsymbol{H}$. Then $g(\tau_0)$ is an integer of H_{fN}. Moreover, if $\mathfrak{P}$ is a prime ideal in K of degree one over a rational prime p with $(p, fND_K)=1$ and if σ denotes the Frobenius automorphism of H_{fN}/K corresponding to $\mathfrak{P}$, then one has

$$g(\tau_0)^\sigma=g(A\tau_0), \tag{7}$$

for A in $SL(2, \boldsymbol{Z})$ taken as follows. Namely let B be a 2 by 2 matix with coefficients in $\boldsymbol{Z}$ such that $B\begin{pmatrix}\mu\\ \nu\end{pmatrix}$ gives a $\boldsymbol{Z}$-basis of $\mathfrak{p}\mathfrak{a}$ with $\mathfrak{p}=\mathfrak{P}\cap\mathcal{O}_f$ and take A satisfying

$$\begin{pmatrix}p & \\ & 1\end{pmatrix}\equiv AB \pmod N.$$

Returning to the notation in Lemma 4, we have

$$\mathcal{O}_{2^k}=\boldsymbol{Z}2^k\mu+\boldsymbol{Z}$$

and

$$\mathfrak{A}\cap\mathcal{O}_{2^k}=\boldsymbol{Z}2^k\mu+\boldsymbol{Z}\nu.$$

Because the functions $s_{(0,1)}$ and $s_{(1,1)}$ satisfy the above conditions for g with $N=2$, their values at $2^k\tau_0$ are integers of $H_{2^{k+1}}$. We prove (6) by induction on k. Since $\nu/2$ gives a primitive 2-division point of $\boldsymbol{C}/\mathfrak{A}$,

$$s_{(0,1)}(\tau_0)\sim 2^{2r_0}$$

by Lemma 3. Let m be a positive integer and assume

$$s_{(0,1)}(2^{m-1}\tau_0)\sim 2^{2r_{m-1}}.$$

By (3) and (4),

$$s_{(0,1)}(\tau)s_{(1,1)}(\tau) = -s_{(0,1)}\left(\frac{\tau}{2}\right)$$

and hence

$$s_{(0,1)}(2^m\tau_0)s_{(1,1)}(2^m\tau_0) = -s_{(0,1)}(2^{m-1}\tau_0) \sim 2^{2r_{m-1}}.$$

If $D_K \equiv 1 \pmod 8$, then $r_{m-1}=0$ and we get (6) for $k=m$. We claim that $s_{(0,1)}(2^m\tau_0)$ and $s_{(1,1)}(2^m\tau_0)$ are conjugate to each other over H_1, the Hilbert class field of K. Then, because every prime ideal of H_1 over 2 ramifies completely in $H_{2^{m+1}}$ when $D_K \not\equiv 1 \pmod 8$, we get (6) for $k=m$ in this case also. This will complete the proof of Lemma 4.

To prove the above claim, take a prime ideal $\mathfrak{P}=\mathcal{O}_K\omega$ in K of degree one with $p=\omega\bar{\omega}$ prime to $2D_K$. Further suppose ω has the form

$$\omega = 2^m a\mu + b \qquad (a, b \in \boldsymbol{Z},\ a \equiv 1(2)),$$

i.e., ω belongs to $\mathcal{O}_{2^m}$ but not to $\mathcal{O}_{2^{m+1}}$. We have $\mathfrak{P}\cap\mathcal{O}_{2^m}=\mathcal{O}_{2^m}\omega$. Define the 2 by 2 integral matrix B by

$$B\begin{pmatrix} 2^m\mu \\ q \end{pmatrix} = \bar{\omega}\begin{pmatrix} 2^m\mu \\ q \end{pmatrix}.$$

One easily sees that

$$B = \begin{pmatrix} b & 2^{2m}a\mu\bar{\mu}/q \\ -aq & 2^m a(\mu+\bar{\mu})+b \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \pmod 2.$$

Hence, by (7) and (5),

$$s_{(0,1)}(2^m\tau_0)^\sigma = s_{(0,1)}\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}2^m\tau_0\right) = s_{(1,1)}(2^m\tau_0),$$

where σ is the Frobenius automorphism of $H_{2^{m+1}}/K$ corresponding to $\mathfrak{P}$. This proves our claim.

It can be seen from the above proof that, more precisely, $s_{(0,1)}(2^m\tau_0)$ and $s_{(1,1)}(2^m\tau_0)$ belong to the ring class field over K modulo 2^{m+1} and are conjugate to each other over the ring class field modulo 2^m $(m \geqq 1)$.

LEMMA 5. *Suppose $\mathcal{O}_L=\mathcal{O}_{2^k}$ with a non-negative integer k and let ϑ be a 2-division point of $\boldsymbol{C}/L$ whose image under the natural map $\boldsymbol{C}/L \to \boldsymbol{C}/\mathcal{O}_K L$ is a primitive 2-division point of $\boldsymbol{C}/\mathcal{O}_K L$. Then $s_L(\vartheta)$ is an algebraic integer of $H_{2^{k+1}}$ and*

$$s_L(\vartheta) \sim 2^{2r_k}.$$

PROOF. The case $k=0$ is just Lemma 3. Let $k \geqq 1$. Because

$$s_{\lambda L}(\lambda\xi) = s_L(\xi), \qquad 0 \neq \lambda \in \boldsymbol{C}, \qquad 0 \neq \xi \in 2^{-1}L/L,$$

we may assume that $L=\mathcal{O}_L\cap\mathfrak{Q}$ and $O_K L=\mathfrak{Q}$ with a prime ideal $\mathfrak{Q}$ of K of

degree one over a prime number q, $(q, 2D_K)=1$. We can write $\mathfrak{O}=\boldsymbol{Z}\mu+\boldsymbol{Z}q$ with μ in $\boldsymbol{H}$. Then $\mathcal{O}_K=\boldsymbol{Z}\mu+\boldsymbol{Z}$ and $L=\boldsymbol{Z}2^k\mu+\boldsymbol{Z}q$. It follows from the assumption on ϑ that

$$\vartheta \equiv \frac{q}{2}, \frac{2^k\mu+q}{2} \pmod{L}$$

and

$$s_L(\vartheta) = s_{(0,1)}(2^k\tau_0),\ s_{(1,1)}(2^k\tau_0)$$

with $\tau_0=\mu/q$. Hence the assertions follows from Lemma 4.

Denote by $\mathfrak{O}_2$ the ring consisting of all algebraic numbers in $\boldsymbol{C}$ integral at 2.

THEOREM 2. *Suppose $\mathcal{O}_L=\mathcal{O}_{2^k}$ $(k\geqq 0)$ and let ϑ be as in Lemma 5. Then, for every point $\alpha\in\boldsymbol{C}/L$, $\alpha\neq 0$ of an odd order, one has*

$$\mathcal{P}(\vartheta)^{-1}\mathcal{P}(\alpha) \equiv 1 \pmod{2^{2-r_k}\mathfrak{O}_2}.$$

PROOF. Take a 4-division point ψ of $\boldsymbol{C}/L$ with $2\psi=\vartheta$. By (2) and Lemma 5, $t=t_L(\psi)$ is a non-zero algebraic integer and

$$t^{-1} \in 2^{-r_k}\mathfrak{O}_2.$$

By Lemma 1, $T(\alpha)=T_L(\alpha;\psi)$ is an algebraic integer prime to 2. The assertion follows from

$$\frac{\mathcal{P}(\alpha)}{\mathcal{P}(\vartheta)} = 1+\frac{12}{tT(\alpha)}.$$

COROLLARY 1. *Assumptions on $\mathcal{O}_L$, ϑ and α being as in Theorem 2, one has*

$$(-\mathcal{P}(\vartheta))^{-1/2}E_1(\alpha) \equiv 1 \pmod{2^{1-r_k/2}\mathfrak{O}_2}.$$

PROOF. Denote by n the order of α. We have the following identities (cf. [10], [11]):

$$nE_1(\alpha) = \sum_{m=1}^{n-2}(E_1(m\alpha)+E_1(\alpha)-E_1((m+1)\alpha)),$$

$$(E_1(m\alpha)+E_1(\alpha)-E_1((m+1)\alpha))^2 = \mathcal{P}(m\alpha)+\mathcal{P}(\alpha)+\mathcal{P}((m+1)\alpha).$$

Note that, for an algebraic number c and a rational number x, $0\leqq x\leqq 1$, one has $c\equiv 1 \pmod{2^x\mathfrak{O}_2}$ if and only if $c^2\equiv 1 \pmod{2^{2x}\mathfrak{O}_2}$. Then, by Theorem 2,

$$(-\mathcal{P}(\vartheta))^{-1/2}(E_1(m\alpha)+E_1(\alpha)-E_1((m+1)\alpha)) \equiv 1 \pmod{2^{1-r_k/2}\mathfrak{O}_2}$$

and the assertion follows.

COROLLARY 2. *Assumptions on $\mathcal{O}_L$ and ϑ being as in Theorem 2, suppose, furthermore, $k\geqq 3$. Then one has*

$$2^k\sqrt{D}_K\mathfrak{P}(\vartheta)^{-1}E_2(0)\equiv 0 \pmod{2^{3-r_k}\mathfrak{O}_2}.$$

PROOF. For every $\mu\in\mathcal{O}_L$ with $(\mu\bar{\mu}, 2)=1$, we have (cf. [**11**], p. 102)

$$\mu I(\mu)E_2(0)=2\sum_{\substack{m\in L/\mu L-\{0\}\\ m \bmod \pm 1}}\mathfrak{P}\left(\frac{m}{\mu}\right).$$

By Theorem 2, the right hand side is congruent to $\mu\bar{\mu}-1$ modulo $2^{3-r_k}\mathfrak{O}_2$. Putting $\mu=1+2^{k-1}\sqrt{D}_K$, we get the assertion.

§3. Main result.

Throughout this section we assume that $\mathcal{O}_L=\mathcal{O}_{2^k}$ $(k\geqq 0)$ and let ϑ be a 2-division point of $\boldsymbol{C}/L$ satisfying the condition in Lemma 5. Further we adapt the convention that $(0/c)=1$ if c is a unit in K.

THEOREM 3. *For two integers a, c in $\mathcal{O}_L$ with $\mathcal{O}_K 2a+\mathcal{O}_K c=\mathcal{O}_K$, one has*

$$-c\mathfrak{P}(\vartheta)^{-1}D(a, c)\equiv c\bar{c}+1-2\left(\frac{a}{c}\right) \pmod{2^{3-r_k}\mathfrak{O}_2}.$$

PROOF. Let α be a point of $\boldsymbol{C}/L$ such that

$$\{m\in\mathcal{O}_L;\ m\alpha=0\}=c\mathcal{O}_L$$

and put

$$f(m)=(-\mathfrak{P}(\vartheta))^{-1/2}E_1(m\alpha)$$

for $m\in\mathcal{O}_L/c\mathcal{O}_L$. This satisfies

$$f(-m)=-f(m)$$

and

$$f(m)\equiv 1 \pmod{2^{1-r_k/2}\mathfrak{O}_2}, \qquad m\neq 0$$

by Corollary 1 of Theorem 2. Since $\mathcal{O}_L/c\mathcal{O}_L$ is isomorphic to $\mathcal{O}_K/c\mathcal{O}_K$, Theorem 3 follows from the next lemma.

For a finite algebraic number field M, we denote by $\mathcal{O}_M$ the integer ring of M.

LEMMA 6. *Let M be a finite algebraic number field in $\boldsymbol{C}$ and $\mathfrak{c}$ an integral ideal in M prime to 2. Suppose that a map $f:\mathcal{O}_M/\mathfrak{c}\to\boldsymbol{C}$ satisfies*

$$f(-m)=-f(m), \qquad m\in\mathcal{O}_M/\mathfrak{c}$$

and

$$f(m)\equiv 1 \pmod{2^{\beta}\mathfrak{O}_2},\ 0\neq m\in\mathcal{O}_M/\mathfrak{c}$$

with a positive rational number β. Then, for every a in $\mathcal{O}_M$ prime to $\mathfrak{c}$,

$$\sum_{m\in\mathcal{O}_M/\mathfrak{c}} f(am)f(m) \equiv N\mathfrak{c}+1-2\left(\frac{a}{\mathfrak{c}}\right)_M \qquad (\mathrm{mod}\ 2^{\gamma}\mathfrak{D}_2),$$

where $(a/\mathfrak{c})_M$ *is the quadratic residue symbol of* M, $N\mathfrak{c}$ *is the absolute norm of* $\mathfrak{c}$ *and*

$$\gamma = \min\{1+2\beta,\ 2+\beta,\ 3\}.$$

PROOF. Let R be a subset of $\mathcal{O}_M/\mathfrak{c}$ such that $R\cap(-R)$ is empty and $\mathcal{O}_M/\mathfrak{c} = R\cup(-R)\cup\{0\}$. By the conditions on f,

$$\begin{aligned}
&\sum_{m\in\mathcal{O}_M/\mathfrak{c}} f(am)f(m) - N\mathfrak{c}+1 \\
&= 2\sum_{m\in R} f(am)f(m) - N\mathfrak{c}+1 \\
&= 2\sum_{m\in R}\{(f(am)-1)(f(m)+1)+f(m)-f(am)\} \\
&\equiv 2\{\sum_{m\in R} f(m) - \sum_{m\in aR} f(m)\} \qquad (\mathrm{mod}\ 2^{1+2\beta}\mathfrak{D}_2).
\end{aligned}$$

Put

$$R_n = \{m\in R\,;\ am\in(-1)^n R\}, \qquad n=0,\ 1.$$

Then $R=R_0\cup R_1$ and $aR=R_0\cup(-R_1)$, the unions being disjoint. Hence

$$2\{\sum_{m\in R} f(m) - \sum_{m\in aR} f(m)\} = 4\sum_{m\in R_1} f(m) \equiv 4\cdot\#R_1 \qquad (\mathrm{mod}\ 2^{2+\beta}\mathfrak{D}_2),$$

where $\#R_1$ is the number of elements of R_1. A generalization of Gauss' lemma (cf. Reichardt [9]) says

$$\#R_1 \equiv \frac{1}{2}\left(1-\left(\frac{a}{\mathfrak{c}}\right)_M\right) \qquad (\mathrm{mod}\ 2).$$

This proves the lemma.

THEOREM 4. *Assume* $k\geqq 3$. *Then, for* $A=\begin{pmatrix} a & b \\ c & d\end{pmatrix}$ *in* $SL(2,\mathcal{O}_L)$ *with* $(c\bar{c},\ 2)=1$,

$$\mathfrak{P}(\vartheta)^{-1}\Phi(A) \equiv 2-2\left(\frac{a}{c}\right) \qquad (\mathrm{mod}\ 2^{3-\gamma k}\mathfrak{D}_2).$$

PROOF. Recall that $\mathcal{O}_L=\mathcal{O}_{2^k}=\boldsymbol{Z}+2^k\mathcal{O}_K$ and note that

$$I\left(\frac{a+d}{c}\right) \in 2^k\sqrt{D_K}\mathfrak{D}_2.$$

Then, by Corollary 2 of Theorem 2,

$$\mathfrak{P}(\vartheta)^{-1}E_2(0)I\left(\frac{a+d}{c}\right) \equiv 0 \qquad (\mathrm{mod}\ 2^{3-\gamma k}\mathfrak{D}_2).$$

Since $c\in 1+2\boldsymbol{Z}+8\mathcal{O}_K$ we see $c\bar{c}\equiv 1\ (\mathrm{mod}\ 8)$ and $c\equiv 1\ (\mathrm{mod}\ 2\mathfrak{D}_2)$. Therefore, by

Theorem 3,

$$c\mathfrak{P}(\vartheta)^{-1}\Phi(A) \equiv 2-2\left(\frac{a}{c}\right) \equiv c\left\{2-2\left(\frac{a}{c}\right)\right\} \pmod{2^{3-r_k}\mathfrak{O}_2}.$$

Because c is a unit of the ring $\mathfrak{O}_2$, we get the theorem.

We need a simple lemma to get a $\boldsymbol{Z}$-valued homomorphism which inherits the congruence of Theorem 4.

LEMMA 7. *Let M be a finite algebraic number field and $\mathfrak{p}$ a prime ideal in M over a prime number p. Then there exists a number μ in M such that*

$$\mathrm{Tr}(\mu) \equiv 1 \pmod{p\boldsymbol{Z}}$$

and, for every m in $\mathfrak{p}$,

$$\mathrm{Tr}(\mu m) \equiv 0 \pmod{p\boldsymbol{Z}}.$$

Here $\mathrm{Tr}(\cdot)$ denotes the trace map from M to $\boldsymbol{Q}$.

PROOF. Denote by $\mathfrak{D}_M$ the different of M. If $\mu \in \mathfrak{D}_M^{-1}p\mathfrak{p}^{-1}$, we have

$$\mathrm{Tr}(\mu m) \equiv 0 \pmod{p\boldsymbol{Z}}$$

for every m in $\mathfrak{p}$. Hence it suffices to show that

$$\mathrm{Tr}(\mathfrak{D}_M^{-1}p\mathfrak{p}^{-1}) \not\subset p\boldsymbol{Z}.$$

Suppose this be false. Then

$$\mathrm{Tr}(\mathfrak{D}_M^{-1}\mathfrak{p}^{-1}) \subset \boldsymbol{Z}$$

and, since

$$\mathfrak{D}_M^{-1} = \{a \in M;\ \mathrm{Tr}(a\mathfrak{O}_M) \subset \boldsymbol{Z}\},$$

we have

$$\mathfrak{D}_M^{-1}\mathfrak{p}^{-1} \subset \mathfrak{D}_M^{-1},$$

which is a contradiction. This concludes the proof.

Now we can prove Theorem 1. Assume $k \geqq 3$. Since $SL(2, \mathfrak{O}_L)$ is finitely generated, the field M generated over $\boldsymbol{Q}$ by all the values of $\mathfrak{P}(\vartheta)^{-1}\Phi$ is a finite algebraic number field and $\mathfrak{P}(\vartheta)^{-1}\Phi(SL(2, \mathfrak{O}_L))$ is a $\boldsymbol{Z}$-module of a finite rank. Take μ in M satisfying the conditions of Lemma 7 for a prime ideal $\mathfrak{p}$ in M over 2. Then, for every $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL(2, \mathfrak{O}_L)$ with $(c\bar{c}, 2)=1$,

$$\Psi(A) := \frac{1}{4}\mathrm{Tr}(\mu\mathfrak{P}(\vartheta)^{-1}\Phi(A)) \equiv \frac{1}{2}\left(1-\left(\frac{a}{c}\right)\right) \pmod{2\mathfrak{O}_2}$$

by Theorem 4. Multiplying μ by a suitable odd integer if necessary, we may assume that Ψ is $\boldsymbol{Z}$-valued. Since $\Psi\begin{pmatrix} & 1 \\ -1 & \end{pmatrix}=0$, one has

$$\Psi(A)=\Psi\left(\begin{pmatrix}&1\\-1&\end{pmatrix}A\right)\equiv\frac{1}{2}\left(1-\left(\frac{c}{a}\right)\right)\pmod 2$$

for $A=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ in $SL(2,\mathcal{O}_L)$ with $c\equiv 0 \pmod{2\mathcal{O}_K}$. Consider the case $k=3$, i.e., $\mathcal{O}_L=\mathcal{O}_8$. Then $SL(2,\mathcal{O}_L)$ contains $\Gamma(8)$ and Ψ satisfies (1) for A in $\Gamma(8)$. For every automorphism σ of $\boldsymbol{C}$, there exists a lattice L' in $\boldsymbol{C}$ such that $\mathcal{O}_{L'}=\mathcal{O}_L$ and

$$(\mathcal{P}(\vartheta)^{-1}\Phi_L)^{\sigma}=\Phi_{L'},$$

cf. [**10**], p. 540 and [**4**]. Hence we have proved Theorem 1.

References

[1] Ph. Cassou-Noguès and M. J. Taylor, Elliptic functions and rings of integers, Birkhäuser, Boston-Basel-Stuttgart, 1987.

[2] R. Fueter, Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen I, II, Teubner, Leipzig-Berlin, 1924, 1927.

[3] G. Harder, On the cohomology of $SL(2,\mathfrak{O})$; Lie groups and their representations, ed. by I. M. Gelfand, A. Hilger, London, 1975, pp. 139-150.

[4] H. Ito, On a property of elliptic Dedekind sums, J. Number Theory, **27** (1987), 17-21.

[5] ———, Dedekind sums and quadratic residue symbols, Nagoya Math. J., **118** (1990), 35-43.

[6] ———, A note on Dedekind sums; Number Theory (Proc. of the 1st Canadian Number Theory Association conference at Banff), ed. by R. A. Mollin, Walter de Gruyter, Berlin-New York, 1990, pp. 239-248.

[7] T. Kubota, Ein arithmetischer Satz über eine Matrizengruppe, J. Reine Angew. Math., **222** (1966), 55-57.

[8] H. Rademacher and E. Grosswald, Dedekind sums, Carus Mathematical Monographs, No. 16, Mathematical Assoc. America, Washington D.C., 1972.

[9] H. Reichardt, Eine Bemerkung zur Theorie des Jacobischen Symbols, Math. Nachr., **19** (1958), 171-175.

[10] R. Sczech, Dedekindsummen mit elliptischen Funktionen, Invent. Math., **76** (1984), 523-551.

[11] ———, Dedekind sums and power residue symbols, Compositio Math., **59** (1986), 89-112.

[12] H. M. Stark, L-functions at $s=1$, IV, Advances in Math., **35** (1980), 197-235.

[13] U. Weselmann, Eisenstein-Kohomologie und Dedekindsummen für GL_2 über imaginärquadratischen zahlkörpern, J. Reine Angew. Math., **389** (1988), 90-121.

Hiroshi ITO

Department of Mathematics
College of Arts and Sciences
University of Tokyo
Komaba, Meguro 153
Japan