M. Koike
Nagoya Math. J.
Vol. 64 (1976), 63-85

CONGRUENCES BETWEEN CUSP FORMS AND LINEAR REPRESENTATIONS OF THE GALOIS GROUP*)

MASAO KOIKE

Let $f(z)$ be a cusp form of type $(1, \varepsilon)$ on $\Gamma_0(N)$ which is a common eigenfunction of all Hecke operators. For such $f(z)$, Deligne and Serre [1] proved that there exists a linear representation

$$\rho: G \longrightarrow GL_2(\boldsymbol{C}) \qquad \text{where } G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}),$$

such that the Artin L-function for ρ is equal to the L-function associated to $f(z)$. In this paper, we shall show that, for almost every prime ℓ, the subfield of $\bar{\boldsymbol{Q}}$ corresponding to the kernel of ρ is realized as a field generated by the coordinates of certain points of finite order of an abelian variety attached to a certain cusp form of type $(2, \varepsilon\psi)$ on $\Gamma_0(N\ell)$, where ψ is a character of $(\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$ of order $\ell - 1$. (See Theorem (2.4).)

We apply the above result to the theory of Shimura [8] to obtain further theorems in § 4.

The proof is based on an idea of Shimura which is very useful for proving congruences between cusp forms. The author wishes to express his hearty thanks to Prof. G. Shimura for suggesting these problems.

Notations and Definitions

§ 0–1. We denote by $\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}$ and $\boldsymbol{C}$, respectively, the ring of rational integers, the rational number field, the real number field and the complex number field. The algebraic closure of $\boldsymbol{Q}$ in $\boldsymbol{C}$ is denoted by $\bar{\boldsymbol{Q}}$. If x is a complex number, $\bar{x}$ denotes its complex conjugate. For an associative ring A with the identity element, $A^\times$ denotes the group of all invertible elements.

For a Dirichlet character χ defined mod N, $\bar{\chi}$ denotes the Dirichlet character defined mod N such that $\bar{\chi}(a) = \overline{\chi(a)}$ for all $a \in \boldsymbol{Z}$, $(a, N) = 1$.

Received May 12, 1976.
*) This work was partially supported by the Sakkokai Foundation.

There is a natural one-to-one correspondence between such Dirichlet characters defined mod N and the $C^\times$-valued characters of the multiplicative group $(Z/NZ)^\times$ of the residue class ring Z/NZ. We identify a Dirichlet character defined mod N with the corresponding character of $(Z/NZ)^\times$.

Let k be an algebraic number field of finite degree. We denote by $\mathfrak{o}_k$ the maximal integer ring of k. For a fractional ideal of $\mathfrak{a}$ in k, $N(\mathfrak{a})$ denotes the absolute norm of $\mathfrak{a}$. For a formal product $\mathfrak{f}$ of an integral ideal $\mathfrak{f}_0$ in k and archimedian primes of k, we denote by $I(\mathfrak{f})$ the group of all fractional ideals in k prime to $\mathfrak{f}_0$ and by $P(\mathfrak{f})$ the subgroup of $I(\mathfrak{f})$ consisting of all the principal ideals generated by the elements α of k such that α is positive at all archimedian primes involved in $\mathfrak{f}$, and $\alpha \equiv 1 \pmod{\mathfrak{f}_\mathfrak{p}}$ for all finite prime factors $\mathfrak{p}$ of $\mathfrak{f}$, where $\mathfrak{f}_\mathfrak{p}$ is the $\mathfrak{p}$-closure of $\mathfrak{f}_0$ in the $\mathfrak{p}$-completion of k. For a real archimedian prime $\mathfrak{p}_\infty$ of k, $(x/\mathfrak{p}_\infty) = 1$ or -1 according as x is positive or negative at $\mathfrak{p}_\infty$.

We shall be discussing homomorphisms χ of the Ideal group $I(\mathfrak{f})$ into a finite group $\mathfrak{g}$ whose kernel contain $P(\mathfrak{f})$. The conductor of χ is defined to be the divisor $\mathfrak{f}'$ of $\mathfrak{f}$ such that: (i) χ is trivial on $I(\mathfrak{f}) \cap P(\mathfrak{f}')$; (ii) no proper divisor of $\mathfrak{f}'$ has the property (i). Then χ can be extended uniquely to a homomorphism χ' of $I(\mathfrak{f}')$ into $\mathfrak{g}$ whose kernel contains $P(\mathfrak{f}')$. We often denote χ' by the same symbol χ.

Let ℓ be a rational prime and let $\tilde{\mathfrak{l}}$ be a prime divisor of $\bar{Q}$ lying above ℓ. We denote by $|x|$, for $x \in \bar{Q}$, the absolute value on $\tilde{\mathfrak{l}}$-adic completion of $\bar{Q}$ normalized so that

$$|\ell| = \ell^{-1} .$$

§0–2. We denote by $\mathfrak{H}$ the complex upper half plane:

$$\mathfrak{H} = \{z \in C \mid \mathrm{Im}\, z > 0\} .$$

For a positive integer κ, a holomorphic function $g(z)$ on $\mathfrak{H}$ and an element $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of $GL_2(R)$ with $\det \alpha > 0$, we define a function $g|[\alpha]_\kappa$ by

$$g|[\alpha]_\kappa = \det(\alpha)^{\kappa/2} \cdot (cz + d)^{-\kappa} g\left(\frac{az + b}{cz + d}\right) .$$

Let N be a positive integer and let ε be an arbitrary $C^\times$-valued character of $(Z/NZ)^\times$ such that

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

$$\varepsilon(-1) = (-1)^{\kappa} .$$

Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}) \mid c \equiv 0 \pmod{N} \right\} ,$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a \equiv d \equiv 1 \pmod{N} \right\} ,$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \mid b \equiv 0 \pmod{N} \right\} .$$

Let $f(z)$ be a modular form of weight κ with respect to $\Gamma_1(N)$ satisfying

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{\kappa}\varepsilon(d)f(z) \qquad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) .$$

We call such $f(z)$ a modular form of type (κ, ε) on $\Gamma_0(N)$. When $f(z)$ is a cusp form, we call $f(z)$ a cusp form of type (κ, ε) on $\Gamma_0(N)$. We denote by $S_\kappa(N, \varepsilon)$ the vector space of all cusp forms of type (κ, ε) on $\Gamma_0(N)$.

Then we can define the Hecke operator $T(p)$ or $U(p)$ as follows. Let $f(z) = \sum a_n e^{2\pi i n z}$ be a modular form of type (κ, ε) on $\Gamma_0(N)$. For each prime p, we put

$$f(z) \mid T(p) = \sum a_{pn} e^{2\pi i n z} + \varepsilon(p) p^{\kappa-1} \sum a_n e^{2\pi i p n z} \qquad \text{if } p \nmid N ,$$

$$f(z) \mid U(p) = \sum a_{pn} e^{2\pi i n z} \qquad \text{if } p \mid N .$$

Thus we obtain another modular form of type (κ, ε) on $\Gamma_0(N)$, which is a cusp form if f is a cusp form.

We define the essential part $S_\kappa^0(N, \varepsilon)$ of $S_\kappa(N, \varepsilon)$ as follows. Let $S_\kappa^1(N, \varepsilon)$ denote the subspace of $S_\kappa(N, \varepsilon)$ spanned by all the functions of the form $g(mz)$, where $g \in S_\kappa(M, \varepsilon)$ for a divisor M $(< N)$ of N, modulo which ε can be defined, and m is a positive divisor of N/M. Then we denote by $S_\kappa^0(N, \varepsilon)$ the orthogonal complement of $S_\kappa^1(N, \varepsilon)$ in $S_\kappa(N, \varepsilon)$ with respect to the Petersson metric.

§ 0–3. Let $f = \sum a_n e^{2\pi i n z}$ and $g = \sum b_n e^{2\pi i n z}$ be formal power series with coefficients in $\bar{\boldsymbol{Q}}$. Let $\tilde{\mathfrak{l}}$ be a prime divisor of $\bar{\boldsymbol{Q}}$. We write

$$f \equiv g \pmod{\tilde{\mathfrak{l}}}$$

when $a_n - b_n$ are $\tilde{\mathfrak{l}}$-adic integers satisfying $a_n - b_n \equiv 0 \pmod{\tilde{\mathfrak{l}}}$ for all n.

§ 1. Preliminaries

§ 1–1. Eisenstein series of weight one

Let ℓ be an odd prime. We fix a prime divisor $\tilde{\mathfrak{l}}$ lying above ℓ in the algebraic closure $\bar{\boldsymbol{Q}}$ of $\boldsymbol{Q}$. Let ψ be the Dirichlet character defined mod ℓ satisfying

$$\psi(a)a \equiv 1 \pmod{\tilde{\mathfrak{l}}} \qquad \text{for all } a \in \boldsymbol{Z},\ (a, \ell) = 1 .$$

In [4], Hecke showed that the space of Eisenstein series of weight 1 with respect to $\Gamma(\ell)$ is generated, for all pairs (a_1, a_2) of rational integers, by

$$G_1(z\,; a_1, a_2, \ell) = C(a_1, a_2, \ell) - \frac{2\pi i}{\ell} \sum_{\substack{m \cdot m_1 > 0 \\ m_1 \equiv a_1 \pmod{\ell}}} \operatorname{sgn} m \zeta_\ell^{a_2 m} e^{2\pi i (m m_1 z/\ell)} ,$$

with

$$C(a_1, a_2, \ell) = \delta\left(\frac{a_1}{\ell}\right) \sum_{m_2 \equiv a_2 \pmod{\ell}}{}' \frac{\operatorname{sgn} m_2}{|m_2|^{1+s}}\bigg|_{s=0} - \frac{\pi i}{\ell} \sum_{m_1 \equiv a_1 \pmod{\ell}}{}' \frac{\operatorname{sgn} m_1}{|m_1|^{s}}\bigg|_{s=0} ,$$

$$\zeta_\ell = e^{2\pi i/\ell} ,$$

where $\sum'$ denotes that the term $m_1 = m_2 = 0$ is to be omitted. Then

$$G_1\left(\frac{az+b}{cz+d}\,; a_1, a_2, \ell\right) = (cz+d) G_1(z\,; aa_1 + ca_2, ba_1 + da_2, \ell) ,$$
$$\text{for } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\boldsymbol{Z}) .$$

For any Dirichlet character χ defined mod ℓ such that $\chi(-1) = -1$, we put

$$G_{1,\chi} = \sum_{a \bmod \ell} \bar{\chi}(a) G_1(z\,; 0, a, \ell) ,$$
$$G_{2,\chi} = \sum_{a,b \bmod \ell} \chi(a) G_1(z\,; a, b, \ell) .$$

Then both $G_{1,\chi}$ and $G_{2,\chi}$ are Eisenstein series of type $(1, \chi)$ on $\Gamma_0(\ell)$, and their Fourier expansions at the cusp ∞ are as follows:

$$G_{1,\chi} = 2L(1, \bar{\chi}) - \frac{4\pi i C(\bar{\chi})}{\ell} \sum_{\substack{m>0 \\ m_1>0}} \chi(m) e^{2\pi i m m_1 z} ,$$
$$G_{2,\chi} = -2\pi i L(0, \chi) - 4\pi i \sum_{\substack{m>0 \\ m_1>0}} \chi(m_1) e^{2\pi i m m_1 z} ,$$

where $L(s, \chi)$ is the Dirichlet's L-function for the character χ and $C(\chi) = \sum_{1 \le a \le \ell-1} \chi(a) e^{2\pi i (a/\ell)}$. By the functional equation of $L(s, \chi)$, we have $L(0, \chi) = (C(\chi)/\pi i) L(1, \bar{\chi})$. Since $C(\chi) C(\bar{\chi}) = -\ell$, we have

$$G_{1,\chi} = \frac{C(\bar{\chi})}{\ell} G_{2,\chi} .$$

Put

$$E_{1,\chi} = \frac{G_{1,\chi}}{2L(1,\bar{\chi})}, \qquad c_\chi = -\frac{2\pi i C(\bar{\chi})}{\ell L(1,\bar{\chi})} = \frac{2}{L(0,\chi)} .$$

So we have

$$E_{1,\chi} = 1 + c_\chi \sum_{\substack{m>0 \\ m_1>0}} \chi(m) e^{2\pi i m m_1 z} .$$

Since

$$L(1,\bar{\chi}) = -\frac{C(\bar{\chi})}{\ell} \cdot \frac{\pi}{i\ell} \sum_{1\le a\le \ell-1} \chi(a)a,$$

it follows

$$c_\chi = -\frac{2\ell}{\sum_{1\le a\le \ell-1} \chi(a)a} .$$

For each χ, there exists a unique odd integer r with $1 \le r \le \ell - 1$ such that $\chi(a) \equiv a^r \pmod{\tilde{1}}$ for all $a \in \boldsymbol{Z}$, $(a, \ell) = 1$. Therefore we have

$$\begin{aligned} \sum_{1\le a\le \ell-1} \chi(a)a &\equiv \sum_{1\le a\le \ell-1} a^{r+1} \pmod{\tilde{1}} , \\ &\equiv \begin{cases} -1 \pmod{\tilde{1}} & \text{if } r = \ell - 2 , \\ 0 \pmod{\tilde{1}} & \text{otherwise} . \end{cases} \end{aligned}$$

Hence $c_\chi \equiv 0 \pmod{\tilde{1}}$ if and only if $\chi = \psi$. When $1 \le r \le \ell - 4$, we have the following informations about c_χ. In [5], it is proved that $|\sum_{1\le a\le \ell-1} \chi(a)a| \ge 2$ if and only if the Bernoulli number B_{r+1} is divisible by ℓ, and it is also proved that, for $\ell \le 4001$, $|\sum_{1\le a\le \ell-1} \chi(a)a| \le 2$ for any χ. Hence we obtain

$$|c_\chi| = \begin{cases} \ell^{-1} & \text{if } \chi = \psi , \\ 1 & \text{if } \chi = \psi^{-r} \text{ and } \ell \nmid B_{r+1} \text{ with } 1 \le r \le \ell - 4 , \\ \ge \ell & \text{otherwise} . \end{cases}$$

We calculate $G_{1,\chi}\left|\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1\right.$:

$$G_{1,\chi}\left|\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1\right. = \sum_{a \bmod \ell} \bar{\chi}(a) G_1(z; 0, a, \ell)\left|\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}_1 \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}_1\right. ,$$

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

$$= \ell^{1/2} \sum_{a \bmod \ell} \bar{\chi}(a) G_1(\ell z; a, 0, \ell) ,$$
$$= \ell^{-1/2} G_{2,\bar{\chi}} .$$

Hence we have

$$E_{1,\chi}\Big|\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1 = \frac{G_{1,\chi}}{2L(1,\bar{\chi})}\Big|\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1 ,$$
$$= \frac{2L(1,\chi)}{2L(1,\bar{\chi})} \frac{\sqrt{\ell}}{C(\chi)} E_{1,\bar{\chi}} ,$$
$$= \frac{c_\chi}{c_{\bar{\chi}}} \frac{\sqrt{\ell}}{C(\bar{\chi})} E_{1,\bar{\chi}} .$$

We summarize these as follows for the later use:
For any character χ of $(\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$ such that $\chi(-1) = -1$, put

$$E_{1,\chi} = 1 + c_\chi \sum_{\substack{m>0 \\ m_1>0}} \chi(m) e^{2\pi i m m_1 z} , \qquad c_\chi = -\frac{2\pi i C(\bar{\chi})}{\ell L(1,\bar{\chi})} .$$

Then $E_{1,\chi}$ is the Eisenstein series of type $(1,\chi)$ on $\Gamma_0(\ell)$ and satisfies

$$E_{1,\chi}\Big|\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1 = \frac{\sqrt{\ell}}{C(\bar{\chi})} \frac{c_\chi}{c_{\bar{\chi}}} E_{1,\bar{\chi}} .$$

Especially for the character ψ, we have the following congruence:

$$E_{1,\psi} \equiv 1 \pmod{\tilde{\mathfrak{l}}} .$$

We should remark that the Eisenstein series $E_{\ell-1}(z)$ of weight $\ell - 1$ on $SL_2(\boldsymbol{Z})$ satisfies the same congruences:

$$E_{\ell-1}(z) = 1 - \frac{2(\ell-1)}{B_{\ell-1}} \sum_{\substack{m>0 \\ m_1>0}} m^{\ell-2} e^{2\pi i m m_1 z} ,$$
$$E_{\ell-1}(z) \equiv 1 \pmod{\tilde{\mathfrak{l}}} \qquad \text{if } \ell \geq 5 ,$$

where $B_{\ell-1}$ is the $\ell - 1$-th Bernoulli number. $E_{p-1}(z)$ was used by Serre in [7] to develop the theory of p-adic modular forms and was also used by Deligne and Serre to prove a theorem about which we shall make a remark in the next section. Our idea, which is due to G. Shimura, is to use $E_{1,\psi}$ instead of $E_{\ell-1}(z)$.

§ 1–2. A theorem of Stickelberger.

The ℓ-adic absolute value of the Gauss sum $C(\chi)$ is calculated in [10]. We recall only the simplest case.

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

Let $K = \boldsymbol{Q}(\zeta_\ell, \zeta_{\ell-1})$ where $\zeta_\ell = e^{2\pi i(1/\ell)}$ and $\zeta_{\ell-1} = e^{2\pi i(1/(\ell-1))}$. Let $\mathfrak{l}$ be a prime factor of ℓ in K. Then $N\mathfrak{l} = \ell$. Let ψ be a $\boldsymbol{C}^\times$-valued character of $(\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$ such that

$$\psi(a)a \equiv 1 \pmod{\mathfrak{l}} \qquad \text{for all } a \in \boldsymbol{Z},\ (a, \ell) = 1 .$$

LEMMA (1.1) (Stickelberger). *The notations being as above, we have, for any $\boldsymbol{C}^\times$-valued character ψ^r with $1 \leq r \leq \ell - 2$ of $(\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$,*

$$\frac{C(\psi^r)}{(\zeta_\ell - 1)^r} \equiv \frac{-1}{r!} \pmod{\mathfrak{l}} .$$

From this follows immediately

PROPOSITION (1.2). *We have*

$$\left| \frac{\sqrt{\ell}\, c_\psi}{C(\bar{\psi}) c_{\bar{\psi}}} \right| = \ell^{-1/2-(1/(\ell-1))} .$$

§ 1–3. Lemma of Deligne and Serre.

LEMMA (1.3) (Deligne and Serre, [1]). *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ be a cusp form of type (κ, ε) on $\Gamma_0(N)$ such that a_n are $\tilde{\mathfrak{l}}$-adic integers for every $n \geq 1$. Suppose a_n satisfy the following congruences for every prime p*

$$\begin{aligned} a_n a_p &\equiv a_{np} + \varepsilon(p) p^{\kappa-1} a_{n/p} \pmod{\tilde{\mathfrak{l}}} \qquad \text{if } p \nmid N , \\ a_n a_p &\equiv a_{np} \pmod{\tilde{\mathfrak{l}}} \qquad \text{if } p \mid N . \end{aligned}$$

Then, there exists a cusp form $g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$ of the same type (κ, ε) as $f(z)$ on $\Gamma_0(N)$ such that

(1–1) *$g(z)$ is a common eigenfunction of the Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N$ and $q \mid N$.*

(1–2) *$b_n \equiv a_n \pmod{\tilde{\mathfrak{l}}}$ for all $n \geq 1$.*

§ 2. Remark on a theorem of Deligne and Serre

§ 2–1. We recall a theorem of Deligne and Serre.

THEOREM (2.1) (Deligne and Serre, [1]). *Let $N \geq 1$ be an integer and let ε be a Dirichlet character defined* mod N *such that $\varepsilon(-1) = -1$. Let*

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} , \qquad a_1 = 1 ,$$

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

be a cusp form of type $(1, \varepsilon)$ *on* $\Gamma_0(N)$ *which is a common eigenfunction of Hecke operators* $T(p)$ *for all primes* $p \nmid N$ *with eigenvalues* a_p. *Then there exists a linear representation*

$$\rho : G \longrightarrow GL_2(\boldsymbol{C}) , \qquad \text{where } G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}) ,$$

such that ρ *is unramified outside of* N *and satisfies*

$$Tr(F_{\rho,p}) = a_p, \ \det(F_{\rho,p}) = \varepsilon(p) \qquad \text{for all primes } p \nmid N ,$$

where $F_{\rho,p}$ *is the image by* ρ *of the Frobenius element related to* p.

The representation ρ associated with f by Theorem (2.1) is irreducible and the image of ρ is finite. We denote by K_f the subfield of $\bar{\boldsymbol{Q}}$ corresponding to the kernel of ρ. Then K_f is a finite Galois extension over $\boldsymbol{Q}$.

§2–2. We recall a theorem of Shimura.

Let $N \geq 1$ be an integer and let χ be a Dirichlet character defined mod N such that $\chi(-1) = 1$. Let

$$h(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z} , \qquad c_1 = 1 ,$$

be a cusp form of type $(2, \chi)$ on $\Gamma_0(N)$ which is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N$ and $q \mid N$. We denote by M the subfield of $\boldsymbol{C}$ generated over $\boldsymbol{Q}$ by the coefficients c_n for all n.

THEOREM (2.2) (Shimura, [8]). *The notations being as above, there exists a couple* (A, θ) *with the following properties*:

(2.1) A *is an abelian subvariety, of dimension* $[M : \boldsymbol{Q}]$, *of the Jacobian variety of the modular function field with respect to* $\Gamma_1(N)$.

(2.2) θ *is an isomorphism of* M *into* $\mathrm{End}(A) \otimes \boldsymbol{Q}$.

(2.3) A *and the elements of* $\theta(M) \cap \mathrm{End}(A)$ *are rational over* $\boldsymbol{Q}$.

(2.4) *For every prime* p, $\theta(c_p)$ *coincides with the homomorphism of* A *naturally induced from the Hecke operator* $T(p)$ *or* $U(p)$.

Changing (A, θ) *by an isogeny over* $\boldsymbol{Q}$, *if necessary, we may assume*

$$\theta(\mathfrak{o}_M) \subset \mathrm{End}(A) .$$

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

§ 2–3. We fix an element

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}, \qquad a_1 = 1,$$

of $S_1^0(N, \varepsilon)$ which is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N$ and $q \mid N$. Let N' be the least common multiple of N and ℓ. If ℓ does not divide N, $f(z)$ is replaced by $f(z) - \alpha f(\ell z)$ where α is a solution of the equation $X^2 - a_\ell X + \varepsilon(\ell) = 0$. For any prime $p \neq \ell$, $f(z)$ and $f(z) - \alpha f(\ell z)$ have the same eigenvalues for the Hecke operators $T(p)$ or $U(p)$.

Put

$$g(z) = f(z) \cdot E_{1,\psi}(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}.$$

Then $g(z)$ is an element of $S_2(N', \varepsilon\psi)$. Since

$$a_{np} = a_n a_p + \varepsilon(p) a_{n/p} \qquad \text{for any prime } p \nmid N',$$

we have

$$\begin{aligned} b_{np} &\equiv b_n b_p + \varepsilon(p) b_{n/p} && (\mathrm{mod}\ \mathfrak{l}), \\ &\equiv b_n b_p + \varepsilon(p)\psi(p) p \cdot b_{n/p} && (\mathrm{mod}\ \mathfrak{l}). \end{aligned}$$

Since

$$a_{nq} = a_n a_q \qquad \text{for any prime } q \mid N',$$

we have

$$b_{nq} \equiv b_n b_q \qquad (\mathrm{mod}\ \mathfrak{l}).$$

Hence, by means of Lemma (1.3), we obtain the following proposition.

PROPOSITION (2.3). *The notations being as above, there exists an element*

$$h(z) = \sum_{n=1}^{\infty} c_n e^{2\pi i n z}, \qquad c_1 = 1,$$

of $S_2(N', \varepsilon\psi)$ *such that*

(2.5) *$h(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N'$ and $q \mid N'$.*

(2.6) $$h(z) \equiv f(z) \qquad (\mathrm{mod}\ \mathfrak{l}).$$

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

Now we assume that ℓ is greater than 3 and is prime to the order of $\mathrm{Gal}(K_f/\boldsymbol{Q})$. Let $h(z)$ be such a cusp form of type $(2, \varepsilon\psi)$ on $\Gamma_0(N')$ corresponding to $f(z)$ as in Proposition (2.3), and let (A, θ) be a couple associated with $h(z)$ by means of Theorem (2.2). We denote by $\mathfrak{l}$ the prime ideal of M which is the restriction of $\tilde{\mathfrak{l}}$ to M. Put

$$A[\mathfrak{l}] = \{t \in A \mid \theta(\mathfrak{l})t = 0\} .$$

We denote by $L_{\mathfrak{l}}$ the subfield of $\boldsymbol{C}$ generated over $\boldsymbol{Q}$ by the coordinates of all points of $A[\mathfrak{l}]$.

THEOREM (2.4). *The notations being as above, we have*

$$L_{\mathfrak{l}} = K_f .$$

We shall use the following two results in our proof of Theorem (2.4).

PROPOSITION (2.5) (Serre, [6]). *Let F be a commutative field. Let H be a finite subgroup of $PGL_2(F)$ whose order is prime to the characteristic of F. Then H is cyclic or dihedral or is isomorphic to one of the groups $\mathfrak{A}_4, \mathfrak{S}_4$ and $\mathfrak{A}_5$.*

PROPOSITION (2.6) (Dickson, [2]). *Let $\ell \geq 5$ be a prime and let F be a finite field in characteristic ℓ. Suppose that G is a subgroup of $PSL_2(F)$ which has order divisible by ℓ and which is irreducible in the sense that it acts without fixed points on $\boldsymbol{P}^1(F)$. Then there is a subfield F' of F such that G is conjugate in $PGL_2(F)$ either to $PGL_2(F')$ or to $PSL_2(F')$.*

Proof of Theorem (2.4). Put $G_{\mathfrak{l}} = \mathrm{Gal}(L_{\mathfrak{l}}/\boldsymbol{Q})$. Taking a basis of $A[\mathfrak{l}]$, we obtain an injective homomorphism

$$\Re : G_{\mathfrak{l}} \longrightarrow GL_2(\mathfrak{o}_M/\mathfrak{l}) .$$

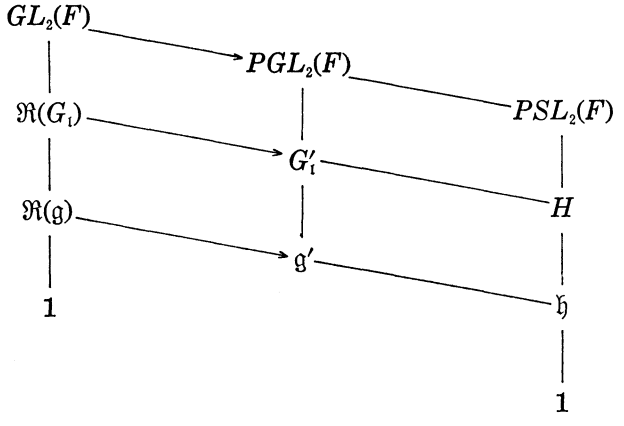
Let p be a prime which does not divide N'. Then p is unramified in $L_{\mathfrak{l}}$. We denote by σ_p the Frobenius element in $G_{\mathfrak{l}}$ related to p. Then we have

$$\begin{aligned} \det(XI_2 - \Re(\sigma_p)) &\equiv X^2 - c_pX + p\varepsilon(p)\psi(p) && (\mathrm{mod}\ \mathfrak{l}) , \\ &\equiv X^2 - a_pX + \varepsilon(p) && (\mathrm{mod}\ \tilde{\mathfrak{l}}) , \\ &\equiv \det(XI_2 - F_{p,p}) && (\mathrm{mod}\ \tilde{\mathfrak{l}}) . \end{aligned}$$

If p is decomposed completely in $L_{\mathfrak{l}}$ over $\boldsymbol{Q}$, we have $\det(XI_2 - \Re(\sigma_p)) = (X-1)^2$. Hence we have

$$\det(XI_2 - F_{\rho,p}) \equiv (X-1)^2 \pmod{\mathfrak{l}} .$$

Since the order of $F_{\rho,p}$ is prime to ℓ, $F_{\rho,p}$ is proved to be equal to the identity. Therefore K_f is contained in $L_\mathfrak{l}$. If the order of $G_\mathfrak{l}$ is prime to ℓ, the same arguments show that $L_\mathfrak{l}$ is contained in K_f. Therefore we may suppose that the order of $G_\mathfrak{l}$ is divisible by ℓ. We denote by $\mathfrak{g}$ the subgroup of $G_\mathfrak{l}$ corresponding to K_f by Galois theory. Put $F = \mathfrak{o}_M/\mathfrak{l}$. Let $\varphi: GL_2(F) \to PGL_2(F)$ be the natural homomorphism. Put $G'_\mathfrak{l} = \varphi \circ \mathfrak{R}(G_\mathfrak{l})$ and $\mathfrak{g}' = \varphi \circ \mathfrak{R}(\mathfrak{g})$. Also put $H = G'_\mathfrak{l} \cap PSL_2(F)$ and $\mathfrak{H} = \mathfrak{g}' \cap PSL_2(F)$.



Since $G_\mathfrak{l}/\mathfrak{g} \simeq \mathrm{Gal}(K_f/\boldsymbol{Q})$, the order of $\mathfrak{g}$ is also divisible by ℓ. Hence the orders of $\mathfrak{H}$ and H are divisible by ℓ.

The case where H is irreducible. By Proposition (2.6), there is a subfield F' of F such that H is conjugate in $PGL_2(F)$ either to $PSL_2(F')$ or to $PGL_2(F')$. Since $\mathfrak{H}$ is a normal subgroup of H, $H/\mathfrak{H}$ has at most order 2; this contradicts to Proposition (2.5).

The case where H is not irreducible. H is conjugate in $PGL_2(F)$ to a subgroup of

$$\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, d \in F^\times, b \in F\right\} \cdot F^\times/F^\times .$$

Since the order of $H/\mathfrak{H}$ is prime ℓ, $H/\mathfrak{H}$ is a cyclic group; this contradicts to Proposition (2.5).

Therefore the order of $G_\mathfrak{l}$ is proved to be prime to ℓ, and the proof of (2.4) is completed. Q.E.D.

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

§ 3. Congruences between cusp forms

§ 3–1. We briefly recall Shimura's theory concerning the relation between the arithmetic of real quadratic fields and the cusp forms of 'Neben'-type in Hecke's sense from his article [8].

Let N be a positive integer and χ be an arbitrary $C^\times$-valued character of $(Z/NZ)^\times$ such that

$$\chi(-1) = 1 .$$

We assume χ is a non-trivial real character, and we denote by k the real quadratic field corresponding to χ. We denote by ε the non-trivial automorphism of k. We fix a non-zero element $h(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ of $S_2^0(N, \chi)$, which is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N$ and $q \mid N$. Replacing h by its suitable constant multiple, we can assume $a_1 = 1$. For a fixed f, we denote by K the subfield of C generated over Q by the coefficients a_n for all n. K is an algebraic number field of finite degree and contains the roots of unity $\chi(n)$ for all n. Moreover, since χ is not trivial, K is a CM-field, namely, a totally imaginary quadratic extension of a totally real algebraic number field. We denote by F the maximal real subfield of K, and denote by ρ the complex conjugation. Let $\mathfrak{b}_0$ be the ideal of $\mathfrak{o}_K$ generated by all x in $\mathfrak{o}_K$ such that $x^\rho = -x$. Then we can define the 'odd part' $\mathfrak{b}$ of $\mathfrak{b}_0$ by the properties: (i) $\mathfrak{b}$ is a divisor of $\mathfrak{b}_0$ prime to 2; (ii) $N(\mathfrak{b}^{-1} \cdot \mathfrak{b}_0)$ is a power of 2. Then $\mathfrak{b}_0$ divides the different of K relative to F, $\mathfrak{b}$ is square-free, $\mathfrak{b}^\rho = \mathfrak{b}$, and $\mathfrak{b}^2 = \mathfrak{c}\mathfrak{o}_K$ with a square-free integral ideal $\mathfrak{c}$ in F. The following result is a fundamental theorem in [8].

THEOREM (3.1) (Shimura, [8]). *Let $\mathfrak{l}$ be a prime factor of $\mathfrak{c}$ in F. Then, there exist $(\mathfrak{o}_F/\mathfrak{l})^\times$-valued characters $r_\mathfrak{l}$ and $s_\mathfrak{l}$ of an ideal group of k satisfying the following properties*:

(3.1) $\mathfrak{f}[r_\mathfrak{l}]^e = \mathfrak{f}[s_\mathfrak{l}]$. *Every finite prime factor of $\mathfrak{f}[r_\mathfrak{l}]$ divides $N(\mathfrak{l})N$.*

(3.2) $r_\mathfrak{l}(\mathfrak{a}) = s_\mathfrak{l}(\mathfrak{a}^e)$ *for every* $\mathfrak{a} \in I(\mathfrak{f}[r_\mathfrak{l}])$.

(3.3) $r_\mathfrak{l}(m\mathfrak{o}_k) = s_\mathfrak{l}(m\mathfrak{o}_k) = (m/p_\infty) \cdot (m \bmod \mathfrak{l})$ *for every* $m \in Z$ *prime to* $\mathfrak{f}[r_\mathfrak{l}]$ *where p_∞ is the archimedian prime of Q.*

(3.4) $r_\mathfrak{l}(\mathfrak{a}) s_\mathfrak{l}(\mathfrak{a}) = (N(\mathfrak{a}) \bmod \mathfrak{l})$ *for all* $\mathfrak{a} \in I(\mathfrak{f}[r_\mathfrak{l}]) \cap I(\mathfrak{f}[s_\mathfrak{l}])$.

(3.5) *If p is a rational prime that is prime to $N(\mathfrak{l}) \cdot N$, and that decom-*

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

poses into two distinct prime ideals $\mathfrak{p}$ *and* $\mathfrak{p}^s$ *in* k, *then*

$$r_\mathfrak{l}(\mathfrak{p}) + s_\mathfrak{l}(\mathfrak{p}^s) = (a_p \bmod \mathfrak{l}) .$$

The properties of these characters $r_\mathfrak{l}$ and $s_\mathfrak{l}$ are connected with the reciprocity law of a certain abelian extension of k which can be generated by the coordinates of certain points of finite order on an abelian variety associated with $h(z)$.

We define a formal power series by

$$\tilde{h}_{r_\mathfrak{l}}(z) = \sum_{\mathfrak{a}} r_\mathfrak{l}(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z} ,$$

where the sum is extended over all integral ideals prime to $\mathfrak{f}[r_\mathfrak{l}]$. Then, from Theorem (3.1), it follows a formal congruence between partial sum of $h(z)$ and $\tilde{h}_{r_\mathfrak{l}}(z)$, namely,

$$\sum_{(n, N(\mathfrak{l})N)=1} a_n e^{2\pi i n z} \equiv \sum_{(\mathfrak{a}, N(\mathfrak{l})N)=1} r_\mathfrak{l}(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z} \qquad (\bmod \mathfrak{b}_\mathfrak{l}) ,$$

where $\mathfrak{b}_\mathfrak{l}$ is the prime factor of $\mathfrak{l}$ in K such that $\mathfrak{b}_\mathfrak{l}^2 = \mathfrak{l}\mathfrak{o}_K$. Shimura conjectured that the congruence holds between entire sums:

$$h(z) \equiv \tilde{h}_{r_\mathfrak{l}}(z) \qquad (\bmod \mathfrak{b}_\mathfrak{l}) . \tag{3.6}$$

It was also proved that the right hand side of (3.6) actually coincides with reduction mod $\tilde{\mathfrak{l}}$ of a cusp form of weight 1, which is the Mellin transform of a L-function of k with a certain class character.

The purpose in this section is, by means of the same idea used in § 2, to prove directly, not by way of abelian varieties, congruences between cusp forms of weight κ with $\kappa \geq 2$ and cusp forms of weight 1 which is the Mellin transform of L-functions of real quadratic fields with certain class characters, and we shall apply this to prove the above conjecture in several cases in the next section.

§ 3–2. Let m be a positive integer prime to ℓ. Let $\sigma_j = \begin{pmatrix} 1 & j \\ 0 & \ell \end{pmatrix}$, $1 \leq j \leq \ell$, and let $W_\ell = \begin{pmatrix} \ell x & 1 \\ \ell m y & \ell \end{pmatrix}$, with some integers x and y, be a matrix with determinant ℓ. Then we have

$$\Gamma_0(m)\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\Gamma_0(m) = \Gamma_0(m) W_\ell \cup \bigcup_{j=1}^{\ell} \Gamma_0(m)\sigma_j , \qquad \text{(disjoint sum)} . \tag{3.7}$$

Put $\rho_j = W_\ell^{-1}\sigma_j$, $1 \leq j \leq \ell$ and $\rho_{\ell+1} = 1$. Then we have

$$\Gamma_0(m) = \bigcup_{j=1}^{\ell+1} \Gamma_0(\ell m)\rho_j , \qquad \text{(disjoint sum)} . \tag{3.8}$$

LEMMA (3.2). *Let $\chi(n)$ be a $C^{\times}$-valued character of $(Z/mZ)^{\times}$. For any element $f(z)$ of $S_k(\Gamma_0(m\ell), \chi)$, both*

$$f + \chi(\ell)^{-1}\ell^{1-k/2} f|[W_\ell]_k|U(\ell) , \tag{3.9}$$

and

$$f|[W_\ell]_k + \ell^{1-k/2} f|U(\ell) , \tag{3.10}$$

are elements of $S_k(\Gamma_0(m), \chi)$.

Proof. For $\gamma = \begin{pmatrix} a & b \\ cm & d \end{pmatrix} \in \Gamma_0(m)$, we have $\rho_j \gamma \rho_i^{-1} \equiv \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \pmod{m}$. Hence $\sum_{j=1}^{\ell+1} f|[\rho_j]_k$ is an element of $S_k(\Gamma_0(m), \chi)$. We have

$$\begin{aligned} \sum_{j=1}^{\ell+1} f|[\rho_j]_k &= f + \sum_{j=1}^{\ell} f|[W_\ell^{-1}]_k[\sigma_j]_k \\ &= f + \chi(\ell)^{-1}\ell^{1-k/2} f|[W_\ell]|U(\ell) , \end{aligned}$$

since $f|[W_\ell]_k^2 = \chi(\ell)f$. It is easily proved that $f|[W_\ell]_k$ is also an element of $S_k(\Gamma_0(m\ell), \chi)$. Hence we obtain (3.10), applying (3.9) to $f|[W_\ell]_k$.

Q.E.D.

For any element of $S_k(\Gamma_0(m\ell), \chi)$, we define

$$Tr(f) = f + \chi(\ell)^{-1}\ell^{1-k/2} f|[W_\ell]_k|U(\ell) . \tag{3.11}$$

Remark (3.3). In [7], Serre defined the trace of modular forms on $\Gamma_0(\ell)$. The above lemma gives a slight generalization of Serre's definition.

§3–3. Let $k = Q(\sqrt{N})$ be a real quadratic field and let N be the discriminant of k. Let $\ell \geq 5$ be a prime which decomposes into two prime ideals in k. We fix a prime factor $\mathfrak{l}_1$ of ℓ in k such that $\mathfrak{l}_1$ is lying under $\mathfrak{l}$. Let $\mathfrak{p}_\infty$ be an archimedian prime of k and let $\mathfrak{m}$ be an integral ideal of k such that $\mathfrak{m}$ is prime to ℓ. Put $m = N_{k/Q}\mathfrak{m}$. Let λ be a $C^{\times}$-valued character of the ideal group of k whose conductor is $\mathfrak{p}_\infty \cdot \mathfrak{m} \cdot \mathfrak{l}_1$. With such a λ, we associate a function $f_\lambda(z)$ by

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) e^{2\pi i N(\mathfrak{a})z} ,$$

where $\mathfrak{a}$ runs over all integral ideals of k prime to $m\mathfrak{l}_1$. On account of the functional equation of the corresponding L-function

$$L(s, \lambda) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) N(\mathfrak{a})^{-s} ,$$

$f_\lambda(z)$ is proved to be an element of $S_1^0(\ell m N, \chi)$ with $\chi(a) = (N/a)\lambda(a\mathfrak{o}_k)$ for

$a \in \boldsymbol{Z}$, $(a, \ell mN) = 1$, where (N/a) is the Legendre symbol. Moreover, on account of that $L(s, \lambda)$ has an Euler product, $f_\lambda(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid \ell mN$ and $q \mid \ell mN$. Then χ is decomposed into the product of χ_1 and χ_2 which are characters of $(\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$ and of $(\boldsymbol{Z}/mN\boldsymbol{Z})^\times$ respectively. Since ψ is a generator of the character group of $(\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$, there exists a unique integer κ with $1 \leq \kappa \leq \ell - 1$ such that

$$\chi_1 = \psi^{-\kappa}\,, \tag{3.12}$$

where ψ is the Dirichlet character introduced in § 1–1.

THEOREM (3.4). *The notations being as above, there exists an element $h(z)$ of $S_{\kappa+1}(mN, \chi_2)$ such that*

(3.13) *$h(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid mN$ and $q \mid mN$,*

$$h(z) \equiv f_\lambda(z) \pmod{\tilde{\mathfrak{l}}}\,. \tag{3.14}$$

Proof. Put $g(z) = f_\lambda(z) \cdot E_{1,\psi}(z)^\kappa$. By (3.12), $g(z)$ is an element of $S_{\kappa+1}(\ell mN, \chi_2)$. We shall show that $\mathrm{Tr}\, g \equiv g \pmod{\tilde{\mathfrak{l}}}$. For that purpose, we shall prove that

$$\ell^{1-(\kappa+1)/2} g \mid [W_\ell]_{\kappa+1} \equiv 0 \pmod{\tilde{\mathfrak{l}}}\,. \tag{3.15}$$

We have

$$\begin{aligned} g \mid [W_\ell]_{\kappa+1} &= f \mid [W_\ell]_1 \cdot (E_{1,\psi} \mid [W_\ell]_1)^\kappa\,, \\ &= f \mid [W_\ell]_1 \cdot \left(\frac{\sqrt{\ell} \cdot c_\psi}{C(\bar{\psi}) \cdot c_{\bar{\psi}}}\right) \cdot E_{1,\bar{\psi}}^\kappa\,, \end{aligned}$$

because

$$E_{1,\psi} \mid [W_\ell]_1 = E_{1,\psi} \left| \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1 \cdot \begin{pmatrix} my, & 1 \\ -\ell x, & -1 \end{pmatrix}_1 = E_{1,\psi} \right| \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}_1 .$$

By Proposition (1.2), we have

$$\left| \frac{\sqrt{\ell} \cdot c_\psi}{C(\bar{\psi}) \cdot c_{\bar{\psi}}} \right| = \ell^{-1/2 - 1/(\ell-1)}\,.$$

Since $f(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid \ell mN$ and $q \mid \ell mN$ by means of Asai's calculation [9], we have

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

$$f|[W_\ell]_1 = \lambda_\ell f^{(\ell)} ,$$

with

$$\lambda_\ell = \begin{cases} C(\chi_1)\ell^{-1/2}\bar{a}_\ell & \text{if } \kappa \neq \ell - 1 , \\ -\ell^{1-1/2}\bar{a}_\ell & \text{if } \kappa = \ell - 1 , \end{cases}$$

where $f^{(\ell)}(z) = \sum_{n=1}^{\infty} a_n^{(\ell)} e^{2\pi i n z}$, $a_1^{(\ell)} = 1$, is an element of $S_1^0(\ell mN, \chi_2\bar{\chi}_1)$ which is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid \ell mN$ and $q \mid \ell mN$, and a_ℓ is the eigenvalue of $f_1(z)$ for the Hecke operator $U(\ell)$. In [9], the explicit relations of Fourier coefficients of both functions $f(z)$ and $f^{(\ell)}(z)$ are given. We should remark the following: in [9], every computation was done under the condition that the level N is square-free, but it is not always necessary. It is easily checked that we can apply his result in our case. Hence we have

$$\left| \ell^{1-(\kappa+1)/2} \cdot \lambda_\ell \cdot \left(\frac{\sqrt{\ell}\, c_\psi}{C(\bar{\psi}) c_{\bar{\psi}}} \right)^{\kappa} \right| = \begin{cases} \ell^{-1}|\bar{a}_\ell| & \text{if } \kappa \neq \ell - 1 , \\ \ell^{-2}|\bar{a}_\ell| & \text{if } \kappa = \ell - 1 . \end{cases}$$

Therefore (3.15) is proved. Q.E.D.

Remark (3.5). We should remark that κ need not be restricted to the interval $1 \leq \kappa \leq \ell - 1$. We may take arbitrary positive κ which satisfies (3.12).

Remark (3.6). Starting from any new form in $S_r^0(m\ell, \chi)$ with $r > 1$, we can obtain the similar results to Theorem (3.4).

§ 4. The case of square-free level N with the character $(N/\ )$

Let $k = \boldsymbol{Q}(\sqrt{N})$ with a positive square-free integer $N \equiv 1 \pmod 4$. Let u_0 be the fundamental unit of k. Suppose $N_{k/\boldsymbol{Q}}(u_0) = -1$. Let $\ell \geq 5$ be a rational prime which divides $N_{k/\boldsymbol{Q}}(u_0 - 1)$. Then ℓ decomposes into two prime ideals in k. Moreover, $u_0 - 1$ is divisible by only one of the two prime factors of ℓ in k. Hence we may assume that $u_0 \equiv 1 \pmod{\mathfrak{l}_1}$ with a prime factor $\mathfrak{l}_1$ of ℓ in k which is lying under $\tilde{\mathfrak{l}}$. Let $\mathfrak{p}_\infty$ be an archimedian prime of k such that $(u_0/\mathfrak{p}_\infty) = 1$. Then, there exists an ideal character λ of k with conductor $\mathfrak{p}_\infty \cdot \mathfrak{l}_1$ satisfying

$$\lambda(\alpha \mathfrak{o}_k) = \left(\frac{\alpha}{\mathfrak{p}_\infty} \right) \cdot \psi^{-1} \circ \iota(\alpha \bmod \mathfrak{l}_1)$$

for every α in k prime to $\mathfrak{l}_1$. Here $\iota : (\mathfrak{o}_k/\mathfrak{l}_1)^\times \to (\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$ is the natural

isomorphism such that $\iota(a \bmod \mathfrak{l}_1) = a \bmod \ell$ for every $a \in \boldsymbol{Z}$, $(a, \ell) = 1$.

We fix such a λ and, with λ, we associate a function $f_\lambda(z)$ by

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z} ,$$

where $\mathfrak{a}$ runs over all integral ideals of k prime to $\mathfrak{l}_1$. Then $f_\lambda(z)$ is an element of $S_1(N\ell, (N/\ )\psi^{-1})$ which is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N\ell$ and $q \mid N\ell$. Applying Theorem (3.4) to $f_\lambda(z)$, we obtain the following

PROPOSITION (4.1). *The notations being as above, there exists an element $h(z)$ of $S_2(N, (N/\ ))$ such that*

(4.1) *$h(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N$ and $q \mid N$,*

$$h(z) \equiv f_\lambda(z) \qquad (\mathrm{mod}\ \tilde{\mathfrak{l}}) . \tag{4.2}$$

We fix such a $h(z)$ obtained in Proposition (4.1) and, to such $h(z)$, we can apply Shimura's theory a part of which is explained in § 3–1, namely, we consider $(A, \theta), K, F, \mathfrak{c}$, etc, for the fixed $h(z)$. As a corollary of Proposition (4.1), we immediately obtain the following

COROLLARY (4.2). *The notations being as above, ℓ is a prime factor of $N(\mathfrak{c})$.*

Hence the prime ideal $\mathfrak{l}$ of F which is lying under $\tilde{\mathfrak{l}}$ is a prime factor of $\mathfrak{c}$. Let $\mathfrak{b}_\mathfrak{l}$ be a prime ideal of K such that $\mathfrak{b}_\mathfrak{l}^2 = \mathfrak{l}\mathfrak{o}_K$. Put

$$A[\mathfrak{b}_\mathfrak{l}] = \{t \in A \mid \theta(\mathfrak{b}_\mathfrak{l})t = 0\}$$

and denote by $L_{\mathfrak{b}_\mathfrak{l}}$ the field generated over $\boldsymbol{Q}$ by the coordinates of all points in $A[\mathfrak{b}_\mathfrak{l}]$. From Theorem (2.4) follows

COROLLARY (4.3). *The notations being as above, we have*

$$L_{\mathfrak{b}_\mathfrak{l}} = K_{f_\lambda} ,$$

if the class number of k is prime to ℓ.

Proof. We have to check only the condition that ℓ is prime to the order of $\mathrm{Gal}\,(K_{f_\lambda}/\boldsymbol{Q})$ is satisfied. The order of $I(\mathfrak{p}_\infty\mathfrak{l}_1)/p(\mathfrak{p}_\infty\mathfrak{l}_1)$ is equal to $h(\ell - 1)$, where h is the class number of k. Since the order of $\mathrm{Gal}\,(K_{f_\lambda}/\boldsymbol{Q})$

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

divides $h^2(\ell - 1)^2$, the above condition is satisfied if h is prime to ℓ. Q.E.D.

We give a relation between the characters λ and $r_\mathfrak{l}$ or $s_\mathfrak{l}$. We denote by $\mathfrak{F}$ the residue field of $\bar{\boldsymbol{Q}}$ with respect to $\tilde{\mathfrak{l}}$. Hence $\mathfrak{o}_F/\mathfrak{l}$ is canonically imbedded into $\mathfrak{F}$. For any fractional ideal $\mathfrak{a}$ of $I(\mathfrak{p}_\infty \cdot \mathfrak{l}_1)$, we define $\tilde{\lambda}(\mathfrak{a})$ by

$$\tilde{\lambda}(\mathfrak{a}) = \lambda(\mathfrak{a}) (\mathrm{mod}\ \tilde{\mathfrak{l}}) .$$

It is obvious that $\tilde{\lambda}$ is a $\mathfrak{F}^\times$-valued character of $I(\mathfrak{p}_\infty \mathfrak{l}_1)$ which is trivial on $P(\mathfrak{p}_\infty \mathfrak{l}_1)$ and that the conductor of $\tilde{\lambda}$ is equal to $\mathfrak{p}_\infty \mathfrak{l}_1$.

COROLLARY (4.4). *The notations being as above, either $r_\mathfrak{l}$ or $s_\mathfrak{l}$ coincides with $\tilde{\lambda}$. Especially the conductor $\mathfrak{f}[r_\mathfrak{l}]$ of $r_\mathfrak{l}$ is equal to $\mathfrak{p}_\infty \cdot \mathfrak{l}_1$ and the following congruence holds:*

$$h(z) \equiv \tilde{f}_{r_\mathfrak{l}} \quad (\mathrm{mod}\ \tilde{\mathfrak{l}}) . \tag{4.3}$$

Proof. Let p be a rational prime not dividing $N(\mathfrak{l}) \cdot N$, $\mathfrak{p}$ a prime ideal in k dividing p and $\mathfrak{B}$ a prime divisor of $\bar{\boldsymbol{Q}}$ which extends $\mathfrak{p}$. Consider reduction modulo $\mathfrak{B}$ and indicate reduced objects by putting tildes. Let π_p denote the Frobenius endomorphism of $\tilde{A}$ of degree p and σ_p a Frobenius element of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/k)$ for $\mathfrak{B}$. We suppose $(N/p) = 1$. Then σ_p is also a Frobenius element of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ for $\mathfrak{B}$. We denote by $\mathfrak{R}$ and R the $\mathfrak{h}_\mathfrak{l}$-adic representations of $\mathrm{End}(A) \otimes \boldsymbol{Q}$ and $\mathrm{End}(\tilde{A}) \otimes \boldsymbol{Q}$ respectively. Then it is known that

$$\mathfrak{R}(\sigma_p) = R(\pi_p)$$

if we take a suitable choice of basis of $A[\mathfrak{h}_\mathfrak{l}^\infty]$ and $\tilde{A}[\mathfrak{h}_\mathfrak{l}^\infty]$. We have

$$R(\pi_p) \ (\mathrm{mod}\ \mathfrak{h}_\mathfrak{l}) = \begin{pmatrix} r_\mathfrak{l}(\mathfrak{p}) & 0 \\ 0 & s_\mathfrak{l}(\mathfrak{p}) \end{pmatrix} .$$

On the other hand, if we restrict $\mathfrak{R}$ to all such σ_p with $(N/p) = 1$, we can obtain diagonal matrices simultaneously, namely,

$$\mathfrak{R}(\sigma_p) \sim \begin{pmatrix} \lambda(\mathfrak{p}) & 0 \\ 0 & \lambda(\mathfrak{p}^\varepsilon) \end{pmatrix} ,$$

where ε is the non-trivial automorphism of k. When $(N/p) = -1$, we have

$$\begin{aligned}\tilde{\lambda}(p\mathfrak{o}_k) &= \psi^{-1}\circ\iota(p \bmod \mathfrak{l}_1) \qquad (\mathrm{mod}\ \tilde{\mathfrak{l}})\\ &= p \qquad (\mathrm{mod}\ \tilde{\mathfrak{l}})\\ &= r_{\mathfrak{l}}(p\mathfrak{o}_k) = s_{\mathfrak{l}}(p\mathfrak{o}_k)\ .\end{aligned}$$

Therefore, either $r_{\mathfrak{l}}$ or $s_{\mathfrak{l}}$ coincides with $\tilde{\lambda}$.

Since it is clear that

$$f_\lambda(z) \equiv \tilde{f}_{r_{\mathfrak{l}}} \qquad (\mathrm{mod}\ \tilde{\mathfrak{l}})\ ,$$

(4.3) follows immediately from (3.14). Q.E.D.

Now we go back to the general theory and explain another conjecture of Shimura. Assume N is a prime. Accordingly $\chi(a) = (N/a)$ and $N \equiv 1 \pmod 4$, so that $k = \boldsymbol{Q}(\sqrt{N})$. Let u_0 be the fundamental unit of k. In [8], Shimura conjectured that

(4.4) *$N(\mathfrak{c})$ and $\mathrm{Tr}_{k/\boldsymbol{Q}}(u_0)$ consist of the same prime factors, if we disregard 2 and 3.*

We can give a partial answer for his conjecture as a direct consequence of Proposition (4.1).

PROPOSITION (4.5). *Let N be a square-free integer such that $N \equiv 1 \pmod 4$, and let u_0 be the fundamental unit of $k = \boldsymbol{Q}(\sqrt{N})$. Suppose $N_{k/\boldsymbol{Q}} = -1$. Let $\ell \geq 5$ be any prime which divides $\mathrm{Tr}_{k/\boldsymbol{Q}} u_0$. Then there exists an element $h(z)$ of $S_2(N, (N/\ ))$ which is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid N$ and $q \mid N$ such that ℓ divides $N(\mathfrak{c})$ for $h(z)$.*

§ 5. The micellaneous cases

In the preceding section, we reconsidered Shimura's result in the case of square-free level N with the character $(N/\ )$ from our view point, namely, congruences between cusp forms of weight one and of weight two. We can also find various detailed examples in the case of arbitrary levels in [3] and [8]. For some of these, we can make the similar arguments to § 4, but we should remark that there are also some cases for which Theorem (3.4) is not effective.

In this section, we choose three of these examples and analyze them.

§ 5–1. The case of level $4N$

Let $k = \boldsymbol{Q}(\sqrt{N})$ with a square-free integer $N \equiv 5 \pmod 8$. Let u_0

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

be the fundamental unit of k. Suppose $N_{k/Q}(u_0) = -1$. We also assume $\mathrm{Tr}_{k/Q} u_0 \not\equiv 0 \pmod 4$. We denote by ε the non-trivial automorphism of k throughout this section.

PROPOSITION (5.1). *The notations being as above,* $u_0 \pmod 2$ *is a generator of* $(\mathfrak{o}_k/2\mathfrak{o}_k)^\times$.

Proof. Since 2 remains prime in k, $(\mathfrak{o}_k/2\mathfrak{o}_k)^\times$ is the cyclic group of order 3. If $u_0 \equiv 1 \pmod 2$, we have $(u_0 - 1)(u_0^\varepsilon - 1) = -\mathrm{Tr}_{k/Q} u_0 \equiv 0 \pmod 4$; this contradicts our assumption. Q.E.D.

Let $\ell \geq 5$ be a prime such that

$$\mathrm{Tr}_{k/Q} u_0^3 \equiv 0 \pmod \ell , \qquad \mathrm{Tr}_{k/Q} u_0 \not\equiv 0 \pmod \ell .$$

Then ℓ decomposes into two prime ideals in k. Let $\mathfrak{l}_1$ be a prime factor of ℓ in k such that $u_0^3 \equiv 1 \pmod{\mathfrak{l}_1}$. We may assume that $\mathfrak{l}_1$ is lying under $\tilde{\mathfrak{l}}$.

Let $\mathfrak{p}_\infty$ be an archimedian prime of k such that $(u_0/\mathfrak{p}_\infty) = 1$. Then there exists a $C^\times$-valued character λ of the ideal group of k with the conductor $\mathfrak{p}_\infty \cdot 2 \cdot \mathfrak{l}_1$ satisfying

$$\lambda(\alpha\mathfrak{o}_k) = \left(\frac{\alpha}{\mathfrak{p}_\infty}\right)\varphi(\alpha \bmod 2)\psi^{-1} \circ \iota(\alpha \bmod \mathfrak{l}_1)$$

where φ is the character of $(\mathfrak{o}_k/2\mathfrak{o}_k)^\times$ such that $\varphi(u_0 \bmod 2) = \psi \circ \iota(u_0 \bmod \mathfrak{l}_1)$.

With such a λ, we associate a function $f_\lambda(z)$ by

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a}) e^{2\pi i N(\mathfrak{a}) z} ,$$

where $\mathfrak{a}$ runs over all integral ideals of k prime to $2 \cdot \mathfrak{l}_1$. Then $f_\lambda(z)$ is an element of $S_1(4N\ell, (N/\ )\psi^{-1})$. Applying Theorem (3.4) to $f_\lambda(z)$, we obtain the following

PROPOSITION (5.2). *The notations being as above, there exists an element* $h(z)$ *in* $S_2(4N, (N/\ ))$ *such that*

(5.1) *$h(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid 4N$ and $q \mid 4N$,*

(5.2) $$h(z) \equiv f_\lambda(z) \pmod{\tilde{\mathfrak{l}}} .$$

Remark (5.3). Some numerical examples in this case are given by Doi and Yamauchi [3].

§ 5–2. The case of level 3^2N

PROPOSITION (5.4). *Let $k = \boldsymbol{Q}(\sqrt{N})$ with a positive square-free integer $N \equiv 1 \pmod 4$. Let u_0 be the fundamental unit of k. Suppose $N_{k/\boldsymbol{Q}}(u_0) = -1$.* (1) *If $N \equiv 2 \pmod 3$, the order of u_0 in $(\mathfrak{o}_k/3\mathfrak{o}_k)^\times$ is 8.* (2) *Let ℓ be a prime. Then $N_{k/\boldsymbol{Q}}(u_0^2 + 1) \equiv 0 \pmod \ell$ if and only if $\mathrm{Tr}_{k/\boldsymbol{Q}}(u_0\sqrt{N}) \equiv 0 \pmod \ell$.*

Proof. Since $(N/3) = -1, 3$ remains prime in k, so $(\mathfrak{o}_k/3\mathfrak{o}_k)^\times$ is a cyclic group of order 8. Put $u_0 = (a + b\sqrt{N})/2$ with rational integers a and b. If $u_0 \equiv a/2 \pmod 3$, we have $u_0^4 \equiv a/2 \pmod 3$. Hence $u_0u_0^4 \equiv a^2/4 \equiv 1 \pmod 3$; this is a contradiction because $N_{k/\boldsymbol{Q}}u_0 = -1$. Since $u_0^3 \equiv (a + bN\sqrt{N})/2 \pmod 3$, we have $u_0^4 \equiv a^2 + N^2b^2 \equiv -1 \pmod 3$. Therefore the order of u_0 in $(\mathfrak{o}_k/3\mathfrak{o}_k)^\times$ is proved to be 8. Since $N_{k/\boldsymbol{Q}}u_0 = -1$, we have $a^2 - b^2N = -4$. $N_{k/\boldsymbol{Q}}(u_0^2 + 1) = 2 + \mathrm{Tr}_{k/\boldsymbol{Q}}\, u_0^2 = 2 + (a^2 + b^2N)/2 = b^2N$. Hence (2) is proved to be valid. Q.E.D.

Let $k = \boldsymbol{Q}(\sqrt{N})$ with a positive square-free integer $N \equiv 5 \pmod{12}$. Let u_0 be the fundamental unit of k. Suppose $N_{k/\boldsymbol{Q}}u_0 = -1$. Let $\ell \geq 5$ be a prime such that $N_{k/\boldsymbol{Q}}(u_0^2 + 1) \equiv 0 \pmod \ell$ and $\ell \nmid N$. Also suppose ℓ is completely decomposed in k. Let $\mathfrak{l}_1$ be a prime factor of ℓ in k such that $u_0^2 + 1 \equiv 0 \pmod{\mathfrak{l}_1}$. We may assume $\mathfrak{l}_1$ is lying under $\tilde{\mathfrak{l}}$. Let χ be a character of $(\mathfrak{o}_k/3\mathfrak{o}_k)^\times$ such that $\chi(u_0) = \psi \circ \iota(u_0 \bmod \mathfrak{l}_1)$. Let $\mathfrak{p}_\infty$ be an archimedian prime of k such that $(u_0/\mathfrak{p}_\infty) = 1$. Then, there exists an ideal character λ with conductor $\mathfrak{p}_\infty \cdot 3 \cdot \mathfrak{l}_1$ satisfying

$$\lambda(\alpha\mathfrak{o}_k) = \left(\frac{\alpha}{\mathfrak{p}_\infty}\right)\chi(\alpha \bmod 3\mathfrak{o}_k)\psi^{-1} \circ \iota(\alpha \bmod \mathfrak{l}_1) ,$$

for every α in k prime to $3\mathfrak{l}_1$. Here $\iota : (\mathfrak{o}_k/\mathfrak{l}_1)^\times \to (\boldsymbol{Z}/\ell\boldsymbol{Z})^\times$ is the canonical isomorphism such that $\iota(a \bmod \mathfrak{l}_1) = a \pmod \ell$ for every rational integer a prime to ℓ.

With such a λ, we associate a function $f_\lambda(z)$ by

$$f_\lambda(z) = \sum_{\mathfrak{a}} \lambda(\mathfrak{a})e^{2\pi i N(\mathfrak{a})z} ,$$

where $\mathfrak{a}$ runs over all integral ideals of k prime to $3\mathfrak{l}_1$. Then $f_\lambda(z)$ is an element of $S_1(3^2N\ell, (N/\ )\psi^{-1})$. Applying Theorem (3.4) to $f_\lambda(z)$, we obtain the following:

PROPOSITION (5.5). *The notations being as above, there exists an element $h(z)$ in $S_2(3^2N, (N/\ ))$ such that*

https://doi.org/10.1017/S0027763000017554 Published online by Cambridge University Press

(5.3) *$h(z)$ is a common eigenfunction of Hecke operators $T(p)$ and $U(q)$ for all primes $p \nmid 3^2N$ and $q \mid 3^2N$,*

$$h(z) \equiv f_\lambda(z) \pmod{\tilde{\mathfrak{l}}} . \tag{5.4}$$

Remark (5.6). Some numerical examples in this case are found in H. Hijikata's article in Japan-U.S. Seminar on Modern Methods in Number Theory, Tokyo, 1971.

§ 5–3. The case of level 5^3

The preceding two examples are concerned with the cusp forms of 'Neben'-type. We give here an example concerned with the cusp forms of 'Haupt'-type. This example was found by Doi and Yamauchi [3], and here we analyze this from our view point, namely, the congruences between cusp forms.

Let $k = \boldsymbol{Q}(\sqrt{5})$. Take the fundamental unit $u_0 = (1 + \sqrt{5})/2$ in k. Then we have $u_0^5 = (11 + 5\sqrt{5})/2$. The prime 11 decomposes into two prime ideals in k. Let $\mathfrak{l}_1$ be a prime factor of 11 in k such that

$$u_0^5 \equiv 1 \pmod{\mathfrak{l}_1} .$$

We may assume that $\mathfrak{l}_1$ is lying under $\tilde{\mathfrak{l}}$. Let $\mathfrak{p}_\infty$ be an archimedian prime of k such that

$$\left(\frac{u_0}{\mathfrak{p}_\infty}\right) = -1 .$$

PROPOSITION (5.7). *There exists a $\boldsymbol{C}^\times$-valued character λ of the ideal group of k with the conductor $\mathfrak{p}_\infty \cdot 5 \cdot \mathfrak{l}_1$ such that*

$$\lambda(\alpha \mathfrak{o}_k) = \left(\frac{\alpha}{\mathfrak{p}_\infty}\right) \varphi(\alpha \bmod 5) \psi^{-1} \circ \iota(\alpha \bmod \mathfrak{l}_1) ,$$

for every α in k prime to $5 \cdot \mathfrak{l}_1$. Here φ is the character of $(\mathfrak{o}_k/5\mathfrak{o}_k)^\times$ such that

$$\varphi(u_0 \bmod 5) = -\psi \circ \iota(u_0 \bmod \mathfrak{l}_1) .$$

Proof. $(\mathfrak{o}_k/5\mathfrak{o}_k)^\times$ is the cyclic group of order 20. Since $u_0^5 \equiv 3 \pmod 5$, $u_0 \pmod 5$ is a generator of $(\mathfrak{o}_k/5\mathfrak{o}_k)^\times$. On the other hand, $u_0 \pmod{\mathfrak{l}_1}$ is of order 5. Hence $-\psi \circ \iota(u_0 \bmod \mathfrak{l}_1)$ is a primitive 10-th root of unity. Therefore φ is well-defined, and satisfies $\varphi(-1 \bmod 5) = 1$. We have

$$\lambda(u_0\mathfrak{o}_k) = -1\cdot\varphi(u_0 \bmod 5)\cdot\psi^{-1}\circ\iota(u_0 \bmod \mathfrak{l}_1) = 1\ ,$$

and

$$\lambda((-1)\mathfrak{o}_k) = -1\cdot 1\cdot -1 = 1\ .$$

Hence λ is proved to be a character of the ideal group of k with the conductor $\mathfrak{p}_\infty\cdot 5\cdot\mathfrak{l}_1$. Q.E.D.

We should remark that the induced character of $(\boldsymbol{Z}/5\boldsymbol{Z})^\times$ given by the restriction of φ to $\boldsymbol{Z}$ coincides with $\chi(n) = (n/5)$. Hence $f(z)$ is an element of $S_1(5^3\cdot 11, \psi^{-1})$. Applying Theorem (3.4) to $f_\lambda(z)$, we obtain the following

PROPOSITION (5.8). *There exists a cusp form $h(z)$ of weight 2 with respect to $\Gamma_0(5^3)$ satisfying*

(5.5) *$h(z)$ is a common eigenfunction of the Hecke operators $T(p)$ and $U(5)$ for all primes $p\nmid 5$,*

(5.6) $$h(z) \equiv f_\lambda(z) \qquad (\mathrm{mod}\ \mathfrak{l})\ .$$

REFERENCES

[1] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, Ann. scient. Éc. Norm. Sup. 4e série, t. **7** (1974), 507–530.

[2] L. E. Dickson, Linear groups with an exposition of the Galois field theory, Leipzig, Teubner, 1901.

[3] K. Doi and M. Yamauchi, On the Hecke operators for $\Gamma_0(N)$ and class fields over quadratic number fields, J. Math. Soc. Japan, **25** (1973), 629–643.

[4] E. Hecke, Theorie der Eisensteinschen Reihen höherer Stufe und ihre Anwendung auf Funktionen theorie und Arithmetik, Math. Werke, 461–486.

[5] K. Iwasawa and C. C. Sims, Computation of invariants in the theory of cyclotomic fields, J. Math. Soc. Japan, **18** (1966), 86–96.

[6] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones math., **15** (1972), 259–331.

[7] J.-P. Serre, Formes modulaires et fonction zêta p-adique, Modular functions of one variable III, Proc. Intern. Summer School, Univ. Antwerp, 1972, Springer Lecture Notes in Mathematics No. 350, 191–268.

[8] G. Shimura, Class fields over real quadratic fields and Hecke operators, Ann. of Math., **95** (1972), 130–190.

[9] T. Asai, On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution, J. Math. Soc. Japan, **28** (1976), 48–61.

[10] L. Stickelberger, Über eine Verallgemeinerung der Kreistheilung, Math. Ann., **37** (1890), 321–367.

Nagoya University