Advanced Studies in Pure Mathematics 13, 1988
Investigations in Number Theory
pp. 171–192

A_4-extensions over Real Quadratic Fields and Hecke Operators

Masao Koike and Yoshio Tanigawa

§ 0. Introduction

In articles [10], [11], Shimura investigated the relation between the arithmetic of real quadratic fields and cusp forms of real "Neben"-type of weight 2. He showed that the eigenvalues of Hecke operators for such forms are closely connected with the reciprocity law in certain abelian extensions of a real quadratic field k and, moreover, such extensions can be generated by the coordinates of certain points of finite order on an abelian variety associated with these cusp forms. Later, his results were enriched by several authors Doi-Yamauchi [2], Ohta [8] and Koike [4]. Especially, in [4], we understood his result through congruences between the cusp forms of weight 2 and cusp forms of weight 1 which are obtained from Mellin transform of L-functions of the real quadratic field k. These cusp forms of weight 1 correspond to dihedral representations of the Galois group G_Q.

In this paper, we investigate several examples of cusp forms of real "Neben"-type of weight 2 which are congruent to cusp forms of weight 1 corresponding to representations of the Galois group G_Q of type S_4. We also discuss arithmetic properties analogous to the above Shimura's result induced from these congruences.

To state our result precisely, we introduce several notations. Let p, $p\equiv 1 \pmod 4$ be a prime. Let $f(z)=\sum_{n=1}^{\infty} a_n q^n$, $a_1=1$, $q=e^{2\pi\sqrt{-1}z}$, be a primitive form in $S_2\left(p, \left(\frac{}{p}\right)\right)$ where $\left(\frac{}{p}\right)$ denotes the Legendre symbol. Put $K_f=Q(a_n | n\geqq 1)$ the coefficient field of the cusp form $f(z)$. Then K_f is an imaginary CM-field. Let F_f denote the maximal real subfield of K_f. We denote by $\mathfrak{o}_K$ (resp. $\mathfrak{o}_F$) the ring of integers in K_f (resp. F_f). Put $2d=[K_f : Q]$. We fix a prime divisor $\tilde{\mathfrak{p}}$ of the algebraic closure $\bar{Q}$ of Q lying over p. Let ρ denote the complex conjugation.

Prime ideals which Shimura considered in [10] [11] are ramified in the relative quadratic extension K_f over F_f, and they are closely related to the

---

Received November 1, 1985.

fundamental unit of the real quadratic field $k=\boldsymbol{Q}(\sqrt{p})$.

The cusp forms we are interested in in this paper are such that the level p is ramified in the coefficient field K_f. In fact we consider the following condition on $f(z)$:

(♯) Both p-th Fourier coefficients of $f(z)$ and $f^\rho(z)$ are divisible by $\tilde{\mathfrak{p}}$, i.e.,

$$a_p \equiv a_p^\rho \equiv 0 \pmod{\tilde{\mathfrak{p}}}.$$

This condition (♯) induces that p is ramified in K_f.

Theorem 0.1. (i) *For $p=229, 257$, there exists a primitive form in $S_2\left(p, \left(\frac{}{p}\right)\right)$ satisfying the condition* (♯).

(ii) *For any p, $29 \leqq p \leqq 760$, $p \neq 229, 257$, there exists no form in $S_2\left(p, \left(\frac{}{p}\right)\right)$ satisfying the condition* (♯).

Let $f(z)$ be the cusp form satisfying the condition (♯). Let $\mathfrak{p}_K$ (resp. $\mathfrak{p}_F$) denote the prime divisor of K_f (resp. F_f) lying under $\tilde{\mathfrak{p}}$. By observing several numerical examples, we notice the following conjecture.

Conjecture 0.1. *The notation being as above, the Fourier coefficient a_l of $f(z)$ satisfies one of the following congruences for any prime l, $l \neq p$:*

$$a_l \equiv \begin{cases} 0 \\ \pm\sqrt{l} \\ \pm 2\sqrt{l} \end{cases} \pmod{\mathfrak{p}_K} \quad \textit{if } \left(\frac{l}{p}\right)=1, \tag{0.1}$$

$$a_l^2 \equiv \begin{cases} 0 \\ \\ -2l \end{cases} \pmod{\mathfrak{p}_K} \quad \textit{if } \left(\frac{l}{p}\right)=-1. \tag{0.2}$$

Moreover, for each type of congruences, there exists some prime l satisfying that type of congruences.

These congruences are considered as an analogous statement to Proposition 7.38 in [10].

Theorem 0.2. *For $p=229, 257$, let $f(z)$ be the cusp form in $S_2\left(p, \left(\frac{}{p}\right)\right)$ satisfying the condition* (♯). *Then Conjecture* 0.1 *is true for these forms.*

We prove this by showing that there exists a cusp form of weight 1 on $\Gamma_0(p^2)$ which is congruent to the above form modulo $\tilde{\mathfrak{p}}$ and of type S_4.

We recall several facts about Shimura's abelian variety. Let A denote the abelian variety rational over $\boldsymbol{Q}$ of dimension $2d$ associated with f. Then via Shimura [10], there exists an abelian subvariety B rational over the real quadratic field k of dimension d such that

$$A=B+B^{\varepsilon}$$

where ε denotes the non-trivial element in $\mathrm{Gal}(k/\boldsymbol{Q})$. We may assume that there exists an injection θ_F from F_f to $\mathrm{End}_{\boldsymbol{Q}} B$ such that $\theta(\mathfrak{o}_F) \subset \mathrm{End}\, B$. Put

$$B[\mathfrak{p}_F]=\{t \in B \mid \theta_F(\mathfrak{p}_F)t=0\}.$$

Let M_B denote the field generated over k by the coordinates of all points in $B[\mathfrak{p}_F]$. Then via $\mathfrak{p}_F$-adic representation of B, we obtain an injective map

$$R\colon \mathrm{Gal}(M_B/k) \longrightarrow GL_2(\mathfrak{o}_F/\mathfrak{p}_F).$$

Let G denote the image of $\mathrm{Gal}(M_B/k)$ by R, and C denote the intersection of G and the center of $GL_2(\mathfrak{o}_F/\mathfrak{p}_F)$.

Theorem 0.3. *The notation being as above, we assume that Conjecture* 0.1 *is true. Then the following statements are valid.*

(i) *G/C is isomorphic to A_4*

(ii) *Let M denote the subfield of M_B corresponding to C and let L denote the subfield of M corresponding to the unique normal subgroup of A_4 of order* 4 *via Galois theory. Then L/k is an unramified abelian cubic extension of k.*

(iii) *The class number of k is divisible by* 3.

We can translate the above result into the result on λ-adic representation associated with cusp forms on $SL_2(\boldsymbol{Z})$. In this case, the image of the Galois group in PGL_2 becomes isomorphic to S_4.

We used FACOM M-382 at Nagoya University Computation Center for these calculations.

Notation

We denote by $\boldsymbol{Z}$, $\boldsymbol{Q}$ and $\boldsymbol{C}$ respectively, the ring of rational integers, the rational 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, x^{ρ} denotes its complex conjugate.

Let K be a field and F a subfield of K. If K is a Galois extension of

F, Gal (K/F) denotes the Galois group of K over F.

Let K be an algebraic number field of finite degree over $\boldsymbol{Q}$. We denote by $\mathfrak{o}_K$ the ring of algebraic integers in K. For any prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$, $\mathfrak{o}_K/\mathfrak{p}$ denotes the residue field of $\mathfrak{o}_K$ modulo $\mathfrak{p}$. G_K denotes the Galois group Gal $(\bar{\boldsymbol{Q}}/K)$. For an abelian variety A, we denote by End (A) the ring of all endomorphism of A and put $\mathrm{End}_{\boldsymbol{Q}}(A)=\mathrm{End}(A)\otimes\boldsymbol{Q}$. For any positive integer n, S_n, A_n denote the symmetric and alternating group of degree n.

§ 1.

Let $f(z)=\sum_{n=1}^{\infty} a_n q^n$ be a primitive cusp form in $S_2\left(p, \left(\frac{}{p}\right)\right)$. Then $f^{\rho}(z)=\sum_{n=1}^{\infty} a_n^{\rho} q^n$ is also a primitive cusp form in $S_2\left(p, \left(\frac{}{p}\right)\right)$. It is well-known that

$$a_n^{\rho}=\left(\frac{n}{p}\right)a_n \qquad \text{if } (n, p)=1, \tag{1.1}$$

$$a_p\cdot a_p^{\rho}=p, \tag{1.2}$$

$$f|_2\begin{bmatrix}0 & -1\\ p & 0\end{bmatrix}=\frac{a_p^{\rho}}{\sqrt{p}}f^{\rho}. \tag{1.3}$$

For any $\tilde{\mathfrak{p}}$-adic integer α in $\bar{\boldsymbol{Q}}$, put $\tilde{\alpha}=\alpha \pmod{\tilde{\mathfrak{p}}}$. We denote by S_k and $\tilde{S}_k$ the space of cusp forms of weight k on $SL_2(\boldsymbol{Z})$ and the space of cusp form mod p attached to S_k. Then it is known that $\tilde{S}_k\subset\tilde{S}_{k+p-1}$. The weight of cusp form mod p h is defined by the smallest integer k such that $h\in\tilde{S}_k$.

For any $g=\sum_{n=1}^{\infty} b_n q^n$ in $S_2\left(p, \left(\frac{}{p}\right)\right)$ such that b_n are $\tilde{\mathfrak{p}}$-adic integers in $\bar{\boldsymbol{Q}}$ for all $n\geqq 1$, put $\tilde{g}=\sum_{n=1}^{\infty}\tilde{b}_n q^n$. Then $\tilde{g}$ is a cusp form mod p.

Lemma 1.1. *The notation being as above, the following statements are equivalent*;

(i) *the weight of* $\tilde{f}$ *is* $(p+3)/2$,

(ii) $a_p^{\rho}\equiv 0 \pmod{\tilde{\mathfrak{p}}}$.

Proof. This is obvious from Theorem 4.2 in [5].

Hence we get

Corollary 1.1. *The following statements are equivalent*;

(i) *both* $\tilde{f}$ *and* $\tilde{f}^{\rho}$ *belong to* $\tilde{S}_{(p+3)/2}$,

(ii) *$f(z)$ satisfies the condition* ($\sharp$).

Remark 1.1. It is not generally known that $\tilde{f} \neq \tilde{f}^{\rho}$ holds for any above f.

Theorem 1.1. *The following statements are equivalent;*

(i) *there exists a primitive cusp form* $f(z)=\sum_{n=1}^{\infty} a_n q^n$ *in* $S_2\left(p, \left(\frac{}{p}\right)\right)$ *satisfying the condition* ($\sharp$).

(ii) *zero is the eigenvalue of the Hecke operator* $\tilde{T}(p)$ *on* $\tilde{S}_{(p+3)/2}$.

Proof. By Lemma 1.1, it follows that (i) induces (ii). We assume that (ii) is true. Then there exists an element $h=\sum_{n=1}^{\infty} b_n q^n$ in $\tilde{S}_{(p+3)/2}$ satisfying

(i) h is a common eigenfunction of all the Hecke operators $\tilde{T}(n)$,

(ii) $b_1=1$ and $b_p=0$.

By using Theorem 1.2 in [5], we know that there exists a primitive cusp form $f(z)=\sum a_n q^n$ in $S_2\left(p, \left(\frac{}{p}\right)\right)$ such that $\tilde{f}=h$, hence $a_p \equiv 0 \pmod{\tilde{\mathfrak{p}}}$. Then it is obvious that $a_p^{\rho} \equiv 0 \pmod{\tilde{\mathfrak{p}}}$ by Lemma 1.1.

Corollary 1.2. *Let* $f(z)=\sum_{n=1}^{\infty} a_n q^n$ *be a primitive cusp form in* $S_2\left(p, \left(\frac{}{p}\right)\right)$ *which satisfies the statement* (i) *in the above Theorem. Assume that* $\tilde{f} \neq \tilde{f}^{\rho}$. *Then the following statements are valid.*

(i) *The multiplicity of* 0 *in the eigenvalues of the Hecke operator* $\tilde{T}(p)$ *on* $\tilde{S}_{(p+3)/2}$ *is greater than* 1.

(ii) *For any prime* l *such that* $\left(\frac{l}{p}\right)=-1$, $-\tilde{a}_l$ *is also the eigenvalue of* $\tilde{T}(l)$ *on* $\tilde{S}_{(p+3)/2}$.

(iii) *For any prime* l *such that* $\left(\frac{l}{p}\right)=1$, *the multiplicity of* $\tilde{a}_l$ *in eigenvalues of* $\tilde{T}(l)$ *on* $\tilde{S}_{(p+3)/2}$ *is greater than* 1.

Proof. The above claims follow easily from the fact that both $\tilde{f}$ and $\tilde{f}^{\rho}$ belong to $\tilde{S}_{(p+3)/2}$.

Theorem 1.2. *Let* $f(z)$ *be a primitive cusp form in* $S_2\left(p, \left(\frac{}{p}\right)\right)$ *satisfying the statement* (ii) *of Theorem* 1.1. *Let* $\mathfrak{p}_K$ *be a prime divisor of* K_f *lying under* $\tilde{\mathfrak{p}}$. *Then* K_f *is ramified at* $\mathfrak{p}_K$.

Proof. From the assumption, it follows that $a_p \equiv a_p^{\rho} \equiv 0 \pmod{\mathfrak{p}_K}$. Since $a_p \cdot a_p^{\rho}=p$, $p \equiv 0 \pmod{\mathfrak{p}_K^2}$. Hence K_f is ramified at $\mathfrak{p}_K$.

§ 2. Proof of Theorem 0.1

The proof is done by inspecting the tables in Appendix. They show

(I) the characteristic polynomial of $\tilde{T}(p)$ on $\tilde{S}_{(p+3)/2}$,

(II) the characteristic polynomial of $\tilde{T}(l)$ on $\tilde{S}_{(p+3)/2}$ for some l when $p=229$ and 257,

(III) the characteristic polynomial of $\tilde{T}(l)$ on $\tilde{S}_{(p+3)/2}$ with $\left(\frac{l}{p}\right)=-1$ for some larger p than those given in (I).

By these tables and Corollary 1.2, we get the proof of Theorem 0.1. We can also see that Conjecture 0.1 is true for these eigenvalues.

Theorem 1.2 says that, for $p=229$ and 257, there is a primitive cusp form f in $S_2\left(p, \left(\frac{}{p}\right)\right)$ such that $\mathfrak{p}_K$ is ramified in $K_f/\boldsymbol{Q}$. But, in fact, $\mathfrak{p}_F$ is already ramified in $F_f/\boldsymbol{Q}$. To see this, we first note that

$$S_2\left(229, \left(\frac{}{229}\right)\right)=\boldsymbol{C}\cdot U^{(2)}\oplus\boldsymbol{C}\cdot U^{(16)}$$

and

$$S_2\left(257, \left(\frac{}{257}\right)\right)=\boldsymbol{C}\cdot U'^{(2)}\oplus\boldsymbol{C}\cdot U'^{(18)},$$

where $U^{(d)}$ and $U'^{(d)}$ denote certain irreducible Hecke modules over $\boldsymbol{Q}$ of dimension d. The characteristic polynomials of $T(2)$, $T(3)$ and $T(5)$ for $p=229$ and $T(2)$ and $T(3)$ for $p=257$ are given in Shimura [11] and Wada [13]. The prime factorization mod p of these characteristic polynomials are as follows:

$p=229$

l	$\left(\frac{l}{p}\right)$	$U^{(2)}$	$U^{(16)}$
3	+1	$(x-1)^2$	$(x^4+165x^3+211x^2+73x+60)^2(x+120)^2$ $(x+31)^2(x+71)^4$

p=257

l	$\left(\frac{l}{p}\right)$	$U'^{(2)}$	$U'^{(18)}$
2	+1	$(x+1)^2$	$(x^3+209x^2+4x+111)^2(x^3+177x^2+7x+235)^2$ $(x+9)^2(x+60)^4$

Hence we know that the primitive cusp form $f(z)$ satisfying the statement (i) of Theorem 1.1 belongs to $\boldsymbol{C}\cdot U^{(16)}$ (resp. $\boldsymbol{C}\cdot U'^{(18)}$) for p=229 (resp. 257). For p=229, the maximal real subfield F_f of K_f is generated by a_3 and its minimal polynomial has discriminant $2^6\cdot 3^4\cdot 71^2\cdot 229\cdot 659\cdot 297779$. For p=257, F_f is generated by a_2 and the discriminant of its minimal polynomial is $-2^{10}\cdot 11\cdot 257\cdot 8950888981849$. Hence $\mathfrak{p}_F$ is already ramified in $F_f/\boldsymbol{Q}$. It is expected that this is the case for all $f(z)$ satisfying the condition (♯). These primes are contrary to the ones considered by Shimura in [10] and [11].

Remark 2.1. The primes such that $29\leqq p\leqq 2089$ and the class number of $\boldsymbol{Q}(\sqrt{p})$ is divisible by 3 are 229. 257, 733, 761, 1129, 1229, 1373, 1489, 1901 and 2089. By extended calculations, cusp forms with the property (♯) seem to exist when $p=761$, 1129, 1229, 1489 and 2089. All eigenvalues that we have calculated for these forms satisfy Conjecture 0.1. But there is no such forms for the other primes in the above list.

§ 3. Proof of Theorem 0.3

Let $f(z)=\sum_{n=1}^{\infty} a_n q^n$ be a primitive cusp form in $S_2\left(p, \left(\frac{}{p}\right)\right)$. We assume that Conjecture 0.1 is true for $f(z)$ in this section. To prove Theorem 0.3, it is convenient to consider a primitive cusp form $g(z)=\sum_{n=1}^{\infty} b_n q^n$, $b_1=1$ in $S_{(p+3)/2}$ such that

$$a_n \equiv b_n \pmod{\tilde{\mathfrak{p}}} \qquad \text{for all } n\geqq 1,$$

at the same time.

Proposition 3.1. *The notation being as above, we have*

$$b_l^2\cdot l^{-(p+1)/2}\equiv 0,\ 1,\ 2,\ \textit{or}\ 4 \pmod{\tilde{\mathfrak{p}}}$$

for all prime $l\neq p$.

Proof. Since $\left(\frac{l}{p}\right)\equiv l^{(p-1)/2} \pmod{p}$, these are obvious from (0.1) and (0.2).

Put $E=\boldsymbol{Q}(b_n|n\geqq 1)$ and let λ denote the prime divisor of E lying under $\tilde{\mathfrak{p}}$. We consider the reduction mod λ of the λ-adic representation of $G_{\boldsymbol{Q}}$ associated with $g(z)$. Namely, there exists a continuous homomorphism

$$\phi\colon G_{\boldsymbol{Q}}\longrightarrow GL_2(\mathfrak{o}_E/\lambda)$$

which is unramified outside p and $\phi(\sigma_l)$ has characteristic polynomial

$$X^2 - b_l X + l^{(p+1)/2} \pmod{\lambda} \tag{3.1}$$

for any prime $l \neq p$. Here σ_l denotes a Frobenius element of l in G_Q. Let G' denote the image of G_Q by ϕ and let H' denote the image of G' in $PGL_2(\mathfrak{o}_E/\lambda)$.

We assume that $\mathfrak{o}_E/\lambda \cong \boldsymbol{F}_p$. Then, by virtue of Corollary 1 in [12] and Proposition 3.1, we conclude that H' is isomorphic to S_4. However, it does not hold in general that $\mathfrak{o}_E/\lambda \cong \boldsymbol{F}_p$.

Hence we need to consider a p-adic representation of G_k obtained from Shimura's abelian variety.

We recall Shimura's theory for the abelian variety associated with cusp forms.

Let $f(z) = \sum_{n=1}^{\infty} a_n q^n$, $a_1 = 1$, be a primitive cusp form in $S_2\left(p, \left(\frac{}{p}\right)\right)$. By virtue of [10], we obtain an abelian variety A of dimension $2d$ and an isomorphism θ of K_f into $\mathrm{End}_Q(A)$. A and $\theta(a)$ for all $a \in K_f$ are rational over $\boldsymbol{Q}$. Further, A has an automorphism μ rational over $k = \boldsymbol{Q}(\sqrt{p})$ such that

$$\mu^2 = 1,$$
$$\mu \cdot \theta(a) = \theta(a^\rho) \cdot \mu \qquad \text{for all } a \in K_f,$$
$$\mu^\varepsilon = -\mu$$

where ε denotes the generator of $\mathrm{Gal}(k/\boldsymbol{Q})$. Put

$$B = (1+\mu)A.$$

Then B is an abelian subvariety of A rational over k, and

$$A = B + B^\varepsilon.$$

We can define an injection θ_F of F_f into $\mathrm{End}_Q(B)$ such that $\theta_F(a)$ is the restriction of $\theta(a)$ to B for all $a \in F_f$. Changing (A, θ) by an isogeny over $\boldsymbol{Q}$ if necessary, we may assume that

$$\theta(\mathfrak{o}_K) \subset \mathrm{End}(A), \qquad \theta_F(\mathfrak{o}_F) \subset \mathrm{End}(B).$$

Hereafter we assume that Conjecture 0.1 is valid for $f(z)$, and we are interested in the points of B annihilated by $\theta_F(\mathfrak{p}_F)$. Put

$$B[\mathfrak{p}_F] = \{t \in B \mid \theta_F(\mathfrak{p}_F)t = 0\}.$$

Then $B[\mathfrak{p}_F]$ is isomorphic to $(\mathfrak{o}_F/\mathfrak{p}_F)^2$ as $\mathfrak{o}_F$-module. We denote by M_B the fields generated over k by the coordinates of the points in $B[\mathfrak{p}_F]$. These are Galois extensions over k. Taking a basis of $B[\mathfrak{p}_F]$ as $\mathfrak{o}_F$-module, we obtain a representation R

$$R\colon \mathrm{Gal}\,(M_B/k) \longrightarrow GL_2(\mathfrak{o}_F/\mathfrak{p}_F)$$

satisfying that

$$\det(X-R(\sigma_{\mathfrak{l}})) \equiv \begin{cases} X^2 - a_l X + l \pmod{\tilde{\mathfrak{p}}} & \text{if } \left(\dfrac{l}{p}\right)=1, \\ X^2-(a_l^2+2l)X+l^2 \pmod{\tilde{\mathfrak{p}}} & \text{if } \left(\dfrac{l}{p}\right)=-1. \end{cases}$$

where $\mathfrak{l}$ is a prime divisor of k over l and $\sigma_{\mathfrak{l}}$ denotes a Frobenius element in $\mathrm{Gal}\,(M_B/k)$ of $\mathfrak{l}$.

By virtue of congruences (0.1) and (0.2) in Conjecture 0.1, we see that all coefficients of $\det(X-R(\sigma_{\mathfrak{l}}))$ belong to $\boldsymbol{F}_p$. Hence, by Lemma 6.13 in [1], there is a semi-simple representation R'

$$R'\colon G_k \longrightarrow GL_2(\boldsymbol{F}_p)$$

such that $\det(X-R'(\sigma_{\mathfrak{l}}))=\det(X-R(\sigma_{\mathfrak{l}}))$ for all $\mathfrak{l}$.

By virtue of Conjecture 0.1, we see that R is not reducible. Hence R is isomorphic to R' by Lemma 3.2 in [1].

With these preparations, we can prove Theorem 0.3 as follows. The notation is the same as in Introduction. By the above argument, G is considered to be a subgroup of $GL_2(\boldsymbol{F}_p)$. Then by virtue of Conjecture 0.1 and Lemma 2 in [12], we know that G/C is isomorphic to A_4 or S_3. On the other hand R is isomorphic to the restriction of ϕ to $\mathrm{Gal}\,(\bar{\boldsymbol{Q}}/k)$. Hence we know that H' has a subgroup of index 2 which is isomorphic to G/C. So the order of G' is prime to p. Therefore, by the classification theorem of finite group contained in $GL_2(F)$ where F is a finite field, we conclude that

(3.2) $\qquad G/C$ is isomorphic to A_4,

(3.3) $\qquad H'$ is isomorphic to S_4.

The statement (iii) follows from the similar argument in pages 34 and 35 in [12]. This completes the proof.

Corollary 3.1. *The notation being as above, it holds that H' is isomorphic to S_4.*

Proof. This is obvious from the above argument.

§ 4. Proof of Theorem 0.2

In this section we shall give the proof of Theorem 0.2. The method is the same as in K. Haberland [3] where he showed that the prime 59 is an exceptional prime of type S_4 for the cusp form ΔQ of weight 16 on $SL_2(Z)$ (see also H.P.F. Swinnerton-Dyer [12]).

Let $p=229$ or 257. Let $k=Q(\sqrt{p})$ and L the absolute class field of k. Since the class number of k is 3, the degree of L over k is 3 and L is a Galois extension over Q with the Galois group isomorphic to S_3.

We take a prime ideal $\tilde{\mathfrak{p}}$ over p in $\bar{Q}$ anp fix it. Let χ_p denote the Teichmüller character for $\tilde{\mathfrak{p}}$ i.e.

$$\chi_p(l)\equiv l \bmod \tilde{\mathfrak{p}}$$

for all l prime to p.

Let χ be a Dirichlet character mod p and let

$$E_{1,\chi}(z)=1-\frac{2}{B_{1,\chi}}\sum_{n=1}^{\infty}\sum_{d\mid n}\chi(d)q^n$$

where $B_{1,\chi}$ is the generalized Bernoulli number. Then $E_{1,\chi}$ is a modular form of weight 1 on $\Gamma_0(p)$ with character χ. It is well known that

$$E_{1,\chi_p^{-1}}\equiv 1 \qquad \bmod \tilde{\mathfrak{p}}.$$

In order to prove our theorem, we first construct a Galois extension M over Q satisfying the following condition:

(4.1) M is unramified at all finite primes outside p,

(4.2) $\mathrm{Gal}\,(M/Q)\cong S_4$.

We should remark that, when $p=229$, Tate constructed such extensions and showed the existence of cusp forms f_1, f_2 of type S_4 on $\Gamma_0(229)$ of weight 1. In [9] 8.2, Serre showed that f_1, f_2, f_1^ρ, f_2^ρ are the basis of this space. But we know that all θ-transforms of these forms are not congruent to $f(z)$ in Theorem 0.2. Therefore we have to search for cusp forms of weight 1 on $\Gamma_0(229^2)$.

We put

$$F_{229}(x)=x^3-4x-1$$

and

$$F_{257}(x)=x^3+2x^2-3x-1.$$

The field L is the splitting field of $F_p(x)$ over $\boldsymbol{Q}$. Let $x_i^{(p)}$ $(i=1, 2, 3)$ be the roots of $F_p(x)=0$, and let M be the field generated by all $\sqrt{x_i^{(p)}}$. Then M is a Galois extension over $\boldsymbol{Q}$ with the Galois group S_4. We denote by $\mathfrak{p}_M$ (resp. $\mathfrak{p}_L$) the prime ideal under $\tilde{\mathfrak{p}}$ in M (resp. L). We will write x_i for $x_i^{(p)}$ if there is no fear of confusion.

Lemma 4.1. *Let the notation be as above and let Z and T denote the decomposition and inertia group for $\mathfrak{p}_M$ respectively. Then the following statements are valid.*

(i) *M satisfies* (4.1),

(ii) *M is unramified over L at $\mathfrak{p}_L$,*

(iii) *Z is an abelian group of type* (2, 2) *generated by two transpositions, and T is a subgroup of index* 2.

Proof. (i) It is clear that M is unramified over $\boldsymbol{Q}$ at $l\neq 2, p$. For $l=2$, we note first that L is unramified over $\boldsymbol{Q}$ at 2. On the other hand, we have

$$x_i=(x_i^2-2)^2-4\equiv(x_i^2-2)^2 \bmod 4 \qquad \text{for } p=229,$$

and

$$x_i=x_i^2((x_i+1)^2-4)\equiv[x_i(x_i+1)]^2 \bmod 4 \qquad \text{for } p=257.$$

By Kummer theory any prime over 2 is unramified in $L(\sqrt{x_i})/L$ for all i, therefore 2 is unramified in $M/\boldsymbol{Q}$.

(ii) It is clear because the $\mathfrak{p}_L$-exponent of (x_i) is zero for any i.

(iii) By (ii) and the group theoretical considerations, the structures of Z and T are one of the following types:

(a) $Z=\{1, \sigma, \tau, \sigma\tau\}$ $T=\{1, \sigma\}$ where σ and τ are transpositions and $\sigma\tau=\tau\sigma$.

(b) $Z=T=\{1, \sigma\}$ for some transposition σ.

But we have

$$F_{229}(x)\equiv(x-58)(x-200)^2 \bmod 229, \quad \left(\frac{58}{229}\right)=1, \quad \left(\frac{200}{229}\right)=-1$$

and

$$F_{257}(x)\equiv(x-18)(x-247)^2 \bmod 257, \quad \left(\frac{18}{257}\right)=1, \quad \left(\frac{247}{257}\right)=-1.$$

Therefore the case (b) is impossible. q.e.d.

We fix an embedding of Gal (M/Q) into $PGL_2(C)$ and get a projective representation

$$\tilde{\rho}\colon \text{Gal}(\bar{Q}/Q) \longrightarrow PGL_2(C).$$

This is essentially unique because any two embeddings of S_4 in $PGL_2(C)$ are conjugate. The conductor of $\tilde{\rho}$ is p^2 by Serre [9] Section 6. Furthermore, $\tilde{\rho}$ has a lifting

$$\rho\colon \text{Gal}(\bar{Q}/Q) \longrightarrow GL_2(C)$$

such that

(4.3) ρ is odd and tamely ramified at p,

(4.4) the conductor of ρ is p^2,

(4.5) the conductor of $\varepsilon = \det \rho$ is p.

We can regard ε as a Dirichlet character mod p. Since the Artin conjecture is proved by Langlands [7] for this case, we get, by the theorem of Weil-Langlands, the following

Lemma 4.2. *There exists a primitive form $h(z) = \sum_{n=1}^{\infty} c_n q^n$ in $S_1(p^2, \varepsilon)$ such that*

(i) $c_l = \text{tr}\,\rho(\sigma_l)$, $\varepsilon(l) = \det \rho(\sigma_l)$ *for any $l \neq p$, where σ_l is a Frobenius element of l,*

(ii) $$\frac{c_l^2}{\varepsilon(l)} = \begin{cases} 4 & \textit{if } \tilde{\rho}(\sigma_l) \textit{ is of order } 1, \\ 0 & \quad '' \quad 2, \\ 1 & \quad '' \quad 3, \\ 2 & \quad '' \quad 4. \end{cases}$$

Hereafter we will denote by $\delta(l)$ the right hand side of (ii).

Let $\varepsilon = \chi_p^m$. As $\varepsilon(-1) = -1$, m is an odd number. We have

$$h \cdot E_{1,\chi_p^{-1}} \equiv h \mod \tilde{\mathfrak{p}},$$

$$h \cdot E_{1,\chi_p^{-1}} | T(l) \equiv c_l h \cdot E_{1,\chi_p^{-1}} \mod \tilde{\mathfrak{p}},$$

hence there exists a cusp form $g(z) = \sum_{n=1}^{\infty} b'_n q^n \in S_2(p^2, \chi_p^{m-1})$ such that g is a common eigenfunction for all $T(l)$ $l \neq p$, and $b'_n \equiv c_n \mod \tilde{\mathfrak{p}}$.

Put $\xi = \chi_p^{-(m-1)/2}$ and $g_\xi = \sum_{n=1}^{\infty} \xi(n) b'_n q^n$ the ξ-twist of g. g_ξ belongs to $S_2(p^2)$. The Fourier coefficients of $g_\xi = \sum_{n=1}^{\infty} b_n q^n$ satisfy the following congruences:

$$b_l \equiv l^{-(m-1)/2} c_l \mod \tilde{\mathfrak{p}}.$$

Hence the property (ii) of Lemma 4.2 is equivalent to

(4.6) $$\frac{b_l^2}{l} \equiv \delta(l) \mod \tilde{\mathfrak{p}}.$$

Let $\mathscr{A}$ be the ring generated by all Hecke operators mod p $\widetilde{T(l)}$ with $l \neq p$, and $\tilde{\mathscr{A}} = \mathscr{A} \otimes \bar{F}_p$. Let θ be the operator on $F_p[[q]]$ defined by

$$\theta\left(\sum_{n=1}^{\infty} a_n q^n\right) = \sum_{n=1}^{\infty} n a_n q^n.$$

According to Koike [6], the components of $\tilde{\mathscr{A}}$-module $\widetilde{S_2(p^2)}$ are given by

$$\theta^{p-\kappa} \tilde{S}_{2\kappa} \qquad 2 \leq \kappa \leq (p-1)/2$$

and

$$\langle E_{(a)} \rangle \qquad 2 \leq a \leq (p-3)/2,$$

where $E_{(a)} = \sum_{n=1}^{\infty} c_a(n) q^n$ with

$$c_a(n) = \begin{cases} \sum_{d|n, d>0} d^a \left(\frac{n}{d}\right)^{1-a} & \text{if } p \nmid n \\ 0 & \text{if } p \mid n. \end{cases}$$

It is easy to see that any $E_{(a)}$ does not satisfy the congruence relation (4.6). So that we only have to look for the weight t such that there exists a cusp form $G(z) = \sum_{n=1}^{\infty} a_n q^n \in S_t$ with

(4.7) $$\frac{l^{p+1-t} a_l^2}{l} \equiv \delta(l) \mod \tilde{\mathfrak{p}}.$$

First we consider the case $p=229$, Put $l=3$ and 5. The decomposition group for a prime over l is cyclic. On the other hand, $F_{229}(x) \mod l$ is an irreducible polynomial of degree 3, so $\tilde{\rho}(\sigma_l)$ is of order 3. Thus the coefficient b_l satisfies

$$b_l^2 \equiv l \mod \tilde{\mathfrak{p}}.$$

By direct calculations we see that only in $\tilde{S}_{58}$, $\tilde{S}_{116}$ and $\tilde{S}_{172}$ there exist forms with the required congruence. We list the Fourier coefficients mod 229 of the forms in $\tilde{S}_{58}$ and $\tilde{S}_{172}$ in the following table.

l \ form \ t	58		172	
	h_1	h_2	h_3	h_4
2	0	123	0	108
3	1	228	1	228

5	122	122	107	107
7	121	0	106	0
11	107	107	122	122
13	106	0	121	0
17	1	228	1	228
19	228	1	228	1
23	123	106	108	121
29	0	0	0	0
31	0	106	0	121
229	122	1	107	1

Next we take $l=13$. Since

$$F_{229}(x)\equiv(x^2+5x+8)(x+8) \bmod 13$$

and

$$F_{229}(x^2)\equiv(x^4+5x^2+8)(x^2+8) \bmod 13,$$

where each factor of the right hand sides is irreducible over $\boldsymbol{F}_{13}$, $\tilde{\rho}(\sigma_l)$ has order 4. Thus $b_l^2\equiv 2l \bmod \tilde{\mathfrak{p}}$. But the Fourier coefficients of h_2 and h_4 are zero mod 229, which contradicts the above congruence. For the forms h_1 and h_3, we take $l=31$. Similarly we have

$$F_{229}(x)\equiv(x^2+21x+3)(x+10) \bmod 31,$$

and

$$F_{229}(x^2)\equiv(x^4+21x^2+3)(x^2+10) \bmod 31,$$

where each factor of the right hand sides is irreducible over $\boldsymbol{F}_{31}$. By the same reason, the forms h_1 and h_3 are not compatible with our congruence.

Consequently there must be a cusp form $G(z)=\sum_{n=1}^{\infty} a_n q^n \in S_{116}$ such that

$$b_l^2\equiv l^{114}a_l^2\equiv\left(\frac{l}{229}\right)a_l^2 \quad \bmod \tilde{\mathfrak{p}}, \text{ for any prime } l,\ l\neq p.$$

Next we consider the case $p=257$. $F_{257}(x) \bmod l$ is an irreducible polynomial of degree 3 for $l=11$ and 13. So $\tilde{\rho}(\sigma_l)$ has order 3. This time only S_{130} has the forms with congruence relation:

$$l^{258-t}a_l^2 \equiv l \bmod \tilde{\mathfrak{p}}$$

for $l=11$ and 13. Hence there is a form $G(z)=\sum_{n=1}^{\infty} a_n q^n \in S_{130}$ such that

$$b_l^2 \equiv l^{128} a_l^2 \equiv \left(\frac{l}{257}\right) a_l^2 \bmod \tilde{\mathfrak{p}}.$$

If $\left(\frac{l}{p}\right)=1$ (resp. -1), the order of $\tilde{\rho}(\sigma_l)$ is 1, 2 or 3 (resp. 2 or 4). Since $G(z)$ is congruent to $f(z)$ or $f^\rho(z)$ modulo $\tilde{\mathfrak{p}}$, we get (0.1) and (0.2). This completes the proof of Theorem 0.2.

Remark 4.1. If $a_l \equiv \pm 2\sqrt{l} \bmod \tilde{\mathfrak{p}}$, $\tilde{\rho}(\sigma_l)$ is an identity element. For $l \leq 691$, there are three such l's, i.e.

$$l=193, \quad 509 \quad \text{and } 593 \quad \text{for } p=229$$

and

$$l=157, \quad 643 \quad \text{and } 653 \quad \text{for } p=257.$$

In fact, for these cases, $F_p(x^2) \bmod l$ is completely reducible. For example,

$$a_{193} \equiv 90 \bmod \tilde{\mathfrak{p}},$$
$$F_{229}(x) \equiv (x-42)(x-157)(x-187) \bmod 193,$$
$$\left(\frac{42}{193}\right)=\left(\frac{157}{193}\right)=\left(\frac{187}{193}\right)=1$$

for $p=229$ and

$$a_{157} \equiv 63 \bmod \tilde{\mathfrak{p}},$$
$$F_{257}(x) \equiv (x-25)(x-49)(x-81) \bmod 157$$

for $p=257$.

Remark 4.2. The forms in the above table are congruent to the forms constructed by Tate. It is easily seen that $h_1 \equiv f_1$, $h_2 \equiv f_2 \bmod \tilde{\mathfrak{p}}$ where f_i is the forms stated in Serre [9] 8.2, and $h_3 \equiv f_1^\rho$, $h_4 \equiv f_2^\rho \bmod \tilde{\mathfrak{p}}$. But we must note that in Tate's case, $\mathfrak{p}_M$ is ramified over L and the decomposition group is cyclic of order 4.

Remark 4.3. For $p=229$ and 257, the field M constructed in this section coincides with that given in Theorem 0.3.

Appendix

Table (I)

p:=prime w:=weight $(p+3)/2$
$\tilde{H}_p(x)$:=factorization mod p of the characteristic polynomial of $T(p)$ on S_w

p	w	$\tilde{H}_p(x)$
29	16	$x+6$
37	20	$x+2$
41	22	$x+6$
53	28	$x^2+12x+17$
61	32	$(x+9)(x+44)$
73	38	$x^2+16x+57$
89	46	$(x+12)(x^2+79x+79)$
97	50	$x^3+24x^2+37x+38$
101	52	$(x+100)(x^3+86x^2+61x+64)$
109	56	$(x+2)(x+19)(x^2+72x+38)$
113	58	$(x+26)(x+88)(x^2+19x+105)$
137	70	$(x^2+31x+75)(x^3+120x^2+50x+64)$
149	76	$(x+27)(x^5+112x^4+139x^3+67x^2+83x+87)$
157	80	$(x+22)(x^5+143x^4+152x^3+122x^2+109x+31)$
173	88	$(x^2+16x+157)(x^5+24x^4+30x^3+83x^2+121x+151)$
181	92	$(x^2+9x+95)(x^5+154x^4+12x^3+2x^2+37x+93)$
193	98	$(x+11)(x^2+107x+68)(x^2+160x+20)(x^2+168x+123)$
197	100	$(x+23)(x+194)(x^2+95x+158)(x^4+72x^3+6x^2+63x+152)$
229	116	$x^2(x+69)(x+110)(x+215)(x^4+64x^3+14x^2+195x+176)$
233	118	$x^9+4x^8+35x^7+147x^6+41x^5+196x^4+207x^3+133x^2+88x+216$
241	122	$(x^3+43x^2+169x+209)(x^6+25x^5+145x^4+95x^3+110x^2+233x+129)$
257	130	$x^2(x+30)(x+163)(x^3+85x^2+247x+5)(x^3+252x^2+178x+118)$
269	136	$(x^4+63x^3+175x^2+18x+46)\times$ $(x^7+210x^6+233x^5+108x^4+98x^3+88x^2+172x+69)$

277	140	$(x^2+180x+182)(x^4+197x^3+60x^2+273x+112)\times$ $(x^5+185x^4+263x^3+207x^2+237x+18)$
281	142	$(x^4+76x^3+29x^2+185x+269)\times$ $(x^7+203x^6+127x^4+140x^3+243x^2+197x+271)$
293	148	$(x+83)(x+206)(x^2+205x+40)\times$ $(x^8+136x^7+281x^6+287x^5+131x^4+287x^3+206x^2+51x+279)$
313	158	$(x+60)(x^2+36x+66)(x^2+56x+292)(x^2+173x+306)\times$ $(x^2+213x+59)(x^3+172x^2+173x+53)$
373	188	$(x+311)(x+371)^2(x^6+143x^5+56x^4+252x^3+123x^2+347x+48)\times$ $(x^6+302x^5+282x^4+330x^3+75x^2+156x+348)$
401	202	$(x+288)(x^2+242x+98)(x^{13}+288x^{12}+81x^{11}+372x^{10}+68x^9+112x^8$ $+337x^7+202x^6+45x^5+132x^4+241x^3+275x^2+141x+252$

Table (II)

(i) $p:=229$ $w:=116$

$\tilde{H}_l(x)$: =factorization mod 229 of the characteristic polynomial of $T(l)$ on S_{116}

l	$\left(\frac{l}{p}\right)$	$\tilde{H}_l(x)$		
2	-1	$x+15$	$x+214$	$(x+37)(x+53)(x+120)(x^4+48x^3+32x^2+146x+197)$
3	$+1$	$x+71$	$x+71$	$(x+31)(x+120)(x+228)(x^4+165x^3+211x^2+73x+60)$
5	$+1$	$x+66$	$x+66$	$(x+17)(x+120)(x+226)(x^4+195x^3+9x^2+208x+216)$
7	-1	$x+98$	$x+131$	$x(x+133)(x+196)(x^4+137x^3+135x^2+192x+80)$
11	$+1$	$x+195$	$x+195$	$(x+177)(x+186)(x+226)(x^4+167x^3+156x^2+88x+201)$
13	-1	$x+64$	$x+165$	$x(x+44)(x+190)(x^4+179x^3+38x^2+102x+83)$
17	$+1$	$x+186$	$x+186$	$(x+3)(x+25)(x+101)(x^4+182x^3+54x^2+198x+102)$
19	$+1$	$x+83$	$x+83$	$(x+1)(x+106)(x+136)(x^4+51x^3+89x^2+135x+174)$
23	-1	x	x	$(x+19)(x+128)(x+155)(x^4+96x^3+56x^2+131x+87)$
29	-1	x	x	$(x+74)(x+142)(x+155)(x^4+4x^3+26x^2+54x+153)$
31	-1	$x+204$	$x+25$	$x(x+9)(x+125)(x^4+18x^3+66x^2+73x+131)$
37	$+1$	x	x	$(x+103)(x+215)(x+227)(x^4+157x^3+49x^2+16x+44)$
41	-1	$x+190$	$x+39$	$(x+146)(x+155)(x+208)(x^4+147x^3+183x^2+225x+21)$
53	$+1$	x	x	$(x+20)(x+205)(x+223)(x^4+18x^3+161x^2+90x+198)$
193	$+1$	$x+139$	$x+139$	$(x+24)(x+111)(x+215)(x^4+38x^3+171x^2+46x+72)$

229	0	x	x	$(x+69)(x+110)(x+215)(x^4+64x^3+14x^2+195x+176)$
509	+1	$x+152$	$x+152$	$(x+73)(x+212)(x+223)(x^4+92x^3+107x^2+55x+215)$
593	+1	$x+178$	$x+178$	$(x+120)(x+151)(x+223)(x^4+125x^3+223x^2+8x+225)$

(ii) $p:=257$ $w:=130$

$\tilde{H}_l(x):=$factorization mod 257 of the characteristic polynomial of $T(l)$ on S_{130}

l	$\left(\frac{l}{p}\right)$	$\tilde{H}_l(x)$	
2	+1	$(x+60)^2$	$(x+1)(x+9)(x^3+177x^2+7x+235)(x^3+209x^2+4x+111)$
3	−1	x^2+6	$(x+68)(x+234)(x^3+76x^2+51x+66)(x^3+200x^2+242x+215)$
5	−1	x^2+10	$(x+121)(x+188)(x^3+80x^2+46x+166)(x^3+106x^2+119x+56)$
7	−1	x^2+14	$(x+18)(x+68)(x^3+38x^2+180x+250)(x^3+195x^2+83x+166)$
11	+1	$(x+221)^2$	$x(x+103)(x^3+24x^2+249x+135)(x^3+202x^2+136x+65)$
13	+1	$(x+229)^2$	$(x+56)(x+255)(x^3+27x^2+90x+116)(x^3+236x^2+225x+94)$
17	+1	$(x+187)^2$	$(x+111)(x+253)(x^3+81x^2+152x+202)(x^3+217x^2+17x+221)$
19	−1	x^2	$(x+94)(x+204)(x^3+218x^2+197x+254)(x^3+233x^2+234x+159)$
23	+1	$(x+199)^2$	$(x+67)(x+253)(x^3+143x^2+223x+121)(x^3+173x^2+26x+163)$
29	+1	$(x+172)^2$	$(x+91)(x+253)(x^3+111x^2+171x+82)(x^3+222x^2+110x+7)$
31	+1	$(x+206)^2$	$x(x+51)(x^3+82x^2+86x+175)(x^3+217x^2+138x+194)$
37	−1	x^2+74	$(x+106)(x+160)(x^3+79x^2+97x+45)(x^3+99x^2+153x+91)$
41	−1	x^2	$x(x+248)(x^3+39x^2+171x+179)(x^3+161x^2+188x+71)$
61	+1	x^2	$(x+12)(x+36)(x^3+68x^2+12x+152)(x^3+147x^2+246x+170)$
67	+1	x^2	$(x+12)(x+200)(x^3+72x^2+94x+148)(x^3+233x^2+69x+91)$
157	+1	$(x+194)^2$	$(x+235)(x+253)(x^3+15x^2+192x+115)(x^3+125x^2+69x+162)$
257	0	x^2	$(x+30)(x+163)(x^3+85x^2+247x+5)(x^3+252x^2+178x+118)$
643	+1	$(x+60)^2$	$(x+2)(x+40)(x^3+31x^2+29x+242)(x^3+58x^2+119x+185)$
653	+1	$(x+82)^2$	$(x+142)(x+253)(x^3+213x^2+143x+196)(x^3+236x^2+75x+15)$

Table (III)

p:=prime w:=weight $(p+3)/2$

$\tilde{H}_l(x)$:=factorization mod p of the characteristic polynomial of $T(l)$ of on S_w with $\left(\frac{l}{p}\right)=-1$

p	w	l	$\tilde{H}_l(x)$
317	160	3	$(x^2+294x+108)(x^{11}+200x^{10}+54x^9+180x^8+237x^7+201x^6+231x^5+121x^4+170x^3+163x^2+226x+217)$
337	170	5	$(x+282)(x^5+225x^4+174x^3+166x^2+255x+74)\times(x^7+177x^6+68x^5+315x^4+288x^3+58x^2+153x+260)$
349	176	2	$x(x^5+54x^4+143x^3+320x^2+334x+152)\times(x^8+11x^7+176x^6+311x^5+104x^4+21x^3+157x^2+139x+135)$
		7	$(x+237)(x^5+232x^4+45x^3+294x^2+248x+290)\times(x^8+45x^7+185x^6+180x^5+309x^4+201x^3+139x^2+233x+92)$
353	178	5	$(x+100)(x^2+344x+66)(x^4+327x^3+104x^2+73x+77)\times(x^7+350x^6+314x^5+214x^4+68x^3+324x^2+278x+233)$
373	188	2	$(x+104)(x+269)(x+355)(x^6+11x^5+309x^4+200x^3+52x^2+212x+329)\times(x^6+212x^5+214x^4+366x^3+119x^2+175x+248)$
		5	$(x+58)(x+165)(x+208)(x^6+108x^5+138x^4+290x^3+330x^2+353x+202)(x^6+366x^5+354x^4+201x^3+128x^2+329x+129)$
		11	$x(x+41)(x+145)(x^6+313x^5+137x^4+256x^3+129x^2+285x+161)\times(x^6+365x^5+269x^4+198x^3+347x^2+253x+128)$
389	196	3	$(x+86)(x+378)(x^7+235x^6+129x^5+297x^4+203x^3+60x^2+182x+255)\times(x^7+312x^6+202x^5+247x^4+197x^3+99x^2+227x+98)$
397	200	5	$(x+126)(x+294)(x^4+52x^3+137x^2+27x+13)(x^{10}+335x^9+151x^8+345x^7+110x^6+239x^5+384x^4+377x^3+61x^2+200x+136)$
401	202	3	$(x+1)(x^2+167x+338)(x^{13}+336x^{12}+116x^{11}+290x^{10}+11x^9+322x^8+394x^7+77x^6+388x^4+298x^4+23x^3+312x^2+212x+285)$
409	206	7	$(x+110)(x+196)(x^{14}+201x^{13}+136x^{12}+134x^{11}+168x^{10}+197x^9+244x^8+227x^7+196x^6+353x^5+70x^4+321x^2+49x+232)$
421	212	2	$(x+117)(x+407)(x^2+338x+340)(x^{13}+272x^{12}+335x^{11}+242x^{10}+401x^9+386x^8+318x^7+345x^6+236x^5+349x^4+274x^3+13x^2+261x+162)$
433	218	5	$(x^5+50x^4+420x^3+306x^2+205x+72)(x^5+83x^4+332x^3+136x^2+108x+35)(x^7+268x^6+76x^5+43x^4+123x^3+29x^2+318x+18)$
449	226	3	$(x^2+240x+373)(x^2+294x+161)(x^3+340x^2+238x+384)(x^{11}+17x^{10}+367x^9+267x^8+43x^7+158x^6+292x^5+87x^4+89x^3+283x^2+341x+404)$

457	230	5	$(x+58)(x+437)(x^2+407x+178)(x^{14}+364x^{13}+28x^{12}+388x^{11}+357x^{10}$ $+271x^9+106x^8+386x^7+350x^6+392x^5+82x^4+125x^3+224x^2+198x$ $+355)$
461	232	2	$(x+220)(x^5+356x^4+22x^3+193x^2+43x+12)(x^6+397x^5+455x^4$ $+247x^3+322x^2+225x+368)(x^7+89x^6+237x^5+134x^4+36x^3$ $+101x^2+295x+263)$
509	256	2	$(x+356)(x^{20}+10x^{19}+334x^{18}+52x^{17}+x^{16}+252x^{15}+24x^{14}+455x^{13}$ $+83x^{12}+316x^{11}+407x^{10}+463x^9+487x^8+465x^7+287x^6+408x^5$ $+128x^4+447x^3+318x^2+36x+113)$
521	262	3	$(x+374)(x+432)(x^{19}+335x^{18}+66x^{17}+72x^{16}+206x^{15}+332x^{14}+78x^{13}$ $+408x^{12}+48x^{11}+207x^{10}+459x^9+98x^8+342x^7+387x^6+174x^5$ $+202x^4+101x^3+351x^2+511x+186)$
541	272	2	$(x+71)(x^8+29x^7+435x^6+31x^5+371x^4+91x^3+334x^2+430x+80)\times$ $(x^{13}+454x^{12}+374x^{11}+478x^{10}+63x^9+226x^8+43x^7+82x^6+10x^5$ $+347x^4+368x^3+280x^2+313x+391)$
557	280	2	$(x+376)(x^2+455x+424)(x^3+105x^2+387x+398)(x^{17}+497x^{16}+547x^{15}$ $+327x^{14}+258x^{13}+260x^{12}+141x^{11}+184x^{10}+262x^9+503x^8+278x^7$ $+14x^6+331x^5+123x^4+64x^3+157x^2+211x+528)$
569	286	3	$x^{23}+90x^{22}+116x^{21}+421x^{20}+110x^{19}+25x^{18}+12x^{17}+568x^{16}+108x^{15}$ $+92x^{14}+332x^{13}+303x^{12}+67x^{11}+553x^{10}+519x^9+416x^8+555x^7$ $+87x^6+442x^5+497x^4+38x^3+109x^2+239x+146$
577	290	5	$(x^2+236x+344)(x^5+379x^4+432x^3+202x^2+199x+110)\times$ $(x^{16}+68x^{15}+16x^{14}+85x^{13}+95x^{12}+538x^{11}+145x^{10}+511x^9$ $+78x^8+275x^7+187x^6+345x^5+293x^4+219x^3+559x^2+208x+131)$
593	298	3	$(x^{11}+498x^{10}+185x^9+533x^8+487x^7+112x^6+46x^5+111x^4+274x^3$ $+294x^2+165x+455)(x^{13}+30x^{12}+378x^{11}+255x^{10}+357x^9+503x^8$ $+157x^7+229x^6+328x^5+516x^4+297x^3+336x^2+557x+448)$
601	302	7	$(x^2+316x+351)(x^3+188x^2+389x+122)(x^{19}+154x^{18}+398x^{17}+562x^{16}$ $+566x^{15}+446x^{14}+403x^{13}+293x^{12}+290x^{11}+480x^{10}+329x^9+500x^8$ $+320x^7+546x^6+20x^5+464x^4+209x^3+81x^2+187x+129)$
613	308	2	$(x+549)(x^3+69x^2+579x+206)(x^3+259x^2+383x+174)(x^{18}+189x^{17}$ $+42x^{16}+354x^{15}+491x^{14}+374x^{13}+65x^{12}+331x^{11}+248x^{10}+432x^9$ $+165x^8+605x^7+127x^6+48x^5+468x^4+488x^3+351x^2+220x+510)$
617	310	3	$(x+579)(x^4+188x^3+161x^2+261x+261)(x^6+285x^5+212x^4+392x^3$ $+340x^2+247x+194)(x^{14}+147x^{13}+77x^{12}+253x^{11}+134x^{10}+352x^9$ $+389x^8+185x^7+153x^6+42x^5+521x^4+225x^3+409x^2+379x+537)$

641	322	3	$(x+29)(x+184)(x+277)(x+387)(x+492)(x^8+533x^7+508x^6+473x^5+7x^4+542x^3+569x^2+128x+341)(x^{13}+390x^{12}+380x^{11}+116x^{10}+602x^9+60x^8+223x^7+330x^6+154x^5+29x^4+269x^3+389x^2+242x+570)$
653	328	2	$(x+278)(x+435)(x^2+36x+651)(x^2+559x+366)(x^2+617x+651)\times(x^4+180x^3+273x^2+649x+207)(x^{15}+594x^{14}+574x^{13}+617x^{12}+142x^{11}+532x^{10}+132x^9+576x^8+576x^7+279x^6+70x^5+171x^4+435x^3+644x^2+374x+546)$
661	332	2	$(x+214)(x+475)(x^2+328x+47)(x^5+416x^4+461x^3+254x^2+479x+522)(x^8+428x^7+581x^6+596x^5+259x^4+117x^3+426x^2+192x+447)\times(x^{10}+320x^9+23x^8+595x^7+240x^6+432x^5+287x^4+222x^3+604x^2+396x+99)$
673	338	5	$(x+160)(x+181)(x^3+347x^2+311x+209)(x^{22}+182x^{21}+63x^{20}+526x^{19}+191x^{18}+547x^{17}+389x^{16}+55x^{15}+652x^{14}+134x^{13}+566x^{12}+179x^{11}+142x^{10}+413x^9+475x^8+8x^7+460x^6+276x^5+575x^4+281x^3+484x^2+18x+175)$
677	340	3	$(x+459)(x^{27}+493x^{26}+464x^{25}+269x^{24}+263x^{23}+97x^{22}+342x^{21}+338x^{20}+586x^{19}+103x^{18}+352x^{17}+550x^{16}+497x^{15}+41x^{14}+591x^{13}+306x^{12}+417x^{11}+202x^{10}+324x^9+243x^8+38x^7+541x^6+267x^5+663x^4+252x^3+289x^2+320x+98)$
701	352	2	$(x^2+543x+14)(x^4+12x^3+616x^2+557x+18)(x^4+169x^3+575x^2+104x+443)(x^6+135x^5+543x^4+679x^3+583x^2+369x+281)\times(x^6+529x^5+572x^4+25x^3+422x^2+284x+125)(x^7+140x^6+431x^5+672x^4+667x^3+533x^2+525x+443)$
709	356	2	$(x^5+434x^4+330x^3+258x^2+565x+351)(x^8+615x^7+128x^6+588x^5+625x^4+503x^3+373x^2+519x+60)(x^{16}+603x^{15}+287x^{14}+380x^{13}+45x^{12}+185x^{11}+321x^{10}+662x^9+373x^8+144x^7+212x^6+518x^5+464x^4+247x^3+309x^2+58x+493)$
733	368	2	$(x^2+59x+731)(x^{28}+465x^{27}+683x^{26}+598x^{25}+227x^{24}+704x^{23}+182x^{22}+157x^{21}+71x^{20}+498x^{19}+661x^{17}+53x^{16}+245x^{15}+610x^{14}+730x^{13}+450x^{12}+467x^{11}+139x^{10}+295x^9+498x^8+57x^7+515x^6+555x^5+310x^4+43x^3+644x^2+204x+83)$
757	380	2	$(x+190)(x+539)(x^{12}+575x^{11}+439x^{10}+703x^9+77x^8+30x^7+103x^6+578x^5+722x^4+68x^3+486x^2+218x+116)(x^{17}+267x^{16}+137x^{15}+267x^{14}+31x^{13}+645x^{12}+477x^{11}+599x^{10}+569x^9+351x^8+228x^7+363x^6+291x^5+575x^4+380x^3+727x^2+212x+200)$

References

[1] P. Deligne and J-P. Serre, Formes modulaires de poids 1, Ann. Sci. École Norm. Sup., **7** (1974), 507–530.

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

[3] K. Haberland, Perioden von Modulformen einer Variabler und Gruppencohomologie, III, Math. Nachr., **112** (1983), 297–315.

[4] M. Koike, Congruences between cusp forms and linear representations of the Galois group, Nagoya Math. J., **64** (1976), 63–85.

[5] ——, A note on modular forms mod p, Nagoya Math. J., **89** (1983), 89–107.

[6] ——, Eigenvalues of Hecke operators mod p, II, preprint.

[7] R. P. Langlands, Base Change for $GL(2)$, Ann. of Math. Studies 96, Princeton U. Press, 1980.

[8] M. Ohta, The representation of Galois group attached to certain finite group schemes and its application to Shimura's theory, Algebraic Number Theory, edited by S. Iyanaga, Kyoto Intern. Symp., 1976, Japan Soc. for the Promotion of Sci. 1977.

[9] J-P. Serre, Modular forms of weight one and Galois representation, Algebraic Number fields edited by A. Fröhlich, 193–268, London, Academic Press 1977.

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

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

[12] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, Modular functions of one variable III. Proc. Intern. Summer School, Univ. Antwerp. Lect. Notes in Math., **350**, Springer, (1972), 1–55.

[13] H. Wada, Tables of Hecke operators (1), Seminar on Modern Methods in Number Theory, 1971.

Department of Mathematics
Faculty of Science
Nagoya University
Chikusa-ku, Nagoya 464
Japan