# AN EFFECTIVE ISOMORPHY CRITERION FOR MOD $\ell$ GALOIS REPRESENTATIONS.

YUUKI TAKAI

Abstract. In this paper, we consider mod $\ell$ Galois representations of $\mathbb{Q}$. In particular, we obtain an effective criterion to distinguish two semisimple 2-dimensional, odd mod $\ell$ Galois representations up to isomorphism. Serre's conjecture (Khare-Wintenberger's theorem), Sturm's theorem, and its modification by Kohnen are used in our proof.

## 1. Introduction.

In this paper, we consider mod $\ell$ Galois representations of $\mathbb{Q}$. In particular, we find an effective criterion to distinguish two mod $\ell$ Galois representations. More precisely, we consider the following problem:

**Problem.** *Let $\ell$ be a prime number, $d$ and $N$ be two positive integers such that $\ell \nmid N$, and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$, where $\overline{\mathbb{Q}}$ is an algebraic closure. Let $\rho, \rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_d(\overline{\mathbb{F}}_\ell)$ be two $d$-dimensional (semisimple) mod $\ell$ Galois representations with Artin conductor (outside $\ell$) dividing $N$ (defined in section 2.2). Is there an effectively computable constant $\kappa = \kappa(\ell, N)$ satisfying the following condition $(*)$?*

$(*)$ *If*

$$\det(1 - \rho(\mathrm{Frob}_p)T) = \det(1 - \rho'(\mathrm{Frob}_p)T) \text{ in } \overline{\mathbb{F}}_\ell[T]$$

*for every prime number $p$ such that $p \leq \kappa$ and $p \nmid \ell N$, $\rho$ is isomorphic to $\rho'$.*

*Here $\mathrm{Frob}_p$ is a Frobenius element at $p$.*

On the 1-dimensional case, we can trivially take $\kappa = \ell N$. Using Burgess' result on the estimate of character sums [Bur63], we obtain the better estimate for $\kappa$ as follows:

$$\kappa \ll_{r,\varepsilon} (\ell N)^{\frac{r+1}{4r}+\varepsilon}$$

for every positive integer $r$ and every positive number $\varepsilon$. Ankeny [Ank52] proved, under the assumption of GRH, a sharper estimate of character sums. By Ankeny's result, under the assumption of GRH, we obtain

$$\kappa \ll (\log(\ell N))^2.$$

*Date*: October 15, 2010.

For the details, see section 3.1.

In this paper, we consider the 2-dimensional case. The main result is the following theorem:

**Theorem 1.** *Let $\ell$ be a prime number and $N$ be a positive integer such that $\ell \nmid N$. Let $\rho, \rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_\ell)$ be two semisimple 2-dimensional Galois representations with Artin conductor dividing $N$. Assume that $\rho$ is odd (i.e., $\det(\rho)(c) = -1$ for a complex conjugation $c$). Let*

$$\kappa = \kappa(N, \ell) = \begin{cases} \dfrac{\ell(\ell^2-1)^2}{12} NN' \displaystyle\prod_{p|N} \left(1 + \frac{1}{p}\right) & \text{if } \ell > 2, \\ 4NN' \prod_{p|N} \left(1 + \dfrac{1}{p}\right) & \text{if } \ell = 2, \end{cases}$$

*where $N' = \prod_{p|N,\ p^2 \nmid N} p$. If*

$$\det(1 - \rho(\mathrm{Frob}_p)T) = \det(1 - \rho'(\mathrm{Frob}_p)T) \quad \text{in } \overline{\mathbb{F}}_\ell[T]$$

*i.e.,*

$$\begin{aligned} \mathrm{Tr}(\rho(\mathrm{Frob}_p)) &= \mathrm{Tr}(\rho'(\mathrm{Frob}_p)) \quad \text{in } \overline{\mathbb{F}}_\ell, \\ \det(\rho(\mathrm{Frob}_p)) &= \det(\rho'(\mathrm{Frob}_p)) \quad \text{in } \overline{\mathbb{F}}_\ell \end{aligned}$$

*for every prime number $p$ satisfying $p \leq \kappa$ and $p \nmid \ell N$, then $\rho$ is isomorphic to $\rho'$.*

In our proof, we use the theory of modular forms. Recently, Khare and Wintenberger proved Serre's conjecture for modularity of Galois representations [KW]. Serre's conjecture is the assertion that every odd irreducible 2-dimensional mod $\ell$ Galois representation arises from a newform. While every odd reducible 2-dimensional mod $\ell$ Galois representation arises from an Eisenstein series. By these facts, we can apply the theory of modular forms to analyse such Galois representations. We also use Sturm's and Kohnen's theorems for mod $\ell$ modular forms ([Stu87], [Koh04]). Roughly speaking, these theorems are assertions that the all Fourier coefficients modulo $\ell$ of modular forms are determined by the first few Fourier coefficients modulo $\ell$. We obtain the main theorem by applying Sturm's and Kohnen's result to modular forms associated with Galois representations.

**Acknowledgements.** *The author would like to thank Kazuhiro Fujiwara for for his elaborated guidance and invaluable discussion. Akihiko Gyoja read earlier versions of this paper and his comments were extremely helpful. I would also like to thank Kevin Buzzard for helpful remarks.*

## 2. Preliminaries.

**Notation and conventions.** In this paper, we follow the notations and definitions in [DS05]. For the details of modular forms, we also refer to [Shi71] or [Miy89].

Let $k$ and $N$ be positive integers. Congruence subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$ is defined as follows:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}.$$

We remark that $\Gamma_0(1) = SL_2(\mathbb{Z})$. Let $\mathcal{H}$ be the complex upper half plane and $GL_2^+(\mathbb{R})$ be the subgroup of $GL_2(\mathbb{R})$ consisting of the elements with positive determinant. For a holomorphic function $f$ on $\mathcal{H}$, the action of $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2^+(\mathbb{R})$ on $f$ is defined as follows:

$$(f|[\gamma])(z) = \det(\gamma)^{\frac{k}{2}}(cz+d)^{-k} f(\gamma z).$$

Let $\chi$ be a mod $N$ Dirichlet character. The complex vector space of the holomorphic modular forms of weight $k$ and level $\Gamma_0(N)$ with Nebentypus $\chi$ is denoted by $M_k(\Gamma_0(N), \chi)$ , *i.e.*,

$$M_k(\Gamma_0(N), \chi) = \{f : \mathcal{H} \to \mathbb{C} \mid \text{holomorphic on } \mathcal{H} \text{ and the cusps, } f|[\gamma] = \chi(d)f\}$$

Then $f \in M_k(\Gamma_0, \chi)$ has its Fourier expansion $f = \sum_{n \geq 0} a_n q^n$ where $q = e^{2\pi i z}$ $(z \in \mathcal{H})$.

### 2.1. **Modular forms.**

2.1.1. *Operator $\pi$.* Here we construct an operator on the space of modular forms. For the details, we refer to [Miy89, Lemma 4.6.5].

Let $k$ and $N$ be positive integers, $\chi$ be a Dirichlet character mod $N$, and $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma_0(N), \chi)$. For a positive integer $d$, we define the operator $V(d) : M_k(\Gamma_0(N), \chi) \to M_k(\Gamma_0(dN), \chi)$ as follows:

$$(f|V(d))(z) = \left( f \left| \begin{bmatrix} d & 0 \\ 0 & 1 \end{bmatrix} \right. \right)(z) = \sum_{n=0}^{\infty} a_n q^{dn}.$$

For a prime number $p$ satisfying $p|N$, we define operator $U(p) : M_k(\Gamma_0(N), \chi)$ $\to M_k(\Gamma_0(pN), \chi)$ as follows (cf. [Miy89, Lemma 4.6.5]):

$$(f|U(p))(z) = \frac{1}{p} \sum_{m=0}^{p-1} \left( f \left| \begin{bmatrix} 1 & m \\ 0 & p \end{bmatrix} \right. \right)(z) = \sum_{n=0}^{\infty} a_{pn} q^n.$$

It is easy to show that if $N = p^r N_0$ such that $r \geq 2$ and $(p, N_0) = 1$, and $\chi$ is of mod $p^{r-1}N_0$, then $U_p : M_k(\Gamma_0(p^r N_0), \chi) \to M_k(\Gamma_0(p^{r-1}N_0), \chi)$.

For a prime number $p$ dividing $N$, we set operator $\pi_p = V(p) \circ U(p) : M_k(\Gamma_0(N), \chi) \to M_k(\Gamma_0(M), \chi)$, where

$$M = \begin{cases} pN & \text{if } p^2 \nmid N, \\ N & \text{otherwise.} \end{cases}$$

Then, we have

$$\pi_p(f)(z) = \sum_{n=0}^{\infty} a_{pn} q^{pn}.$$

The operator $\pi : M_k(\Gamma_0(N), \chi) \to M_k(\Gamma_0(NN'), \chi)$ is defined as follows:

$$\pi = \mathrm{id} - \sum_{p|N:\text{prime}} \pi_p + \sum_{p_1,p_2|N:\text{prime}} \pi_{p_1} \circ \pi_{p_2} - \cdots = \prod_{p|N:\text{prime}} (\mathrm{id} - \pi_p),$$

where

$$N' = \prod_{p|N,\ p^2 \nmid N} p$$

and id is the identity of $M_k(\Gamma_0(NN'), \chi)$, and the product in the last equation is taken as operators. Then, we have

$$\pi(f)(z) = \sum_{n \geq 1:(n,N)=1} a_n q^n.$$

2.1.2. *Sturm's and Kohnen's result.* We recall Sturm's and Kohnen's result (in a form we need). These are results on the number of the first Fourier coefficients that determine the all Fourier coefficients (mod $\ell$) of modular forms.

Let $K$ be a number field, and $\mathcal{O}_K$ be the ring of integers of $K$.

**Lemma 1** (Sturm [Stu87, Th. 1])**.** *Let $k$ and $N$ be positive integers, and $\chi$ be a mod $N$ Dirichlet character. For $f, g \in M_k(\Gamma_0(N), \chi)$,*

$$\begin{aligned} f(z) &= \sum_{n=0}^{\infty} a_n q^n, \\ g(z) &= \sum_{n=0}^{\infty} b_n q^n \end{aligned}$$

*denote their Fourier expansions. Let $\ell$ be a prime number, and $\lambda$ be a prime ideal of $\mathcal{O}_K$ such that $\lambda | \ell\mathcal{O}_K$. We assume that $a_n, b_n$, and the values of $\chi$ are in $\mathcal{O}_K$ for all $n$. If $a_n \equiv b_n \pmod{\lambda}$ for every $n$ such that*

$$n \leq \frac{k}{12}[\Gamma_0(1) : \Gamma_0(N)],$$

*then $a_n \equiv b_n \pmod{\lambda}$ for all $n$.*

**Lemma 2** (Kohnen [Koh04, Th. 1])**.** *Let $k_1$ and $k_2$ be two positive integers such that $k_1, k_2 \geq 2$ and $k_1 \neq k_2$, $N$ be a positive integer, and $\chi$ be a mod $N$ Dirichlet character. For $f \in M_{k_1}(\Gamma_0(N), \chi)$ and $g \in M_{k_2}(\Gamma_0(N), \chi)$,*

$$\begin{aligned} f(z) &= \sum_{n=0}^{\infty} a_n q^n, \\ g(z) &= \sum_{n=0}^{\infty} b_n q^n \end{aligned}$$

*denote their Fourier expansions. Let $\ell$ be a prime number, and $\lambda$ be a prime ideal of $\mathcal{O}_K$ such that $\lambda | \ell \mathcal{O}_K$. We assume that $a_n, b_n$, and the values of $\chi$ are in $\mathcal{O}_K$ for all $n$. If $a_n \equiv b_n \pmod{\lambda}$ for every $n$ such that*

$$n \leq \frac{\max\{k_1, k_2\}}{12} \begin{cases} [\Gamma_0(1) : \Gamma_0(N) \cap \Gamma_1(\ell)] & \text{if } \ell > 2, \\ [\Gamma_0(1) : \Gamma_0(N) \cap \Gamma_1(4)] & \text{if } \ell = 2, \end{cases}$$

*then $a_n \equiv b_n \pmod{\lambda}$ for all $n$.*

*Remark* 1. We remark that Lemma 2 holds even for $k_1 = k_2$. Indeed, because $[\Gamma_0(1) : \Gamma_0(N)] \leq [\Gamma_0(1) : \Gamma_0(N) \cap \Gamma_1(\ell)]$, applying Sturm's theorem if $k_1 = k_2$, we can show that the first

$$\frac{\max\{k_1, k_2\}}{12} [\Gamma_0(1) : \Gamma_0(N) \cap \Gamma_1(\ell)]$$

coefficients determine the all Fourier coefficients (mod $\lambda$) of modular forms for every $k_1, k_2 \geq 2$ and $\ell > 2$. Similarly, also in the case of $\ell = 2$, the first

$$\frac{\max\{k_1, k_2\}}{12} [\Gamma_0(1) : \Gamma_0(N) \cap \Gamma_1(4)]$$

coefficients determine the all Fourier coefficients (mod 2) of modular forms for every $k_1, k_2 \geq 2$.

## 2.2. **Galois representations.**

2.2.1. *$\ell$-adic and mod $\ell$ Galois representations.* Let $\ell$ be a prime number, $d$ be a positive integer, and $L$ be a finite extension of $\mathbb{Q}_\ell$. Then a $d$-dimensional $\ell$-adic Galois representation over $L$ is a continuous homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_d(L).$$

For two $d$-dimensional $\ell$-adic representations $\rho$ and $\rho'$, $\rho$ is isomorphic (or equivalent) to $\rho'$ (denoted by $\rho \simeq \rho'$) if there is an element $A \in GL_d(L)$ such that $\rho(\sigma) = A^{-1}\rho'(\sigma)A$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. $\rho$ is absolutely irreducible if for every finite extension $L'$ of $L$, the composition representation $f \circ \rho$ is also irreducible, where $f : GL_d(L) \hookrightarrow GL_d(L')$. $\rho$ is odd if $\det(\rho(c)) = -1$ for a complex conjugation $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $\mathbb{F}$ be a finite field or an algebraic closed field of characteristic $\ell$. A $d$-dimensional mod $\ell$ Galois representation over $\mathbb{F}$ is a continuous homomorphism $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_d(\mathbb{F})$, where $GL_d(\mathbb{F})$ has a discrete topology. The notions of isomorphic, absolutely irreducible, and odd are defined as above.

Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is compact, $\rho$ has a finite image. Therefore, when $\mathbb{F} = \overline{\mathbb{F}}_\ell$, there is a finite subfield $\mathbb{F}'$ of $\mathbb{F}$ such that $\rho$ is defined over $\mathbb{F}'$. Let $\mathbb{F}$ be a field of characteristic $\ell$, and $V = \mathbb{F}^d$. For a $d$-dimensional mod $\ell$ representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$, Artin conductor (outside $\ell$) $N(\rho)$ of $\rho$ is defined as follows:

$$N(\rho) = \sum_{p \neq \ell : \text{prime}} p^{n_p(\rho)}, \ n_p(\rho) = \sum_{i \geq 0} \frac{1}{(G_{p,0} : G_{p,i})} \dim(V/V^{G_{p,i}}),$$

where $G_{p,i}$ is the $i$-th ramification group of the decomposition group at $p$. It is known that $n_p(\rho)$ is a non-negative integer. Thus $N(\rho)$ is also a positive integer. We remark that the Artin conductor is relatively prime to $\ell$.

There is the fundamental fact on isomorphy of Galois representations.

**Lemma 3.** *Let $R$ be a finite extension field of $\mathbb{Q}_\ell$ or a finite extension field of $\mathbb{F}_\ell$. Let $\rho, \rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_d(R)$ be two semisimple continuous Galois representations. Then if $\det(1 - \rho(\mathrm{Frob}_p)T) = \det(1 - \rho'(\mathrm{Frob}_p)T) \in R[T]$ for all but finitely many prime number $p$, $\rho$ is isomorphic to $\rho'$.*

*Proof.* The lemma follows from Chebotarev's density theorem and Brauer and Nesbitt's theorem (cf. [DS74, Lem. 3.2]). □

Next, we discuss mod $\ell$ reductions of $\ell$-adic representations. Let $L$ be a finite extension of $\mathbb{Q}_\ell$, $\mathcal{O}_L$ be the ring of integers in $L$, and $\lambda$ be a maximal ideal in $\mathcal{O}_L$ such that $\lambda | \ell\mathcal{O}_L$. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(V)$ be a $d$-dimensional $\ell$-adic Galois representation, where $V$ is a $d$-dimensional vector space over $L$. Then the following fact is known:

**Proposition 1.** *$\rho$ admits a Galois stable lattice i.e., there is a lattice $\mathcal{L} \subset V$ such that $\mathcal{L}$ is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

*Proof.* For the proof, cf. [DS05, Prop. 9.3.5]. □

By choosing some basis which generates a Galois stable lattice in $V$ for $\rho$, we can take $GL_d(\mathcal{O}_L)$ as the image of $\rho$. A reduction $\overline{\rho}$ of $\rho$ is defined as the composition $f \circ \rho$, where $f$ is a surjective continuous homomorphism $GL_d(\mathcal{O}_L) \to GL_d(\mathcal{O}_L/\lambda)$. We remark that the semisimplification of $\overline{\rho}$ does not depend on any choice of Galois stable lattices.

2.2.2. *Modularity of 2-dimensional mod $\ell$ Galois representations.* In this section, we discuss the theory of between modular forms and $\ell$-adic and mod $\ell$ Galois representations. In the beginning, we recall $\ell$-adic Galois representations associated to newforms. Let $f \in S_k(\Gamma_0(N), \epsilon)$ be a normalised newform with Nebentypus $\epsilon$ (for the definition, cf. [DS05, Def. 5.8.1]) and $f = \sum a_n q^n (q = e^{2\pi i z})$ denotes the Fourier expansion of $f$. Let $K = \mathbb{Q}(\ldots, a_n, \ldots, \epsilon)$ be the field generated by the all Fourier coefficients of $f$ and the values of $\epsilon$. Then it is known that $K$ is a finite extension of $\mathbb{Q}$ and coefficients $a_n$ are in $\mathcal{O}_K$ (cf. [Shi71, Theorem 3.48]). Let $\ell$ be a prime number such that $\ell \nmid N$ and $\lambda$ be a prime ideal of $\mathcal{O}_K$ such that

$\lambda|\ell\mathcal{O}_K$. The $\ell$-adic Galois representation associated to $f$ is a 2-dimensional representation $\rho = \rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_{K_\lambda})$ such that

$$\begin{aligned} \mathrm{Tr}(\rho(\mathrm{Frob}_p)) &= a_p, \\ \det(\rho(\mathrm{Frob}_p)) &= \epsilon(p)p^{k-1} \end{aligned}$$

for all prime number $p$ satisfying $(p, \ell N) = 1$, where $K_\lambda$ is the completion of $K$ at $\lambda$. A mod $\ell$ Galois representation associated to $f$ is denoted by $\overline{\rho_f}$. We also define $\ell$-adic and mod $\ell$ Galois representations associated to Eisenstein series which are normalised eigenforms as well as newforms (cf. [DS05, Th. 9.6.6]).

Next, We recall some facts of modularity of 2-dimensional mod $\ell$ Galois representations. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_\ell)$ be a mod $\ell$ Galois representation. We assume that $\rho$ is semisimple, odd, and $N(\rho)|N$.

When $\rho$ is reducible, $\rho$ comes from an Eisenstein series. More precisely, we explain modularity in the reducible case. At first, we review some facts on Eisenstein series (for the details, cf. [DS05, Sect. 4.5]). Let $N$, $u$ and $v$ be positive integers such that $uv|N$, $\psi$ (resp. $\phi$) be a (resp. primitive) mod $u$ (resp. $v$) Dirichlet character, and $k$ be an integer $k \geq 2$ such that $(\psi\phi)(-1) = (-1)^k$. $E_k^{\psi,\phi}$ denotes the Eisenstein series defined in [DS05, Sect. 4.5, Sect. 4.6]. We remark that $E_k^{\psi,\phi}$ is holomorphic if $k \geq 3$, but is not holomorphic if $\psi$ and $\phi$ are principal and $k = 2$. $E_k^{\psi,\phi}$ has the following Fourier expansion:

$$E_k^{\psi,\phi}(z) = \delta(\psi)L(1-k,\phi) + 2\sum_{n=1}^{\infty}\sigma_{k-1}^{\psi,\phi}(n)q^n,$$

where

$$\delta(\psi) = \begin{cases} 1 & \text{if } \psi \text{ is a primitive character,} \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\sigma_{k-1}^{\psi,\phi}(n) = \sum_{d|n,d>0} \psi\left(\frac{n}{d}\right)\phi(d)d^{k-1}.$$

For a positive integer $t$ such that $tuv|N$, we set

$$E_k^{\psi,\phi,t}(z) = \begin{cases} E_k^{\psi,\phi}(z) - tE_k^{\psi,\phi}(tz) & \text{if } \psi \text{ and } \phi \text{ are primitive and } k = 2, \\ E_k^{\psi,\phi}(tz) & \text{otherwise.} \end{cases}$$

Then, $E_k^{\psi,\phi,t}(z)$ is a holomorphic modular form. If $uv = N$ or $k = 2$, $\psi = 1$, $\phi = 1$, $t$ is a prime and $N$ is a power of $t$, then $E_k^{\psi,\phi,t}$ is an eigenform for all Hecke operators. Let $\rho$ be as above. We assume that $\rho$ is reducible. Then, we can show that

$$\rho \simeq \begin{pmatrix} \psi\chi_\ell^a & 0 \\ 0 & \phi\chi_\ell^b \end{pmatrix},$$

where $\psi$ and $\phi$ are Dirichlet characters such that $\psi\phi$ is a mod $N$ Dirichlet character, $\chi_\ell$ is the cyclotomic character, and $a$ and $b$ are integers such that $0 \leq a, b \leq \ell - 2$ (cf. §.3.1). When $a = 0$, $\rho$ comes from $\frac{1}{2}E_k^{\psi,\phi,t}$ for $2 \leq k \leq \ell + 1$ and $k \equiv b \mod \ell - 1$ (cf. [DS05, Th. 9.6.7]). When $a = 1, \ldots, \ell - 2$, for a positive integer $k$ such that $k \equiv b - a + 1 \mod \ell - 1$ and $2 \leq k \leq l + 1$, $\rho$ comes from eigenform $\frac{1}{2}\theta^a E_k^{\psi,\phi,t}$. Here $\theta$ is the theta operator (cf. [Edi92, Sect. 3]). We remark that the filtration $w(\frac{1}{2}\theta^a E_k^{\psi,\phi,t})$ of $\frac{1}{2}\theta^a E_k^{\psi,\phi,t}$ is $2 \leq w(\frac{1}{2}\theta^a E_k^{\psi,\phi,t}) \leq \ell^2 - 1$ if $a = 1, 2, \ldots, \ell - 2$.

When $\rho$ is irreducible, Khare and Wintenberger proved the following theorem known as Serre's modularity conjecture:

**Theorem** (Khare and Wintenberger [KW]). *Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_\ell)$ be an irreducible odd 2-dimensional mod $\ell$ Galois representation. Then there is a newform $f \in S_{k(\rho)}(\Gamma_0(N(\rho)), \epsilon(\rho))$ such that $\rho$ is isomorphic to $\overline{\rho_f}$. Here the integers $N(\rho), k(\rho)$, and the mod $N(\rho)$ Dirichlet character $\epsilon(\rho)$ are defined by Serre* [Ser87, Sect. 1 and Sect. 2].

*Remark* 2. By the definitions in [Ser87, Sect. 2], $2 \leq k(\rho) \leq \ell^2 - 1$ if $\ell > 2$ and $k(\rho) = 2$ or 4 if $\ell = 2$. We remark that both the reducible case and the irreducible case, we can take a modular form corresponding to $\rho$ of weight $k$ such that $2 \leq k \leq \ell^2 - 1$ if $\ell > 2$ and $k = 2$ or 4 if $\ell = 2$.

## 3. One and two-dimensional cases.

3.1. **One-dimensional case.** Let $\ell$ be a prime number, and $N$ be a positive integer such that $\ell \nmid N$. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_1(\overline{\mathbb{F}}_\ell)$ be a 1-dimensional mod $\ell$ Galois representation of the Artin conductor $N$. Since $\rho$ has a finite image, there is a finite abelian extension $F$ over $\mathbb{Q}$ such that $\mathrm{image}(\rho) \simeq \mathrm{Gal}(F/\mathbb{Q})$. Thus, by Kronecker-Weber theorem, there is a positive integer $M$ and we have the factorisation $\rho = \rho_\chi = \rho_{\chi,M} \circ \pi_M$, where $\rho_{\chi,M} : \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q}) \simeq (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\chi} \overline{\mathbb{F}}_\ell^\times$ and $\pi_M : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$. Since $\rho$ is tamely ramified at $\ell$, we may take $M = \ell N$ where $N$ is the Artin conductor of $\rho$. In particular, $\rho$ comes from a mod $\ell N$ character.

Let $\rho$ and $\rho'$ be two 1-dimensional mod $\ell$ Galois representations of Artin conductors $N$, and $\chi$ and $\chi'$ be two mod $\ell N$ Dirichlet characters such that $\rho = \rho_\chi$ and $\rho' = \rho_{\chi'}$. On the 1-dimensional case of the problem, we claim that there is a positive number $\kappa = \kappa(N, \ell)$ such that if $\rho(\mathrm{Frob}_p) = \rho'(\mathrm{Frob}_p)$ in $\overline{\mathbb{F}}_\ell^\times$ for every prime number $p$ satisfying $(p, \ell N) = 1$ and $p \leq \kappa$, then $\rho \simeq \rho'$.

First, we discuss a trivial estimate. If $\rho_\chi \not\simeq \rho_{\chi'}$, $(\chi/\chi')(n) \neq 1$ for an integer $n$ such that $1 < n < \ell N$. Then there is a prime $p|n$ such that $(\chi/\chi')(p) \neq 1$. Thus we can take $\kappa = \ell N$. It is a trivial estimate for $\kappa$.

Using Burgess' estimate for character sums [Bur63], we obtain a better estimate for $\kappa$. Let $d$ be a positive integer, $M$ be an integer such that $0 < M < d$, and $\chi_0$ be a non-trivial mod $d$ Dirichlet character. According

to Burgess [Bur63, Th. 2],

$$|\sum_{n=1}^{M}\chi_0(n)| \ll_{r,\varepsilon} M^{1-\frac{1}{r}}d^{\frac{r+1}{4r^2}+\varepsilon}$$

for every positive integer $r$ and every positive number $\varepsilon$. This inequality means that

$$|\sum_{n=1}^{M}\chi_0(n)| < cM^{1-\frac{1}{r}}d^{\frac{r+1}{4r^2}+\varepsilon}$$

for every positive integer $r$ and every positive number $\varepsilon$ with a positive constant $c$ depending on $r$ and $\varepsilon$. When $M > c^r d^{\frac{r+1}{4r}+r\varepsilon}$, $cM^{1-\frac{1}{r}}d^{\frac{r+1}{4r^2}+\varepsilon} < M$. Thus $\chi_0(n) \neq 1$ for $0 < n < c^r d^{\frac{r+1}{4r}+r\varepsilon}+1$. In our case, applying Burgess' result with $d = \ell N$ and $\chi_0 = \chi/\chi'$, we can take $\kappa = c^r(\ell N)^{\frac{r+1}{4r}+r\varepsilon}+1$ with the above $c, r, \varepsilon$. Thus we obtain the estimate

$$\kappa \ll_{r,\varepsilon} (\ell N)^{\frac{r+1}{4r}+r\varepsilon}.$$

On the estimate of character sums, it is conjectured that the bound is some polynomial order of the logarithm. Indeed, Ankeny [Ank52, Th. 2] proved, under GRH, the following estimate:

$$|\sum_{n=1}^{M}\chi_0(n)| \ll (\log(\ell N))^2.$$

Using this, we obtain

$$\kappa \ll (\log(\ell N))^2$$

under GRH.

3.2. **Two-dimensional case.** In the 2-dimensional case, we prove the following main result:

**Theorem 1.** *Let $\ell$ be a prime number and $N$ be a positive integer such that $\ell \nmid N$. Let $\rho, \rho' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_\ell)$ be two semisimple 2-dimensional mod $\ell$ Galois representations with Artin conductor dividing $N$. Assume that $\rho$ is odd. Let*

$$\kappa = \kappa(N,\ell) = \begin{cases} \dfrac{\ell(\ell^2-1)^2}{12} NN' \displaystyle\prod_{p|N}\left(1+\frac{1}{p}\right) & \text{if } \ell > 2, \\ 4NN' \prod_{p|N}\left(1+\dfrac{1}{p}\right) & \text{if } \ell = 2. \end{cases}$$

*where $N' = \prod_{p|N,\ p^2\nmid N} p$. If*

$$\det(1-\rho(\mathrm{Frob}_p)T) = \det(1-\rho'(\mathrm{Frob}_p)T) \quad \text{in } \overline{\mathbb{F}}_\ell[T]$$

*for every prime number $p$ satisfying $p \leq \kappa$ and $p \nmid \ell N$, $\rho$ is isomorphic to $\rho'$.*

*Proof.* First, we prove that $\rho'$ is odd. By the assumption,

$$\det(\rho(\mathrm{Frob}_p)) = \det(\rho'(\mathrm{Frob}_p))$$

for every prime $p$ satisfying $p < \ell N < \kappa$ and $p \nmid \ell N$. Thus, by the trivial estimate on the 1-dimensional case,

$$\det(\rho) = \det(\rho')$$

holds for every prime number $p$ satisfying $p \nmid \ell N$. Thus, $\rho'$ is also odd. By Remark 2, semisimple odd continuous 2-dimensional mod $\ell$ Galois representations come from Hecke eigenforms. Because $N(\rho), N(\rho')|N$ and $N|\ell N$, we can take the appropriate eigenform $f \in M_{k_1}(\Gamma_0(\ell N), \epsilon)$ (resp. $g \in M_{k_2}(\Gamma_0(\ell N), \epsilon)$) such that $\rho \simeq \overline{\rho_f}^{ss}$ (resp. $\rho' \simeq \overline{\rho_g}^{ss}$), $2 \leq k_1, k_2 \leq \ell^2 - 1$ if $\ell > 2$, and $k_1, k_2 = 2, 4$ if $\ell = 2$. Here $\overline{\rho_f}^{ss}$ is the semisimplification of $\overline{\rho_f}$.

Next, we apply the operator $\pi$ defined in §. 2.1.1. We set $\tilde{f} = \pi(f)(z) \in M_{k_1}(\Gamma_0(\ell^2 NN'), \epsilon)$ and $\tilde{g} = \pi(g)(z) \in M_{k_2}(\Gamma_0(\ell 62NN'), \epsilon)$. Let $\tilde{f}(z) = \sum_{n=1}^{\infty} a_n q^n$ and $\tilde{g}(z) = \sum_{n=1}^{\infty} b_n q^n$ be their Fourier expansions. Remark that $a_n = b_n = 0$ for all $n$ such that $(n, \ell N) > 1$ and

$$\begin{cases} a_{mn} = a_m a_n \\ b_{mn} = b_m b_n \end{cases} \quad \text{for all } (m,n) = 1,$$

$$\begin{cases} a_{p^n} = a_{p^n - 1} a_p + \epsilon(p) p^{k_1 - 1} a_{p^{n-2}} \\ b_{p^n} = b_{p^n - 1} b_p + \epsilon(p) p^{k_2 - 1} b_{p^{n-2}} \end{cases}$$

for every prime number $p$ such that $p \nmid \ell N$. Let $K_f = \mathbb{Q}(\ldots, a_n, \ldots, \epsilon)$ (resp. $K_g = \mathbb{Q}(\ldots, b_n, \ldots, \epsilon)$) be the field generated by the all Fourier coefficients of $f$ (resp. $g$) and the values of $\epsilon$, and $\mathcal{O}_{K_f}$ (resp. $\mathcal{O}_{K_g}$) be the ring of integers of $K_f$ (resp. $K_g$). Let $\lambda_f$ (resp. $\lambda_g$) be a maximal ideal in $\mathcal{O}_{K_f}$ (resp. $\mathcal{O}_{K_g}$) such that $\lambda_f | \ell \mathcal{O}_{K_f}$ (resp. $\lambda_g | \ell \mathcal{O}_{K_g}$) and $\mathbb{F}_f = \mathcal{O}_{K_{f,\lambda_f}}/\lambda_f$ (resp. $\mathbb{F}_g = \mathcal{O}_{K_{f,\lambda_g}}/\lambda_g$). Then

$$\begin{aligned} \det(1 - \rho(\mathrm{Frob}_p)T) &= 1 - a_p T + \epsilon(p) p^{k_1 - 1} T^2 \quad \text{in } \mathbb{F}_f[T], \\ \det(1 - \rho'(\mathrm{Frob}_p)T) &= 1 - b_p T + \epsilon(p) p^{k_2 - 1} T^2 \quad \text{in } \mathbb{F}_g[T] \end{aligned}$$

for every prime $p$ such that $p \nmid \ell N$. Let $L$ be the Galois closure of the composite of $K_f$ and $K_g$, $\mathcal{O}_L$ be the ring of the integers of $L$, and $\lambda$ be a maximal ideal in $\mathcal{O}_L$ such that $\lambda | \lambda_f \mathcal{O}_L$ and $\lambda | \lambda_g \mathcal{O}_L$, and $\mathbb{F} = \mathcal{O}_{L,\lambda}/\lambda$. Then

$$\begin{aligned} \det(1 - \rho(\mathrm{Frob}_p)T) &= 1 - a_p T + \epsilon(p) p^{k_1 - 1} T^2 \quad \text{in } \mathbb{F}[T], \\ \det(1 - \rho'(\mathrm{Frob}_p)T) &= 1 - b_p T + \epsilon(p) p^{k_2 - 1} T^2 \quad \text{in } \mathbb{F}[T] \end{aligned}$$

for all prime $p$ such that $p \nmid \ell N$.

On the assumption, we have

$$a_p \equiv b_p \pmod{\lambda}$$

for every prime $p$ such that $p \nmid \ell N$ and $p \leq \kappa$ (for $\kappa$ in Theorem 1). Because $a_{mn} = a_m a_n, b_{mn} = b_m b_n$ for $(m,n) = 1$ and $a_{p^n} \equiv b_{p^n} \pmod{\lambda}$ for every

prime number $p$ such that $p \leq \kappa$ (indeed, for such prime $p$,

$$\begin{aligned} a_{p^2} &= a_p^2 + \epsilon(p)p^{k_1-1}a_1 \\ &\equiv a_p^2 + \det(\rho(\mathrm{Frob}_p)) \pmod{\lambda} \\ &\equiv b_p^2 + \det(\rho'(\mathrm{Frob}_p)) \pmod{\lambda} \\ &\equiv b_p^2 + \epsilon(p)p^{k_2-1}b_1 \pmod{\lambda} \\ &= b_{p^2} \end{aligned}$$

and by the induction), we have

$$a_n \equiv b_n \pmod{\lambda}$$

for every $n$ such that $n \leq \kappa$. While it is easy to check that

$$\kappa = \begin{cases} \dfrac{\ell^2-1}{12}[\Gamma_0(1) : \Gamma_0(\ell^2 NN') \cap \Gamma_1(\ell)] & \text{if } \ell > 2, \\ \dfrac{4}{12}[\Gamma_0(1) : \Gamma_0(4NN') \cap \Gamma_1(4)] & \text{if } \ell = 2. \end{cases}$$

By Lemma 1 and Lemma 2 and the fact that $2 \leq k(\rho), k(\rho') \leq \ell^2 - 1$ if $\ell > 2$ and $k(\rho), k(\rho') = 2$ or 4 if $\ell = 2$, we have $\tilde{f} \equiv \tilde{g} \pmod{\lambda}$. It means that $a_n \equiv b_n \pmod{\lambda}$ for all $n$. Therefore $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv \mathrm{Tr}(\rho'(\mathrm{Frob}_p)) \pmod{\lambda}$ for every prime $p$ such that $p \nmid \ell N$. By Lemma 3, $\rho$ is isomorphic to $\rho'$. □

By Theorem 1, we have estimate

$$\kappa \ll \ell^5 N^2 \log N.$$

Comparing with the estimate under GRH on the 1-dimensional case in section 3.1, it is clear the above estimate is very large. We guess that the estimate for $\kappa$ can be improved in the 2-dimensional case. In general, we guess that we can take some polynomial of $\log \ell N$ as the upper bound for $\kappa$ in the arbitrary dimensional case. Thus we ask the following question:

**Question.** *Let $n$ be a positive integer, and $\kappa$ be the positive number in the problem of the $n$-dimensional case. Then can we take*

$$\kappa = (\log \ell N)^d$$

*for some positive integer $d$?*

## References


[Ank52] N.C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[Bur63] D.A. Burgess. On character sums and $L$-series. II. *Proc. London Math. Soc. (3)*, 13:524–536, 1963.

[DS74] P. Deligne and J.-P. Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup., (4)*, 7:507–530, 1974.

[DS05] F. Diamond and J. Shurman. *A first course in modular forms*. Number 228 in Graduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[Edi92] B. Edixhoven. The weight in Serre's conjectures on modular forms. *Inventiones mathematicae*, 109(1):563–594, 1992.

[Koh04] W. Kohnen. On Fourier coefficients of modular forms of different weights. *Acta Arith.*, 113(1):57–67, 2004.

[KW] C. Khare and J-P. Wintenberger. Serre's modularity conjecture I and II. available at http://www.math.utah.edu/ shekhar/papers.html.

[Miy89] T. Miyake. *Modular forms*. Springer-Verlag, Berlin, 1989.

[Ser87] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic forms*. Princeton University Press, Princeton, NJ, 1971.

[Stu87] J. Sturm. On the congruence of modular forms. In *Number theory*, volume 1240 of *Lecture Notes in Math.*, pages 275–280, New York, 1984-1985, 1987. Springer, Berlin.

Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Japan

*E-mail address*: yuuki-takai@math.nagoya-u.ac.jp