Refinement of Tate's Discriminant Bound and Non-Existence Theorems for Mod p Galois Representations

Dedicated to Professor Kazuya Kato
on the occasion of his fiftieth birthday

Hyunsuk Moon[1] and Yuichiro Taguchi

Received: November 30, 2002
Revised: February 4, 2003

Abstract. Non-existence is proved of certain continuous irreducible mod p representations of degree 2 of the absolute Galois group of the rational number field. This extends previously known results, the improvement based on a refinement of Tate's discriminant bound.

2000 Mathematics Subject Classification: 11F80, 11R29, 11R39
Keywords and Phrases: Mod p Galois Representation, Discriminant

Introduction. Let $G_{\mathbb{Q}}$ be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the rational number field $\mathbb{Q}$, and $\overline{\mathbb{F}}_p$ an algebraic closure of the prime field $\mathbb{F}_p$ of p elements. In this paper, we are motivated by Serre's conjecture [19] to prove that there exists no continuous irreducible representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ unramified outside p for $p \leq 31$ and with small Serre weight k. This extends the previous works by Tate [21], Serre [18], Brueggeman [1], Fontaine [5], Joshi [6] and Moon [11], [12]. Our main result is:

Theorem 1. *There exists no continuous irreducible representation* $\rho :\ G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ *which is unramified outside p and of reduced Serre weight k (cf. Sect. 1) in the following cases marked with* $\times$*, and the same is true if we assume the Generalized Riemann Hypothesis (GRH) in the following cases marked with* $\times_{\mathrm{R}}$:

[1]The first author was supported by the JSPS Postdoctoral Fellowship for Foreign Researchers.

$k\backslash p$	2	3	5	7	11	13	17	19	23	29	31
2	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$
3	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	f	f	f
4		$\times$	$\times$	$\times$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\mathrm{f_R}$	$\mathrm{f_R}$
5			$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	f	f	f
6			$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\mathrm{f_R}$	$\mathrm{f_R}$	?	?	?
7				$\times$	$\times$	$\times$	$\times$	$\times$	f	f	$\mathrm{f_R}$
8				?	?	?	?	?	?	?	?
9					$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\mathrm{f_R}$	$\mathrm{f_R}$	$\mathrm{f_R}$
10					?	?	?	?	?	?	?
11					$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\mathrm{f_R}$	$\mathrm{f_R}$	$\mathrm{f_R}$
12					$\exists$	$\exists$	$\exists$	$\exists$	?	$\exists$	$\exists$
13						$\mathrm{f_R}$	$\times_{\mathrm{R}}$	$\times_{\mathrm{R}}$	$\mathrm{f_R}$	$\mathrm{f_R}$	$\mathrm{f_R}$
14						?	?	?	?	?	?
15							$\mathrm{f_R}$	$\mathrm{f_R}$	$\mathrm{f_R}$	$\mathrm{f_R}$	$\mathrm{f_R}$
16							$\exists$	$\exists$	$\exists$	$\exists$	?
17							?	?	?	$\mathrm{f_R}$	$\mathrm{f_R}$
18							$\exists$	$\exists$	$\exists$	$\exists$	$\exists$
19								?	?	?	?
20								$\exists$	$\exists$	$\exists$	$\exists$

In this table, an f *(resp.* $\mathrm{f_R}$*) means that, unconditionally (resp. under the GRH), there exist only finitely many* ρ *in that case, and an* $\exists$ *means that there does exist an irreducible representation in that case. A ? means that the non-existence/finiteness is unknown (at present) in that case.*

Note that the reduced Serre weight takes values $1 \leq k \leq p+1$; the table can be continued further down to $k = 32$ in an obvious manner (with many ?'s and some $\exists$'s). The case $k = 1$ of the Theorem is trivial since $k = 1$ means that ρ is unramified at p. In the above table, the cases $p = 2, 3, 5$ are proved respectively in [21], [18], [1]. The case where $p = 7$ and ρ is even (i.e. k is odd) is proved in [12]. For $k = 2$ and $p \leq 17$, Fontaine [5] proved the non-existence of certain types of finite flat group schemes (not just of two-dimensional Galois representations). Joshi [6] proved the non-existence of ρ for $p \leq 13$ and of Hodge-Tate weight $1, 2$ (instead of Serre weight $2, 3$; presumably, one has $k-1$ = the Hodge-Tate weight in the sense of Joshi if the Serre weight k satisfies $1 \leq k \leq p-1$). The representations marked with $\exists$ are provided by cusp forms (mod p) of weight 12, 16, 18, 20 and level 1 (cf. [16], §3.3–3.5).

As a corollary, it follows from this theorem that, under the GRH and for $3 \leq p \leq 31$, (i) any finite flat group scheme over $\mathbb{Z}$ of type (p, p) is the direct sum of two group schemes which are isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or μ_p (cf. [19], Théorème 3); and (ii) any p-divisible group over $\mathbb{Z}$ of height 2 is the direct sum of two p-divisible groups which are either constant or multiplicative (cf. [5], Théorème 4 and its Corollaries).

Our strategy in the proof is basically the same as in the above cited works; to deduce contradiction by comparing two kinds of inequalities of the opposite direction for the discriminant of the field corresponding to the kernel of ρ — one from above (the Tate bound), and the other from below (the Odlyzko bound). The novelty in this paper is in the refinement of the Tate bound (Theorem 3), which gives the precise value of the discriminant in terms of the reduced Serre weight $\tilde{k}(\rho)$ of ρ. This is done in Section 1. In Section 2, we compare this with the Odlyzko bound ([14] and [15]) to prove the above Theorem. To deal with the case where ρ is odd and has solvable image, we use the fact that Serre's conjecture is true for such ρ if $p \geq 3$ ([7]).

Another interesting case to consider is where the representation ρ has Serre weight 1 (i.e. unramified at p) and non-trivial Artin conductor outside p. Although a mod p modular form in Katz' sense lifts to a classical one of the same weight in most cases if the weight is ≥ 2, this may not be the case for weight 1 forms (Lemma 1.9 of [4]). If this is the case and Serre's conjecture is true, then an odd and irreducible ρ of Serre weight 1 is put under a severe restraint on its image. Indeed, if ρ comes from a mod p eigenform f which lifts to a classical eigenform F of weight 1, then ρ has also to lift to an Artin representation $\rho_F : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$ associated to F ([2]). In particular, in such a case, an irreducible ρ cannot have image of order divisible by p (or equivalently, its projective image cannot contain a subgroup isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$) if $p \geq 5$. Conversely, if there are no such representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ and if the Artin conjecture is true, then any mod p eigenform of weight 1 lifts, at least "outside the level", to a classical eigenform of weight 1. In this vein, we prove:

THEOREM 2. *Assume the GRH. Then for each prime $p \geq 5$, there exists a positive integer N_p such that there exists no continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ with reduced Serre weight 1, $N(\rho) \leq N_p$ and projective image containing a subgroup isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$. The N_p can be computed explicitly; for large enough p (say, $p \geq 1000003$), we can take $N_p = 44$, and for some small p, we can take $N_5 = 20$, $N_7 = 24$, $N_{11} = 29$, ..., $N_{31} = 34$, ...*

This is just a simple application of the Odlyzko bound. One can give also an unconditional version of this theorem. Theorem 2, together with some extensions of Theorem 1 to the case of non-trivial Artin conductors, is proved in Section 3.

In this paper, we follow the definitions, notations and conventions in [4] for, e.g., the Serre weight $k(\rho)$, the notion of mod p modular forms, and the formulation of Serre's conjecture. There are slight differences (cf. [4], §1) between these and those of Serre's original ones in [19].

It is our pleasure to dedicate this paper to Professor Kazuya Kato on the occasion of his fiftieth birthday. The second named author got interested in Serre's conjecture when he read the paper [19] as a graduate student under the direction of Professor Kato, and a decade later his continued interest was conveyed to the first named author.

1. REFINEMENT OF THE TATE BOUND.

In this section, we refine Tate's discriminant bound [21] for the finite Galois extension $K/\mathbb{Q}_p$ corresponding to the kernel of a continuous representation $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of the absolute Galois group $G_{\mathbb{Q}_p}$ of the p-adic number field $\mathbb{Q}_p$. Namely, we give a formula which gives the valuation of the different $\mathcal{D}_{K/\mathbb{Q}_p}$ of $K/\mathbb{Q}_p$ in terms of the reduced Serre weight (defined below) of ρ.

Let $k(\rho)$ be the Serre weight of ρ, and χ the mod p cyclotomic character. Then by the definition of $k(\rho)$, there exists an integer α (mod $(p-1)$) such that $k(\chi^{-\alpha} \otimes \rho) \leq p+1$. It will be convenient for our purpose to define the *reduced Serre weight* $\tilde{k}(\rho)$ of ρ by

$$\tilde{k}(\rho) \ := \ k(\chi^{-\alpha} \otimes \rho)$$

with the α which minimizes the value of $k(\chi^{-\alpha} \otimes \rho)$. This α (mod $(p-1)$) is unique unless the restriction of ρ to an inertia group at p is the direct sum of two different powers of χ.

If ρ is tamely ramified, then we have $v_p(\mathcal{D}_{K/\mathbb{Q}_p}) < 1$, where v_p denotes the valuation of K normalized by $v_p(p) = 1$. So we assume from now on that ρ is wildly ramified. Let us recall the definition of the Serre weight $k(\rho)$ in this case. A wildly ramified representation ρ, restricted to an inertia group I_p at p, has the following form:

$$\rho|_{I_p} \ \sim \ \begin{pmatrix} \chi^\beta & * \\ 0 & \chi^\alpha \end{pmatrix} \qquad \text{with } * \neq 0, \tag{1.1}$$

where $\sim$ denotes the equivalence relation of representations of I_p. Take the integers α and β (uniquely) so that $0 \leq \alpha \leq p-2$ and $1 \leq \beta \leq p-1$. We set $a = \min(\alpha, \beta)$, $b = \max(\alpha, \beta)$, and define

$$k(\rho) \ := \ \begin{cases} 1 + pa + b + p - 1 & \text{if } \beta - \alpha = 1 \text{ and } \chi^{-\alpha} \otimes \rho \text{ is not finite,} \\ 1 + pa + b & \text{otherwise.} \end{cases}$$

Thus, if we write

$$\rho|_{I_p} \ \sim \ \chi^\alpha \begin{pmatrix} \chi^{k-1} & * \\ 0 & 1 \end{pmatrix}$$

with $2 \leq k \leq p$, then we have

$$\tilde{k}(\rho) \ = \ \begin{cases} p+1 & \text{if } k = 2 \text{ and } \chi^{-\alpha} \otimes \rho \text{ is not finite,} \\ k & \text{otherwise.} \end{cases}$$

We shall prove

Theorem 3. *Suppose $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is wildly ramified, with α, β as in (1.1). Let $\tilde{k} = \tilde{k}(\rho)$ be the reduced Serre weight of ρ. Put $d := (\alpha, \beta, p-1) = (\alpha, \tilde{k}-1, p-1)$. Let p^m be the wild ramification index of $K/\mathbb{Q}_p$. Then we have*

$$v_p(\mathcal{D}_{K/\mathbb{Q}_p}) \ = \ \begin{cases} 1 + \frac{\tilde{k}-1}{p-1} - \frac{\tilde{k}-1+d}{(p-1)p^m} & \text{if } \ 2 \leq \tilde{k} \leq p, \\ 2 + \frac{1}{(p-1)p} - \frac{2}{(p-1)p^m} & \text{if } \ \tilde{k} = p+1. \end{cases}$$

Remarks. (1) The value of $v_p(\mathcal{D}_{K/\mathbb{Q}_p})$ is the largest in the last case, so we have in general

$$v_p(\mathcal{D}_{K/\mathbb{Q}_p}) \;\le\; 2+\frac{1}{(p-1)p}-\frac{2}{(p-1)p^m}.$$

This bound coincides with Tate's one ([21], Remark 1 on p. 155) if $m=1$ or $p=2$, and is smaller if $m>1$ and $p>2$.

(2) The case of $\tilde{k}=2$ is comparable to (the $n=1$ case of) the bound of Fontaine ([5], Théorème 1); the main term $1+1/(p-1)$ is the same. We have the correction term $-2/(p-1)p^m$.

(3) Suppose $2<\tilde{k}\le p$. If $d_0 := (\tilde{k}-1,p-1)\ge 2$, then the value of $d=(\alpha,\tilde{k}-1,p-1)$ may vary if ρ is twisted by a power of χ. The largest value d_0 is attained by $\chi^{-\alpha}\otimes\rho$. So the minimum value of $v_p(\mathcal{D}_{K/\mathbb{Q}_p})$, with $K/\mathbb{Q}_p$ corresponding to $\mathrm{Ker}(\chi^i\otimes\rho)$ for various i, is $1+\frac{\tilde{k}-1}{p-1}-\frac{\tilde{k}-1+d_0}{(p-1)p^m}$.

Proof. Let $K_0/\mathbb{Q}_p$ (resp. $K_1/\mathbb{Q}_p$) be the maximal unramified (resp. maximal tamely ramified) subextension of $K/\mathbb{Q}_p$ (so K_1/K_0 is cut out by the representation $\chi^\alpha\oplus\chi^\beta$ and K/K_1 by the representation $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$). Then K_1 is a subfield of $K_0(\zeta_p)$, where ζ_p is a primitive pth root of unity, and K_1/K_0 has degree (and ramification index) $e:=(p-1)/d$. The extension K/K_1 has degree (and ramification index) p^m. Set $\Delta=\mathrm{Gal}(K_1/K_0)$ and $H=\mathrm{Gal}(K/K_1)$. Then Δ may be identified with a quotient of $\mathrm{Gal}(K_0(\zeta_p)/K_0)\simeq(\mathbb{Z}/p\mathbb{Z})^\times$. In fact, we have $\Delta\simeq((\mathbb{Z}/p\mathbb{Z})^\times)^d\simeq\mathbb{Z}/e\mathbb{Z}$, and its character group $\widehat{\Delta}$ is generated by χ^d. The group Δ acts on the $\mathbb{F}_p$-module H by conjugation and, in view of (1.1), this action is via $\chi^{\beta-\alpha}=\chi^{\tilde{k}-1}$;

$$\begin{pmatrix}\chi^\beta(\sigma) & b(\sigma)\\ 0 & \chi^\alpha(\sigma)\end{pmatrix}\begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}\begin{pmatrix}\chi^\beta(\sigma) & b(\sigma)\\ 0 & \chi^\alpha(\sigma)\end{pmatrix}^{-1} = \begin{pmatrix}1 & \chi^{\beta-\alpha}(\sigma)*\\ 0 & 1\end{pmatrix}$$

for $\sigma\in I_p$. Thus we have $H=H(\chi^{\tilde{k}-1})$ if we denote by $\mathcal{H}(\chi^i)$ the χ^i-part (= the part on which $\sigma\in\Delta$ acts by multiplication by $\chi^i(\sigma)$) of any $\mathbb{F}_p[\Delta]$-module $\mathcal{H}$.

Now set $U=(1+\pi\mathcal{O})^\times/(1+\pi\mathcal{O})^p$, where π (resp. $\mathcal{O}$) is a uniformizer (resp. the integer ring) of K_1. Here and elsewhere, we denote by $(1+\pi\mathcal{O})^p$ the subgroup of pth powers in $(1+\pi\mathcal{O})^\times$. By local class field theory, we have the reciprocity map

$$r:\; U \twoheadrightarrow H.$$

The Galois group Δ acts naturally on U, so U decomposes as $U=\oplus_{i=1}^e U(\chi^{di})$. Since the map r is compatible with the actions of Δ on U and H, only $U(\chi^{\tilde{k}-1})$ is mapped onto H and the other parts go to 0;

$$r(U(\chi^{di})) \;=\; \begin{cases}0 & \text{if } di\not\equiv\tilde{k}-1 \pmod{p-1},\\ H & \text{if } di\equiv\tilde{k}-1 \pmod{p-1}.\end{cases} \tag{1.2}$$

Next we shall examine $U(\chi^i)$ more closely. Any element of U can be represented by an element $1+u_1\pi+u_2\pi^2+\dots$ of $(1+\pi\mathcal{O})^\times$, where u_i are units of K_0.

Claim. For any $\sigma \in \Delta$, a unit u of K_0, and $i \geq 1$, one has

$$\sigma(1+u\pi^i) \ \equiv \ (1+u\pi^i)^{\chi^{di}(\sigma)} \qquad (\mathrm{mod}\ \pi^{i+1}).$$

Proof. By considering K_1 as a subfield of $K_0(\zeta_p)$, we may reduce this to the case of $K_1 = K_0(\zeta_p)$ and $d = 1$. Also the validity of the Claim is independent of the choice of a uniformizer π. So it is enough to show

$$\sigma(1+u\pi^i) \ \equiv \ (1+u\pi^i)^{\chi^{i}(\sigma)} \qquad (\mathrm{mod}\ \pi^{i+1})$$

assuming that $\pi = \zeta_p - 1$. Since $\sigma(\zeta_p) = \zeta_p^{\chi(\sigma)}$, we have $\sigma(\pi) \equiv \chi(\sigma)\pi$ (mod π^2), hence if u is a unit of K_0 then $\sigma(u\pi^i) \equiv \chi^i(\sigma)u\pi^i$ (mod π^{i+1}). This implies the above congruence. $\square$

Let $U^{(i)}$ be the image of $(1+\pi^i\mathcal{O})^\times$ in U. Note that $(1+p\pi^2\mathcal{O})^\times \subset (1+\pi\mathcal{O})^p$ (i.e. $U^{(e+2)} = U^{(p+1)} = 0$) if $d = 1$, and $(1+p\pi\mathcal{O})^\times \subset (1+\pi\mathcal{O})^p$ (i.e. $U^{(e+1)} = 0$) if $d \geq 2$. By the above Claim, we have

$$(1.3) \qquad \begin{cases} U(\chi^{di}) \xrightarrow{\sim} U^{(i)}/U^{(i+1)} & \text{if } d \geq 2 \text{ or } 2 \leq i \leq e, \\ U(\chi) \xrightarrow{\sim} U^{(1)}/U^{(2)} \oplus U^{(p)} & \text{if } d = i = 1. \end{cases}$$

This shows that, if $d \geq 2$ or $\tilde{k} \neq 2, p+1$, then by (1.2) we have

$$(1.4) \qquad r(U^{(i)}) \ = \ \begin{cases} 0 & \text{if } i > \frac{\tilde{k}-1}{d}, \\ H & \text{if } i \leq \frac{\tilde{k}-1}{d}. \end{cases}$$

If $d = 1$ and $\tilde{k} = 2, p+1$, we claim that $r(U^{(p)}) = 0$ if and only if $\tilde{k} = 2$, so that (1.4) is valid also in this case. Indeed, it is proved in §2.8 of [19] that $\tilde{k} = 2$ (i.e. $(\chi^{-\alpha} \otimes \rho)|_{I_p}$ is finite) if and only if K/K_1 is "peu ramifiée", i.e., K is obtained by adjoining pth roots of *units* of K_1 (actually, this was his original definition of the Serre weight's being 2). Suppose $\tilde{k} = 2$ or $p+1$. By (1.3), a non-trivial cyclic subextension $K_1(\xi^{1/p})/K_1$ has conductor (π^2) or (π^{p+1}), and accordingly has different (π^2) or (π^{p+1}). But the different is easily seen to divide (p) if ξ is a unit. Thus K/K_1 is peu ramifiée if and only if $r(U^{(p)}) = 0$.

To calculate the value of $v_p(\mathcal{D}_{K/\mathbb{Q}_p})$, we now distinguish the two cases, $2 \leq \tilde{k} \leq p$ and $\tilde{k} = p+1$.

Case $2 \leq \tilde{k} \leq p$: By (1.4), any non-trivial character $\psi \in \widehat{H} := \mathrm{Hom}(H, \mathbb{C}^\times)$ has conductor $(\pi^{(\tilde{k}-1)/d+1})$. By the Führerdiskriminantenproduktformel, we have

$$\begin{aligned} v_p(\mathcal{D}_{K/K_1}) \quad &= \quad \frac{1}{[K:K_1]} v_p(d_{K/K_1}) \\ &= \quad \frac{p^m-1}{p^m}\left(\frac{\tilde{k}-1}{d}+1\right) v_p(\pi) \ = \ \left(\frac{\tilde{k}-1}{p-1}+\frac{1}{e}\right)\left(1-\frac{1}{p^m}\right). \end{aligned}$$

Combining this with the tame part

$$v_p(\mathcal{D}_{K_1/K_0}) \ = \ \frac{1}{[K_1:K_0]} v_p(d_{K_1/K_0}) \ = \ 1 - \frac{1}{e},$$

we have

$$v_p(\mathcal{D}_{K/\mathbb{Q}_p}) \;=\; 1 + \frac{\tilde{k}-1}{p-1} - \frac{\tilde{k}-1+d}{(p-1)p^m}.$$

Case $\tilde{k} = p+1$: We have $d = 1$ in this case, and (1.4) shows that non-trivial characters $\psi \in \widehat{H}$ have conductor either (π^2) or (π^{p+1}). In fact, exactly one pth of all the characters have conductor dividing (π^2) and the rest have conductor (π^{p+1}) (this is remarked in Remarque (2) in §2.4 of [19], and a similar fact had been noticed already in the proof of the Lemma in [21]). We reproduce here the proof given in [10], Lemma 3.5.4. This follows from the fact that the subgroup $(1+\pi\mathcal{O})^p$ has index p in $(1+\pi p\mathcal{O})^\times$. To show this, consider the commutative diagram

$$\begin{tikzcd}
(1+\pi\mathcal{O})^p/(1+\pi^2 p\mathcal{O})^\times \arrow[r, "\subset"] \arrow[d, "\wr"'] & (1+\pi p\mathcal{O})^\times/(1+\pi^2 p\mathcal{O})^\times \arrow[d, "\wr"] \\
\wp(\mathbb{F}) \arrow[r, "\subset"'] & \mathbb{F},
\end{tikzcd}$$

where $\mathbb{F}$ is (the additive group of) the residue field of K_1, $\wp(\mathbb{F})$ is the subgroup $\{x + (\pi^{p-1}/p)x^p;\ x \in \mathbb{F}\}$ of $\mathbb{F}$, and the right vertical arrow is the map $1 + \pi p x (\mathrm{mod}\ \pi^2 p) \mapsto x (\mathrm{mod}\ \pi)$. This map induces the map $(1+\pi x)^p (\mathrm{mod}\ \pi^2 p) \mapsto x + (\pi^{p-1}/p)x^p (\mathrm{mod}\ \pi)$ on the left-hand side. We claim that $\wp(\mathbb{F})$ has index p in $\mathbb{F}$. This is equivalent to that the map

$$\begin{array}{rccc} \wp : & \mathbb{F} & \rightarrow & \mathbb{F} \\ & x & \mapsto & x + ux^p, \end{array}$$

where $u := \pi^{p-1}/p \ (\mathrm{mod}\ \pi)$, has kernel of dimension 1 over $\mathbb{F}_p$. The dimension depends only on the class of u in $\mathbb{F}^\times/(\mathbb{F}^\times)^{p-1}$, which is independent of the choice of a uniformizer π of K_1. Since $K_1 = K_0(\zeta_p) = K_0((-p)^{1/(p-1)})$ now, we may take π so that $\pi^{p-1}/p = -1$, in which case the kernel has dimension 1. Now again by the Führerdiskriminantenproduktformel, we have

$$\begin{aligned}
v_p(\mathcal{D}_{K/K_1}) &= \frac{1}{[K:K_1]} v_p(d_{K/K_1}) \\
&= \frac{1}{p^m}((p^m - p^{m-1})(p+1) + (p^{m-1}-1)2)v_p(\pi) \\
&= 1 + \frac{2}{p-1} - \frac{1}{p} - \frac{2}{(p-1)p^m}.
\end{aligned}$$

Combining this with the tame part

$$v_p(\mathcal{D}_{K_1/K_0}) \;=\; 1 - \frac{1}{p-1},$$

we obtain

$$v_p(\mathcal{D}_{K/\mathbb{Q}_p}) \;=\; 2 + \frac{1}{(p-1)p} - \frac{2}{(p-1)p^m}.$$

2. Proof of Theorem 1. In this section, we prove Theorem 1. As in [21], the proof splits into two cases, according as $G = \mathrm{Im}(\rho)$ is solvable or not. We assume $p \geq 5$ since the cases $p = 2$ and 3 are done respectively in [21] and [18] (cf. also [1] and [12] for the cases of $p = 5, 7$).

(1) Solvable case. Suppose G is solvable. To deal with the cases $p \leq 19$, we proceed as follows: According to [20], a maximal irreducible solvable subgroup $\mathbf{G}$ of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ has the following structure: either

(i) Imprimitive case: $\mathbf{G}$ is isomorphic to the wreath product $\overline{\mathbb{F}}_p^\times \wr (\mathbb{Z}/2\mathbb{Z})$, or

(ii) Primitive case: one has exact sequences

$$\begin{array}{llll} 1 \to \mathbf{A} \to & \mathbf{G} & \to \overline{\mathbf{G}} \to 1, & \text{with } \overline{\mathbf{G}} \simeq \mathrm{SL}_2(\mathbb{F}_2) \simeq S_3, \\ 1 \to \overline{\mathbb{F}}_p^\times \to & \mathbf{A} & \to \overline{\mathbf{A}} \to 1, & \text{with } \overline{\mathbf{A}} \simeq \mathbb{F}_2^{\oplus 2}. \end{array}$$

Note that, in either case, a finite subgroup of $\mathbf{G}$ has order prime to p. So, when $p \leq 19$, we are done if we show the following lemma, since the pth cyclotomic field $\mathbb{Q}(\zeta_p)$ has class number 1 for $p \leq 19$.

Lemma 1. *If $\mathbb{Q}(\zeta_p)$ has class number 1, then there exists no non-abelian solvable extension of $\mathbb{Q}$ which is unramified outside p and of degree prime to p.*

Proof. It is enough to show that there exists no non-trivial abelian extension of $\mathbb{Q}(\zeta_p)$ which is unramified outside p and of degree prime to p. Let $\mathcal{O}_p$ be the p-adic completion of the integer ring of $\mathbb{Q}(\zeta_p)$. By class field theory (together with the assumption "class number 1"), the Galois group of the maximal such extension is isomorphic to the quotient of $\mathcal{O}_p^\times/(1 + (\zeta_p - 1)\mathcal{O}_p)^\times \simeq \mathbb{F}_p^\times$ by the image of the global units. This group is trivial since we have at least the cyclotomic units $(\zeta_p^i - 1)/(\zeta_p - 1) \equiv i \pmod{\zeta_p - 1}$, $1 \leq i \leq p - 1$. □

To deal with the odd cases with $p \geq 23$, we appeal to the solvable case of Serre's conjecture:

Theorem 4 (cf. [7]). *Let $p \geq 3$. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an odd and irreducible representation with solvable image. Then ρ is modular of the type predicted by Serre.*

Proof. If ρ is irreducible and $G := \mathrm{Im}(\rho)$ is solvable, then as we saw above, either G has order prime to p (if $p \geq 5$) or $p = 3$ and G is an extension of a subgroup of the symmetric group S_3 by a finite solvable group of order prime to 3. By Fong-Swan's theorem (Th. 38 of [17]), there is an odd and irreducible lifting $\hat{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ of ρ to some ring $\mathcal{O}$ of algebraic integers. By Langlands-Tunnell ([8], [22]), $\hat{\rho}$, and hence ρ, is modular of weight 1. By the ε-conjecture ([4], Th. 1.12), ρ is modular of the type predicted by Serre. □

By this theorem, we can exclude the possibility of the existence of ρ with solvable image, unramified outside p, and with even Serre weight $k(\rho) \leq 10$.

(2) Non-solvable case. Suppose $G = \mathrm{Im}(\rho)$ is non-solvable. In this case, we compare the discriminant bound in Section 1 and the Odlyzko bound ([14], [15]) to deduce contradictions. We distinguish the two cases where ρ is odd

and even. If ρ is even, then the complex conjugation is mapped by ρ to $\pm\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$, so the field $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ cut out by ρ is totally real or CM. Note that the Odlyzko bound is much better (i.e. gives larger values) for totally real fields. Let K be either $\overline{\mathbb{Q}}^{\mathrm{Ker}(\rho)}$ or its maximal real subfield according as ρ is odd or even. Let $n := [K : \mathbb{Q}]$ (so $n = |G|$ or $|G|/2$ according as ρ is odd or even), and let $d_K^{1/n}$ denote the root discriminant of K.

For the Odlyzko bound to work for our purpose, the degree $n = [K : \mathbb{Q}]$ has to be large to a certain extent. Set $G_1 := G \cap \mathrm{SL}_2(\overline{\mathbb{F}}_p)$. We have an exact sequence

$$1 \;\to\; G_1 \;\to\; G \;\to\; \det(G) \;\to\; 1.$$

Since $\det\rho = \chi^{k-1}$, we have $\det(G) = (\mathbb{F}_p^\times)^{k-1} \simeq \mathbb{Z}/e\mathbb{Z}$ if we put $e := (p-1)/(k-1, p-1)$. If G is non-solvable, so is the image $\overline{G}_1$ of G_1 in $\mathrm{PSL}_2(\overline{\mathbb{F}}_p)$, and hence we have $|\overline{G}_1| \geq 60$. Furthermore, Brueggeman makes a nice observation after the proof of Lemma 3.1 of [1] as follows: Since G_1 is non-solvable, it contains an element of order 2, which must be $-\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ as it is the only element of order 2 of $\mathrm{SL}_2(\overline{\mathbb{F}}_p)$ if $p \neq 2$. Thus we have $|G| \geq 120e$.

If ρ is at most tamely ramified, then we have $d_K^{1/n} < p$. On the other hand, if $n \geq 120e$, by the Odlyzko bound [14], we have $d_K^{1/n} > p$ in all the cases we need (assuming the GRH for $p = 23, 29, 31$). Thus we may assume ρ is wildly ramified.

If p^m divides the order of G (hence of G_1) and ρ is irreducible, then by §§251–253 of [3], the image $\overline{G}_1$ of G_1 in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$ coincides with a conjugate of $\mathrm{PSL}_2(\mathbb{F}_{p^m})$. Thus we have $n = |G| \geq 2e \times |\,\mathrm{PSL}_2(\mathbb{F}_{p^m})| = e(p^{2m}-1)p^m$ if ρ is odd, and $n = |G|/2 \geq e \times |\,\mathrm{PSL}_2(\mathbb{F}_{p^m})| = e(p^{2m}-1)p^m/2$ if ρ is even. Let us denote these values by $n(p^m, k)$;

$$n(p^m, k) \;:=\; \begin{cases} e(p^{2m}-1)p^m & \text{if } k \text{ is even,} \\ e(p^{2m}-1)p^m/2 & \text{if } k \text{ is odd.} \end{cases}$$

To show the non-existence of a ρ, it is enough to show the non-existence of a twist $\chi^{-\alpha} \otimes \rho$ of it. So in what follows, we may assume that ρ has Serre weight $k \leq p+1$ (hence $d = (k-1, p-1)$ in the notation of Theorem 3) for our ρ; this minimizes the bound of Theorem 3 (see Remark (3) after Theorem 3).

We compare inequalities implied by Odlyzko and Tate bounds for each (p, k, m) to deduce contradictions proving the non-existence of ρ, the Odlyzko bound being calculated with $n \geq n(p^m, k)$ by using either [14] or [15] (Eqn. (10) (assuming the GRH) and (16) of *loc. cit.*). In general, under the GRH and for not too large n, the values from [14] are better, and otherwise we use [15]. In most cases, it is enough to compare the $n \geq n(p^1, k)$ case of the Odlyzko bound and the $m = \infty$ case of the Tate bound. Sometimes, however, it happens that we have to look at the cases $m = 1$ and $m \geq 2$ separately.

Also, to prove the finiteness of ρ's, we only need to have the contradictions for sufficiently large n, because if the degree n is bounded, by the Hermite-Minkowski theorem, there exist only finitely many extensions $K/\mathbb{Q}$ which are unramified outside a given finite set of primes and of degree $\leq n$. Thus we only need to compare the Tate bound with $m = \infty$ and the asymptotic Odlyzko bound, which says that, for sufficiently large $n = [K : \mathbb{Q}]$, one has

$$d_K^{1/n} > \begin{cases} 22.381 & \text{for any } K, \\ 60.839 & \text{for totally real } K, \\ 44.763 & \text{under GRH, for any } K, \\ 215.332 & \text{under GRH, for totally real } K. \end{cases}$$

The comparison for proving the finiteness is easily done, so in the following we focus on the proof of the non-existence. As typical cases, we present here only the proof of the cases of $p = 11$ and 23.

Case $p = 11$: For $k = 2, ..., 12$, we have respectively $n(11, k) = 13200$, 3300, 13200, 3300, 2640, 3300, 13200, 3300, 13200, 660, 13200. If $n \geq n(11, k)$, the Odlyzko bound implies

$$d_K^{1/n} > \begin{cases} 22.108 & \text{for } k = 2, 4, 8, 10, 12, \\ 58.598 & \text{for } k = 3, 5, 7, 9, \\ 21.592 & \text{for } k = 6, \\ 54.517 & \text{for } k = 11, \\ 34.768 & \text{under GRH, for } k = 2, 4, 8, 10, 12, \\ 122.112 & \text{under GRH, for } k = 3, 5, 7, 9, \\ 31.645 & \text{under GRH, for } k = 6, \\ 97.979 & \text{under GRH, for } k = 11. \end{cases} \tag{2.1}$$

On the other hand, the Tate bound ($m = \infty$) implies

$$d_K^{1/n} \leq \begin{cases} 13.981 & \text{if } k = 2, \\ 17.770 & \text{if } k = 3, \\ 22.585 & \text{if } k = 4, \\ 28.705 & \text{if } k = 5, \\ 36.483 & \text{if } k = 6, \\ 46.370 & \text{if } k = 7, \\ 58.935 & \text{if } k = 8, \\ 74.905 & \text{if } k = 9, \\ 95.203 & \text{if } k = 10, \\ 121 & \text{if } k = 11, \\ 123.667 & \text{if } k = 12. \end{cases} \tag{2.2}$$

Comparing (2.1) and (2.2), we obtain contradictions for $k = 2, 3, 5, 7$, and also for $k = 4, 9$ assuming the GRH. For $k = 6, 11$, we look at the cases $m = 1$ and

$m \geq 2$ separately. If $m = 1$, the Tate bound implies

$$d_K^{1/n} \ < \ \begin{cases} 29.338 & \text{if } k = 6, \\ 78.243 & \text{if } k = 11. \end{cases} \tag{2.3}$$

Comparing (2.1) and (2.3), we obtain contradictions for $k = 6, 11$ assuming the GRH. For $m = 2$ and $k = 6, 11$, we have $n(11^2, k) = 3542880, 885720$. If $n \geq n(11^2, k)$, the Odlyzko bound implies

$$d_K^{1/n} \ > \ \begin{cases} 40.458 & \text{under GRH, for } k = 6, \\ 168.971 & \text{under GRH, for } k = 11. \end{cases} \tag{2.4}$$

Comparing (2.2) and (2.4), we obtain contradictions for $k = 6, 11$ assuming the GRH.

Case $p = 23$: For $p = 23, 29, 31$, we rely on Theorem 4 in the solvable image case, so we can prove the non-existence at most in the odd case (i.e. when k is even). Let $p = 23$. We have $n(23, k) = 267168$ for $k = 2, 4, 6$. If n is greater than or equal to this value, the Odlyzko bound implies

$$d_K^{1/n} \ > \ 37.994 \qquad \text{under GRH.} \tag{2.5}$$

On the other hand, the Tate bound implies

$$d_K^{1/n} \ < \ \begin{cases} 26.524 & \text{if } k = 2, \\ 35.272 & \text{if } k = 4, \\ 46.905 & \text{if } k = 6. \end{cases} \tag{2.6}$$

Comparing (2.5) and (2.6), we obtain contradictions for $k = 2, 4$.

3. Representations with non-trivial Artin conductor.

In this section, we prove Theorem 2 and extend Theorem 1 to some other cases where the representations ρ have non-trivial Artin conductors outside p. We present in §3.1 (resp. §3.2) the cases where we can prove the non-existence (resp. finiteness) of $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. We denote by $N(\rho)$ the Artin conductor of ρ outside p. In both cases, we use:

Lemma 2. *Let $K/\mathbb{Q}$ be the extension which corresponds to the kernel of ρ, and $n = [K : \mathbb{Q}]$. Let d'_K be the prime-to-p part of the discriminant of K. Then if $|d'_K| > 1$, we have*

$$|d'_K|^{1/n} \ < \ N(\rho).$$

Proof. This is Lemma 3.2, (ii) of [13]. Note that, in the proof there, one has $i_{E/F} > 0$ if the extension E/F is ramified, whence the strict inequality in the above lemma. □

3.1. Non-existence.

We first prove Theorem 2. Let $K/\mathbb{Q}$ be the extension corresponding to the kernel of the representation ρ. If for example $p \geq 1000003$, then for $n \geq 2 \times |\,\mathrm{PSL}_2(\mathbb{F}_p)| \geq 4000036000104000096$, the Odlyzko bound implies, under the GRH, that the root discriminant of K is $> 44.17....$ Noticing

Lemma 2, we conclude that there is no ρ which is unramified at p, with $N(\rho) \leq 44$, and has projective image containing $\mathrm{PSL}_2(\mathbb{F}_p)$.

To extend Theorem 1, we consider as in Section 2 the solvable and non-solvable cases separately. We shall consider only the odd cases. In the solvable case, by Theorem 4, we only need to calculate the dimension of the $\mathbb{C}$-vector space $S_k(\Gamma_1(N))$ of cusp forms of weight k with respect to the congruence subgroup $\Gamma_1(N)$. This is done by using, e.g., Chapters 2 and 3 of [9]. If $N \geq 2$, the values of (N, k) for which $S_k(\Gamma_1(N)) = 0$ are:

$(N, k) = (2, 2), (2, 4), (2, 6), (2, \mathrm{odd})$;

$(N, k) = (3, 2), (3, 3), (3, 4), (3, 5); (4, 2), (4, 3), (4, 4); (5, 2), (5, 3); (6, 2), (6, 3)$;

and

$(N, 2)$ for $N = 7, 8, 9, 10, 12$.

The non-solvable case is also done in a similar way to that in Section 2 by comparing various discriminant bounds, except that we take the Artin conductor into account. Combining with the solvable case, we obtain:

Theorem 5. *There exists no odd and irreducible representation* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ *of reduced Serre weight* k *and Artin conductor* N *outside* p *in the following cases:*

Case $N = 2$*:* $(p, k) = (3, 2), (3, 3), (3, 4); (5, 2); (7, 2)$.

Case $N = 3$*:* $(p, k) = (2, 2), (2, 3)$.

Case $N = 4$*:* $(p, k) = (3, 2)$.

Case $N = 5$*:* $(p, k) = (2, 2)$.

Assuming the GRH, we obtain the non-existence of ρ*, besides the above cases, in the following cases:*

Case $N = 2$*:* $(p, k) = (5, 3); (7, 3); (11, 2); (13, 2)$.

Case $N = 3$*:* $(p, k) = (5, 2); (7, 2)$.

Case $N = 4$*:* $(p, k) = (3, 3)$.

Case $N = 5$*:* $(p, k) = (3, 2)$.

3.2. Finiteness. To prove the finiteness of the set of isomorphism classes of semisimple representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ with bounded Artin conductor $N(\rho)$, we only need to compare the lower bound of the discriminants by Odlyzko and the upper bound obtained as the product of the one in Theorem 3 with $m = \infty$ and the one in Lemma 2. Here we give only the results for odd representations under the assumption of the GRH. Other cases (even and/or unconditional) can be obtained similarly.

Theorem 6. *Assume the GRH. Then there exist only finitely many isomorphism classes of odd and semisimple representations* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ *with reduced Serre weight* k *and Artin conductor* N *outside* p *in the following cases:*

(1) $k = 1$*, any* p*, and* $N \leq 44$.

(2) $p = 2$*:* *(*$k = 2$ *and* $N \leq 11$*), (*$k = 3$ *and* $N \leq 7$*).*

(3) $p = 3$*:* *(*$k = 2$ *and* $N \leq 8$*), (*$k = 3$ *and* $N \leq 4$*), (*$k = 4$ *and* $N \leq 4$*).*

(4) For other p and $k > 1$;
$N = 2$ *and* $(p,k) = (5,2),(5,4),(7,2),(7,4),(11,2),(13,2)$.
(Note that, when $N = 2$, the representation ρ is odd if and only if k is even.)
$N = 3$ *and* $(p,k) = (5,2),(5,3),(7,2),(7,3),(11,2)$.
$N = 4$ *and* $(p,k) = (5,2),(7,2)$.

To keep the table compact, we classified the cases in an unsystematic manner. We hope to give a more convenient table on a suitable web site.

References

[1] S. Brueggeman, *The nonexistence of certain Galois extensions unramified outside 5*, J. Number Theory 75(1999), 47–52

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

[3] L. E. Dickson, *Linear Groups*, Teubner, 1901, Leibzig

[4] B. Edixhoven, *Serre's conjectures*, in: "Modular Forms and Fermat's Last Theorem" (G. Cornell, J.H. Silverman, G. Stevens (eds.)), Springer-Verlag, 1997

[5] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. 81(1985), 515–538

[6] K. Joshi, *Remarks on methods of Fontaine and Faltings*, Intern. Math. Res. Notices 22(1999), 1199–1209

[7] E. Kimura, H. Moon and Y. Taguchi, in preparation

[8] R. Langlands, *Base Change for* GL(2), Princeton Univ. Press

[9] T. Miyake, *Modular Forms*, Springer-Verlag, 1989

[10] H. Moon, *On the finiteness of mod p Galois representations*, Thesis, Tokyo Metropolitan University, 2000

[11] H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory 84(2000), 156–165

[12] H. Moon, *The non-existence of certain mod p Galois representations*, Bull. Korean Math. Soc. 40(2003), 537–544

[13] H. Moon and Y. Taguchi, *Mod p Galois representations of solvable image*, Proc. A.M.S. 129(2001), 2529–2534

[14] A. M. Odlyzko, *Discriminant bounds*, unpublished manuscript (1976), available at:
`http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`

[15] G. Poitou, *Sur les petits discriminants*, Sém. Delange-Pisot-Poitou (Théorie des nombres), 18e année, 1976/77, n^o 6

[16] J.-P. Serre, *Congruences et formes modulaires (d'aprés H.P.F. Swinnerton-Dyer)*, Sém. Bourbaki 1971/72, n^o 416, in: Œuvres III, Springer-Verlag, 1986, pp. 74–88

[17] J.-P. Serre, *Représentations Linéaires des Groupes Finis* (5ème éd.), Hermann, 1998

[18] J.-P. Serre, Note 229.$_2$ on p. 710, Œuvres III, Springer-Verlag, 1986

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

[20] D. A. Suprunenko, *Matrix Groups*, A.M.S., Providence, 1976

[21] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside* 2, Contemp. Math. 174(1994), 153–156

[22] J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. 5(1981), 173–175

Hyunsuk Moon
Graduate School of Mathematics
Kyushu University 33
Fukuoka 812-8581
Japan
moon@math.kyushu-u.ac.jp

Yuichiro Taguchi
Graduate School of Mathematics
Kyushu University 33
Fukuoka 812-8581
Japan
taguchi@math.kyushu-u.ac.jp