Bull. Korean Math. Soc. **40** (2003), No. 3, pp. 537–544

THE NON-EXISTENCE OF CERTAIN MOD p GALOIS REPRESENTATIONS

HYUNSUK MOON

ABSTRACT. The non-existence is proved of continuous irreducible representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ with Artin conductor N outside p for a few small values of p and N.

1. Introduction

Let $G_{\mathbb{Q}}$ be the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$. Let $\overline{\mathbb{F}}_p$ be an algebraic closure of the finite field $\mathbb{F}_p$ of p elements. We consider continuous representations $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. Serre ([9]) conjectured that every odd and irreducible such representation ρ should arise from a modular eigenform with conjectured level, weight and character. In particular, it is conjectured that there exists no odd and irreducible representation ρ which is unramified outside p if $p = 2, 3, 5, 7$, because the conjectured weight, after twisting ρ by a power of the mod p cyclotomic character, is less than or equal to $p + 1$ and cusp forms for $\mathrm{SL}_2(\mathbb{Z})$ do not exist for $k < 12$. Tate ([11]) showed the non-existence in the case of $p = 2$, and Serre ([8]) also remarked that this can be extended to the case of $p = 3$ by the same method. Recently Brueggeman ([3]) showed the non-existence in the case of $p = 5$ assuming the Generalized Riemann Hypothesis (GRH).

Along this line, we show in this paper the non-existence of some representations having non-trivial Artin conductor $N(\rho)$ outside p (see §1 of [9] for the definition of $N(\rho)$):

Received November 13, 2002.

2000 Mathematics Subject Classification: 11F80, 11R39.

Key words and phrases: mod p Galois representation; Serre's conjecture; class field theory; Odlyzko's bound.

This work was partially supported by the Brain Korea 21 Project in 2001.

THEOREM 1. *There exist no non-trivial Galois representations* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ *which are semisimple and have* $N(\rho)$ *dividing 3.*

THEOREM 2. *Assume the GRH. Let* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ *be a non-trivial semisimple representation with* $N(\rho)$ *dividing 2. Then* $\rho \simeq 1 \oplus \chi_3$ *or* $\chi_3 \oplus \chi_3$, *where* χ_3 *is the mod 3 cyclotomic character.*

As in [11], [3], our proof is divided into two parts. If $\mathrm{Im}(\rho)$ is solvable, we use a structure theorem on solvable subgroups of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$, class field theory and Jones' database ([5]). Then we find that our representation is abelian. Here we do not use the condition on the parity of $\det \rho$. If $\mathrm{Im}(\rho)$ is non-solvable, we compare two different estimations of the discriminant of the kernel field of ρ to deduce contradiction.

By using a discriminant estimate, it is impossible (even under the GRH) to prove the conjecture of Serre for $p = 7$ with $N(\rho) = 1$ (cf. [3]). However, for *even* mod 7 representations, we can show:

THEOREM 3. *Assume the GRH. Let* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_7)$ *be a semisimple even representation which is unramified outside 7. Then* $\rho \simeq \chi_7^a \oplus \chi_7^b$ *with* $a + b =$ *even, where* χ_7 *is the mod 7 cyclotomic character.*

This has no relation to the conjecture of Serre anymore. However Ash et al. ([1], [2]) made an analogue of Serre's conjecture for higher dimensional representations by using cohomology classes instead of modular forms. In particular, the direct sum of an even two-dimensional representation and an odd character gives rise to an odd three-dimensional representation. Thus Theorem 3 implies the validity of a special case of the three-dimensional case of this conjecture.

2. Solvable case

Let G be an irreducible solvable subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ and H its maximal abelian normal subgroup. Let A be a normal subgroup of G such that A/H is a maximal abelian normal subgroup of G/H. Then from §19–§21 of [10], G is either of the following types:

(G1)

$$1 \longrightarrow H \longrightarrow G \longrightarrow \mathbb{Z}/2 \longrightarrow 1, \qquad H \subset (\overline{\mathbb{F}}_p^{\times})^2.$$

(G2)

$$1 \longrightarrow A \longrightarrow G \longrightarrow \overline{G} \longrightarrow 1, \qquad \overline{G} \subset S_3 \ (\simeq \mathrm{SL}_2(\mathbb{F}_2)),$$

$$1 \longrightarrow H \longrightarrow A \longrightarrow \overline{A} \longrightarrow 1, \qquad H \subset \overline{\mathbb{F}}_p^{\times}, \quad \overline{A} \subset (\mathbb{Z}/2)^2.$$

Furthermore, if G is maximal, then all the inclusions are the equalities. If $p = 2$, only type (G1) is possible. Also, $\overline{G}$ acts on $\overline{A}$ by conjugation, and $\overline{G}$ injects into $\mathrm{Aut}(\overline{A})$, since $\overline{A}$ is its own centralizer in G/H (cf. [10], §19, Th. 3).

2.1. Case $p = 2$ and $N(\rho) \mid 3$

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ with $N(\rho) \mid 3$. We first note that $N(\rho) = 3$ means that we allow tame ramification at 3. Let $K/\mathbb{Q}$ be the fixed field by $\mathrm{Ker}(\rho)$ and $G = \mathrm{Im}(\rho)$ its Galois group. Suppose G is solvable. When G is a reducible subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$, simisimplicity implies that G is isomorphic to a diagonal matrix group. So G embeds in $\overline{\mathbb{F}}_2^{\times} \oplus \overline{\mathbb{F}}_2^{\times}$ which has no elements of order 2. However, since $K/\mathbb{Q}$ is an abelian extension unramified outside $\{2, 3\}$ and at most tamely ramified at 3, the Kronecker-Weber theorem implies that K is a subfield of a cyclotomic field $\mathbb{Q}(\zeta_{2^r}, \zeta_3)$ and G is isomorphic to a quotient of $(\mathbb{Z}/2^r)^{\times} \times (\mathbb{Z}/3)^{\times}$, which is a 2-group.

When G is an irreducible subgroup, G is of type (G1), that is, K is an abelian extension of odd degree over a quadratic field F. Since K is unramified outside $\{2, 3\}$, F is a quadratic subfield of $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$. By class field theory, an abelian extension of F has 2-power degree, if it is unramified outside $\{2, 3\}$ and at most tamely ramified at 3. Indeed, since each subfield of $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$ has class number 1 or 2 (even in the strong sense if it is real) for each subfield F, we just look at the quotient group $(\mathcal{O}_{F,2}^{\times} \times k_{F,3}^{\times})/\mathcal{O}_F^{\times}$. Here $\mathcal{O}_F$ is the ring of integers of F, $\mathcal{O}_{F,p} := \mathcal{O}_F \otimes_{\mathbb{Z}} \mathbb{Z}_p$ and $k_{F,p}^{\times}$ is the maximal prime-to-p quotient of $\mathcal{O}_{F,p}^{\times}$. For example, if $F = \mathbb{Q}(\sqrt{-1})$, then $\mathcal{O}_{F,2}^{\times} \simeq \mathbb{Z}/4\times$ (pro-2 group) and $k_{F,3}^{\times} = \mathbb{F}_9^{\times}$. Also, F has the group of global units isomorphic to $\mathbb{Z}/4$. Thus there is no abelian extension K/F of odd degree. Hence if G is solvable, we have $K \subset \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{-3})$, so G cannot be embedded into $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ semisimply.

2.2. Case $p = 3$ and $N(\rho) \mid 2$

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ with $N(\rho) \mid 2$. Let $K/\mathbb{Q}$ be the fixed field by $\mathrm{Ker}(\rho)$ and $G = \mathrm{Im}(\rho)$ its Galois group. Suppose G is solvable. When G is a reducible subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_3)$, semisimplicity implies that the non-trivial representations are precisely those listed in Theorem 2.

Assume that G is an irreducible subgroup. If G is of type (G1), then K is an abelian extension of degree prime to 3 over the quadratic field $F = \mathbb{Q}(\sqrt{-3})$. This field F has class number 1 and $\mathcal{O}_{F,3}^{\times} = \mathbb{F}_3^{\times}\times$ (pro-3

group), $k_{F,2}^{\times} = \mathbb{F}_4^{\times}$, $\mathcal{O}_F^{\times} \simeq \mathbb{Z}/6$. Hence, by class field theory, there is no abelian extension K/F of degree prime to 3. Thus $K = F = \mathbb{Q}(\sqrt{-3})$.

Next, we suppose that G is of type (G2). The quotient group $\overline{G}$ of G is contained in S_3. If $\overline{G}$ is S_3, then by [5], we know that there are only four S_3-extensions of $\mathbb{Q}$ which are unramified outside $\{2, 3\}$ and at most tamely ramified at 2. Each of these fields has class number 1 and has only one prime above 3, of absolute degree 1. Thus by class field theory, $\overline{A}$ cannot be isomorphic to $(\mathbb{Z}/2)^2$. Since $\overline{G} \hookrightarrow \mathrm{Aut}(\overline{A})$, it is impossible that $\overline{G} = S_3$.

Suppose $\overline{G}$ is C_3. We have just one C_3-extension of $\mathbb{Q}$ which is unramified outside $\{2, 3\}$, that is $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$. This field does not have a $(\mathbb{Z}/2)^2$-extension unramified outside 3. Indeed, such an extension would produce a 2-extension of $\mathbb{Q}(\zeta_9)$ unramified outside 3, which does not exist. So, $\overline{G} \neq C_3$.

It is also impossible that $\overline{G} = C_2$ because $\mathbb{Q}(\sqrt{-3})$ has no abelian extension of degree prime to 3 unramified outside $\{2, 3\}$.

If $\overline{G}$ is trivial, this case is reduced to the case of type (G1), since there is no quartic extension of $\mathbb{Q}$ unramified outside 3. Hence we conclude that G is abelian.

2.3. Case $p = 7$ and $N(\rho) = 1$

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_7)$ with $N(\rho) = 1$. Let $K/\mathbb{Q}$ be the fixed field by $\mathrm{Ker}(\rho)$ and $G = \mathrm{Im}(\rho)$ its Galois group. Suppose G is solvable. When G is a reducible subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_7)$, semisimplicity implies that the even representations are precisely those listed in Theorem 3.

Assume that G is an irreducible subgroup. If G is of type (G1), then K is an abelian extension of degree prime to 7 over the quadratic field $F = \mathbb{Q}(\sqrt{-7})$. F has class number 1 and has only one prime above 7, of absolute degree 1. Hence, by class field theory, we know that $K \subset \mathbb{Q}(\zeta_7)$.

Now, we consider G of type (G2). Since $\mathbb{Q}(\zeta_7)$ is the unique abelian extension of $\mathbb{Q}(\sqrt{-7})$ of degree 3 unramified outside 7, $\overline{G}$ cannot be isomorphic to S_3. If $\overline{G}$ is C_3, then its fixed field is the cubic field $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. This does not have a $(\mathbb{Z}/2)^2$-extension unramified outside 7. Indeed, such an extension would produce a 2-extension of $\mathbb{Q}(\zeta_7)$ unramified outside 7, which does not exist. If $\overline{G} \subset C_2$, by the same argument as in the case of type (G1), we have $K \subset \mathbb{Q}(\zeta_7)$. Hence we conclude G is abelian.

3. Non-solvable case

Let K be an algebraic number field of degree n, with r_1 real conjugate fields and $2r_2$ complex conjugate fields. Poitou ([7], (16)), developing the methods of Odlyzko, showed that

$$\text{(a)} \quad \frac{1}{n}\log|d_K| \geq \begin{cases} \gamma + \log 4\pi + 1 - 8.317302n^{-\frac{2}{3}} & \text{if } r_1 = n, \\ \gamma + \log 4\pi - 6.860404n^{-\frac{2}{3}} & \text{if } r_1 = 0. \end{cases}$$

Assuming the GRH, he also showed ([7], (10)) that

$$\text{(b)} \quad \begin{aligned} \frac{1}{n}\log|d_K| \geq\ & \gamma + \log 8\pi + \frac{r_1}{n}\frac{\pi}{2} \\ & - \frac{2\pi^2(\lambda + \frac{r_1}{n}\beta)}{(\log n)^2} - \frac{16\pi^2(1+\frac{1}{n})}{(\log n)^3(1+\frac{\pi^2}{(\log n)^2})^2}, \end{aligned}$$

where $\lambda = 1.0517997903$, $\beta = 0.9689461463$. Note that these bounds are monotone increasing in n if either $r_1 = n$ or 0.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ with $N(\rho) = N =$ a square free integer (≥ 1). Let $K/\mathbb{Q}$ be the fixed field by $\mathrm{Ker}(\rho)$ and G its Galois group. We let n be the order of G and let d_K be the discriminant of $K/\mathbb{Q}$. If $K/\mathbb{Q}$ is tamely ramified at p, then

$$\text{(A)} \qquad |d_K|^{1/n} \leq p^{\frac{n-1}{n}} \cdot N^{\frac{n-1}{n}} < pN.$$

If $K/\mathbb{Q}$ has wild ramification of degree p^m, Tate ([11]) showed that

$$\text{(B)} \qquad |d_K|^{1/n} \leq p^{2+\frac{1}{p}-\frac{1}{(p-1)p^{m-1}}} \cdot N^{\frac{n-1}{n}} < p^{2+\frac{1}{p}} \cdot N.$$

3.1. Comparison of the two bounds

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ with $N(\rho) = N$. We assume $G = \mathrm{Gal}(K/\mathbb{Q})$ is non-solvable. Then $|G| \geq 60$. From (a) for $n = 60$, we know that $|d_K|^{1/n} > 14.3050$. If K is tamely ramified at p, this contradicts (A) of our cases $(p, N) = (2,3), (3,2), (7,1)$. If K has wild ramification, our argument is more complicated. We consider the composite map (of ρ and the projection) $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p) \to \mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. We let $\widetilde{G}$ be the image of G and $L/\mathbb{Q}$ be the field corresponding to $\mathrm{Ker}(\bar{\rho})$. Then $\widetilde{G}$ is also non-solvable. Suppose $L/\mathbb{Q}$ has wild ramification of index p^m. Then by [4], §§251–253, we have

LEMMA 4. *Let $\widetilde{G}$ be a subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. If its p-Sylow subgroups have order p^m, $m \geq 1$, and are not normal in $\widetilde{G}$, then $\widetilde{G}$ is isomorphic to either $\mathrm{PGL}_2(\mathbb{F}_{p^m})$ or $\mathrm{PSL}_2(\mathbb{F}_{p^m})$.*

Apply this Lemma to our $\widetilde{G} \subset \mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. Note that for $p = 2, 3$ we have $m \geq 2$ because $\widetilde{G}$ is solvable if $m = 1$.

(i) Case $p = 2$ and $N = 3$:

From (B), we have

$$|d_L|^{1/n} < \begin{cases} 12 & \text{if} \quad m = 2, \\ 16.9706 & \text{if} \quad m \geq 3. \end{cases}$$

According to (a),

$$|d_L|^{1/n} > \begin{cases} 14.3050 & \text{if} \quad n \geq 60 = |\mathrm{PSL}_2(\mathbb{F}_4)|, \\ 20.0838 & \text{if} \quad n \geq 504 = |\mathrm{PSL}_2(\mathbb{F}_8)|. \end{cases}$$

Contradiction.

(ii) Case $p = 3$ and $N = 2$:

From (B), we have

$$(*) \qquad |d_L|^{1/n} < \begin{cases} 21.6169 & \text{if} \quad m = 2, \\ 25.9605 & \text{if} \quad m \geq 3. \end{cases}$$

We assume the GRH. Then from (b), we have

$$|d_L|^{1/n} > \begin{cases} 19.5441 & \text{if} \quad n \geq 360 = |\mathrm{PSL}_2(\mathbb{F}_9)|, \\ 20.5495 & \text{if} \quad n \geq 720 = |\mathrm{PGL}_2(\mathbb{F}_9)|, \\ 29.7470 & \text{if} \quad n \geq 9828 = |\mathrm{PSL}_2(\mathbb{F}_{27})|. \end{cases}$$

We have contradiction if $m \geq 3$. For the case $m = 2$, if ρ is odd, we show that the order of G is greater than or equal to $4 \times |\mathrm{PSL}_2(\mathbb{F}_9)| = 1440$ (cf. [3], §3). This follows from the two facts: (1) $G \not\subset \mathrm{SL}_2(\mathbb{F}_9)$, since ρ is odd. (2) $G \cap \mathrm{SL}_2(\mathbb{F}_9)$ contains the unique element $-I$ of order 2 in $\mathrm{SL}_2(\mathbb{F}_9)$, since it is non-solvable and any non-solvable group is of even order. Thus we have contradiction for the case $m = 2$ using the following bound which follows from (b):

$$|d_L|^{1/n} > 22.5793 \qquad \text{if} \quad n \geq 1440.$$

If ρ is even, since $p \neq 2$, K is a totally real or CM field, and L is totally real. From (a) we have

$$|d_L|^{1/n} > 51.6187 \qquad \text{if} \quad n \geq 360.$$

This contradicts $(*)$.
(iii) Case $p = 7$ and $N = 1$:
From (B), we have

$$|d_L|^{1/n} < \begin{cases} 46.7816 & \text{if} \quad m = 1, \\ 61.7737 & \text{if} \quad m \geq 2. \end{cases}$$

We assume the GRH. Since ρ is even, L is totally real. From (b), we have

$$|d_L|^{1/n} > \begin{cases} 46.2963 & \text{if} \quad n \geq 168 = |\mathrm{PSL}_2(\mathbb{F}_7)|, \\ 139.7097 & \text{if} \quad n \geq 58800 = |\mathrm{PSL}_2(\mathbb{F}_{49})|. \end{cases}$$

This bound for $n \geq 168$ is not good enough for our purpose. However, we find a better bound in [6]:

$$|d_L|^{1/n} > 69.897 \qquad \text{if} \quad n \geq 160.$$

Then we have contradiction. Hence the proof is complete.

References

[1] A. Ash, D. Doud, and D. Pollack, *Galois representations with conjectural connections to arithmetic cohomology*, Duke Math. J. **112** (2002), 521–579.

[2] A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod-p cohomology of* $\mathrm{GL}(n, \mathbb{Z})$, Duke Math. J. **105** (2000), 1-24.

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

[4] L. E. Dickson, *Linear Groups*, Dover, New York, 1958.

[5] J. Jones, *Tables of number fields with prescribed ramification*, `http://math.la.asu.edu/~jj/numberfields` (1998).

[6] A. M. Odlyzko, *Discriminant bounds*, tables dated Nov. 29, 1976 (unpublished, appeared in `http://www.dtc.umn.edu/~odlyzko/unpublished`).

[7] G. Poitou, *Sur les petits discriminants*, Seminaire Delange-Pisot-Poitou **18** (1976/ 77), no. 6.

[8] J.-P. Serre, *Œuvres Vol. III, p. 710*, Springer-Verlag, Berlin, 1986.

[9] ———, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.
[10] D. A. Suprunenko, *Matrix Groups*, Amer. Math. Soc., Providence, 1976.
[11] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside 2*, Contemp. Math. **174** (1994), 153–156.

Graduate School of Mathematics, Kyushu University, Fukuoka 812-8581, Japan
E-mail: moon@math.kyushu-u.ac.jp