Trends in Mathematics
Information Center for Mathematical Sciences
Volume 9, Number 1, June, 2006, Pages 13–16

ON MOD 3 GALOIS REPRESENTATIONS WITH CONDUCTOR 4

HYUNSUK MOON

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. In this paper, we prove the non-existence of certain mod 3 Galois representation:

Theorem 1. *There exist no irreducible representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ with $N(\rho)$ dividing* 4.

Here, $N(\rho) = \prod_{p\nmid 3} p^{n_p(\rho)}$ is the Artin conductor of ρ outside 3 ([6], §1.2; the definition of the exponent $n_p(\rho)$ will be recalled below). This proves a special case of Serre's conjecture ([6]). Indeed, the conjecture predicts that such a representation, up to twist by a power of the mod 3 cyclotomic character, come from a cuspidal eigenform of level 4 and weight ≤ 4, but there are no such forms. Such a result may serve as the first step of an inductive proof of Serre's conjecture for $N(\rho) = 4$ if Khare's proof in the case of $N(\rho) = 1$ ([3]) can be extended.

Serre's conjecture is known to be true if the image $\mathrm{Im}(\rho)$ of ρ is solvable ([4], Thm. 4). So, it remains for us to prove the Theorem 1 in the following two cases: (i) $\mathrm{Im}(\rho)$ is non-solvable, (ii) ρ is even and $\mathrm{Im}(\rho)$ is solvable.

1. Proof: Non-solvable case

Our strategy in the proof here is basically the same as in [8]; 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 form above (the refined Tate bound ([4], Thm. 3) and the other from below (the Odlyzko bound [5]). A new ingredient in this paper is the estimate of the prime-to-3 part of the discriminant. To do this, we require a few lemmas. To state them, let D_p ($\subset G_{\mathbb{Q}}$) be the decomposition subgroup for a choice of an extension of the prime ideal (p) to $\overline{\mathbb{Q}}$, and I_p its inertia subgroup. For a continuous representation $\rho : D_p \to \mathrm{GL}_{\overline{\mathbb{F}}_\ell}(V)$, where V is a finite-dimensional $\overline{\mathbb{F}}_\ell$-vector space with $\ell \neq p$, we define the exponent of Artin conductor of ρ by

$$n_p(\rho) \ := \ \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim_{\overline{\mathbb{F}}_\ell}(V/V^{G_i}).$$

Here, G_i is the ith ramification subgroup of $G := \mathrm{Im}(\rho)$.

Let p and ℓ be two distinct prime numbers, and let $\rho : D_p \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be a continuous representation with $n_p(\rho) = 2$.

Lemma 2. *(1) If ρ is irreducible, then it is tamely ramified.*

(2) If ρ is wildly ramified, then it is a direct-sum of two characters, of which one is unramified and the other has exponent of conductor 2.

Remark. This lemma holds true if D_p is the absolute Galois group of any complete discrete valuation field with finite residue filed of characteristic p.

Proof. (1) Since ρ is ramified, the inertia fixed part V^{G_0} is $\neq V$. If $\dim(V^{G_0}) = 1$, then V is reducible as a representation of D_p, because G_0 is normal in G and hence G stabilizes V^{G_0}. Thus the irreducibility of ρ implies that $\dim(V^{G_0}) = 0$. Since

$$(*) \qquad n_p(\rho) \; = \; \dim(V/V^{G_0}) + \frac{1}{(G_0 : G_1)} \dim(V/V^{G_1}) + \cdots \; = \; 2,$$

we must have $\dim(V^{G_i}) = 2$ for all $i \geq 1$, meaning that ρ is tamely ramified.

(2) Suppose ρ is wildly ramified, so that $\dim(V^{G_1}) < 2$. Then the equality $(*)$ implies that $\dim(V^{G_0}) = 1$. This means that ρ is reducible. We may assume that ρ is of the form

$$\rho \; = \; \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix},$$

where $\psi_i : D_p \to \overline{\mathbb{F}}_\ell^\times$ are characters of D_p and ψ_1 is unramified. Let $\rho^{\mathrm{ss}} = \begin{pmatrix} \psi_1 & \\ & \psi_2 \end{pmatrix}$ be the semisimplification of ρ and put $G^{\mathrm{ss}} := \mathrm{Im}(\rho^{\mathrm{ss}})$. Then G sits in a short exact sequence

$$1 \;\to\; H \;\to\; G \;\to G^{\mathrm{ss}} \;\to\; 1,$$

where $H = G \cap \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ is the kernel of the natural homomorphism $G \to G^{\mathrm{ss}}$. Note that G^{ss} is abelian of order prime to ℓ, and H is an elementary abelian ℓ-group of rank at most 2. Let $H_0 := H \cap G_0$. If $H_0 \neq 1$, then it is mapped by the projection $G_0 \to G_0/G_1$ to the unique ℓ-Sylow subgroup of the tame inertia subgroup G_0/G_1. Let $G_0^\flat$ be the inverse image in G_0 of the maximal prime-to-ℓ subgroup of the cyclic group G_0/G_1. Then H_0 and $G_0^\flat$ are both normal in G_0, $H_0 G_0^\flat = G_0$, and $H_0 \cap G_0^\flat = 1$. Hence we have $G_0 = H_0 \times G_0^\flat$. But this is impossible, because any two elements of $\left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$ of order ℓ and of order prime to ℓ do not commute (Note that $G_0^\flat \neq 1$, as $G_1 \neq 1$). Hence $H_0 = 1$ and G_0 has order prime to ℓ. Next we argue in the same way with G/G_0 in place of G_0/G_1. If $H \neq 1$, then it is mapped by the projection $G \to G/G_0$ to the unique ℓ-Sylow subgroup of G/G_0. Let $G^\flat$ be the inverse image in G of the maximal prime-to-ℓ subgroup of the cyclic group G/G_0. Then H and $G^\flat$ are both normal in G, $HG^\flat = G$, and $H \cap G^\flat = 1$. Hence $G = H \times G^\flat$. But this is again impossible by the same reason as above. Hence $G = G^\flat = G^{\mathrm{ss}}$.

□

Lemma 3. *Let $\rho : D_2 \to \mathrm{GL}_2(\overline{\mathbb{F}}_3)$ be a continuous representation with $n_2(\rho) = 2$. Then it is a direct-sum of two characters, of which one is unramified and the other* *has exponent of conductor* 2*. If* G_i *denotes the* i*th ramification subgroup of* $G := \mathrm{Im}(\rho)$*, then one has* $G_0 = G_1 \simeq \mathbb{Z}/2\mathbb{Z}$ *and* $G_2 = 1$*.*

Remark. This lemma holds true if D_2 is the absolute Galois group of a complete discrete valuation field with residue field $\mathbb{F}_2$.

Proof. We first show that ρ cannot be irreducible. Suppose ρ is irreducible. Then by Lemma 2, (1), it is tamely ramified. In particular, G is meta-abelian. An inspection of Chapter V of [7] shows that G is an extension of an elementary abelian 2-group $\overline{G}$ of rank at most 2 by an abelian group H of order prime to 3. Since ρ is tamely ramified, the extension $F/\mathbb{Q}_2$ corresponding to $\overline{G}$ is unramified and $\overline{G} \simeq \mathbb{Z}/2\mathbb{Z}$. Now H is the Galois group of a tamely ramified abelian extension of F. Since the residue field of F is $\mathbb{F}_4$, the inertia subgroup H_0 of H is a quotient of $\mathbb{F}_4^\times \simeq \mathbb{Z}/3\mathbb{Z}$. Since H has order prime to 3, we must have $H_0 = 1$. This contradicts the assumption that $n_2(\rho) = 2$.

Thus ρ is reducible, and we may assume that ρ is of the form

$$\rho = \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix},$$

where $\psi_i : D_2 \to \overline{\mathbb{F}}_3^\times$ are characters of D_2. They factor through the abelianization D_2^{ab} of D_2. Since the inertia subgroup of D_2^{ab} is isomorphic to the pro-2 group $\mathbb{Z}_2^\times$, these characters are either unramified or wildly ramified. Since $n_2(\rho) = 2$, the only possible case is that ψ_1 is unramidied and ψ_2 is wildly ramified (if $* = 0$, then the role of ψ_1 and ψ_2 may be exchanged). By Lemma 2,(2), we have $* = 0$ and $\rho \simeq \psi_1 \oplus \psi_2$. Then since $n_2(\rho) = n_2(\psi_2) = 2$, it follows that $G_0 = G_1 \simeq \mathbb{Z}_2^\times/(1 + 2^2\mathbb{Z}_2) \simeq \mathbb{Z}/2\mathbb{Z}$ and $G_2 = 1$. □

(∗∗) Let $K/\mathbb{Q}_2$ be the extension cut out by the ρ of Lemma 3, and Δ its different. Then by the Führerdiskriminantenproduktformel, we have $v_2(\Delta) = 1$, where v_2 is the valuation of K normalized by $v_2(2) = 1$.

Suppose there was a ρ as in the Theorem. Assume $\mathrm{Im}(\rho)$ is non-solvable. Let K be the corresponding field to kernel of ρ. Let $n := [K : \mathbb{Q}]$, and $d_K^{1/n}$ denote the root discriminant of K.

If 3^m divides the order of G, then by §251-253 of [1], the projective image $\widetilde{G}$ of G in $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ is isomorphic to either $\mathrm{PGL}_2(\mathbb{F}_{3^m})$ or $\mathrm{PSL}_2(\mathbb{F}_{3^m})$. Thus we have $n = |G| \geq |\,\mathrm{PSL}_2(\mathbb{F}_{3^m})|$. Note that we have $m \geq 2$ because $\widetilde{G}$ is solvable if $m = 1$.

From Thm. 3 in [4] and Lemma 2,

$$\begin{aligned} |d_K|^{1/n} &\leq 3^{2+\frac{1}{6}-\frac{1}{3^m}} \cdot 2 \\ &\leq \begin{cases} 19.1329 & \text{if } m = 2 \\ 21.6169 & \text{if } m \geq 3. \end{cases} \end{aligned}$$

Then from [5], we have

$$|d_K|^{1/n} > \begin{cases} 19.567 & \text{if } n \geq 360 = |\,\mathrm{PSL}_2(\mathbb{F}_9)|, \\ 22.021 & \text{if } n \geq 9828 = |\,\mathrm{PSL}_2(\mathbb{F}_{27})|. \end{cases}$$

Comparing these two sets of inequalities, we obtain contradictions.

2. Even and solvable case

Assume ρ is even and $\mathrm{Im}(\rho)$ is solvable. According to §§19–21, of [7], a maximal irreducible solvable subgroup $\mathbb{G}$ of $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ has one of the following structures: (i) Imprimitive case: $\mathbb{G}$ is isomorphic to the wreath product $\overline{\mathbb{F}}_p^\times \wr (\mathbb{Z}/2\mathbb{Z})$, or (ii) Primitive case: $\mathbb{G}/\overline{\mathbb{F}}_p^\times$ is isomorphic to the symmetric group S_4. We remark that, 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 that the field K cut out by ρ is totally real or CM.

Now we show that there exists no such extension K. Let $G := \mathrm{Im}(\rho)$ and $\overline{G}$ its image in $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. If either G is of type (i) or G is of type (ii) and $\overline{G}$ is a 2-group, then K contains a non-trivial abelian extension of degree prime to 3 over a real quadratic field F. Since K is unramified outside $\{2, 3\}$ and its conductor (or, exactly speaking, the conductor of ρ) at 2 is 2^2, F is the field $\mathbb{Q}(\sqrt{3})$. Then K/F is unramified at 2 since it has ramification index 2 at the prime 2 (Lemma 3). Since any ray class group of F of 3-power conductor has 3-power order, there are no non-trivial abelian extension of F which are unramified outside 3 and of degree prime to 3.

Suppose now that G is of type (ii) and $\overline{G}$ is isomorphic to S_4 or A_4. By [2], there are three S_4-extensions (resp. one A_4-extension) of $\mathbb{Q}$ which are unramified outside $\{2, 3\}$ and whose ramification index at 2 divides 2. However, each of these fields has 2-component of the root discriminat greater than 2, which contradicts $(**)$. □

References

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

[2] J. Jones, *Tables of number fields with prescribed ramification*, http://math.la.asu.edu/~jj/

[3] C. Khare, *On Serre's modularity conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals unramified outside p*, preprint

[4] H. Moon and Y. Taguchi, *Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations*, Documenta Math. Extra Volume: Kazuya Kato's Fiftieth Birthday (2003), 641--654

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

[6] 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

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

[8] 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 33, Fukuoka 812-8581, Japan
E-mail address: moon@math.kyushu-u.ac.jp

Current address: Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu 702-701, Korea
E-mail address: hsmoon@knu.ac.kr