Existence of Nonelliptic mod $\ell$ Galois Representations for Every $\ell > 5$

Luis Dieulefait

**CONTENTS**

1. Examples for Every $\ell > 7$
2. The Case $\ell = 7$

References

For $\ell = 3$ and $5$ it is known that every odd, irreducible, two-dimensional representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathbb{F}_\ell$ and determinant equal to the cyclotomic character must “come from” the $\ell$-torsion points of an elliptic curve defined over $\mathbb{Q}$. We prove, by giving concrete counter-examples, that this result is false for every prime $\ell > 5$.

1. EXAMPLES FOR EVERY $\ell > 7$

In [Shepherd-Barron and Taylor 97] it is shown that for $\ell = 3$ and $5$ every odd, irreducible, two-dimensional Galois representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathbb{F}_\ell$ and determinant the cyclotomic character is “elliptic,” i.e., it agrees with the representation given by the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\ell$-torsion points of an elliptic curve defined over $\mathbb{Q}$.

In this note we will show that this is false for every prime $\ell > 5$, i.e., that for every such prime there exists a Galois representation verifying the above properties but “nonelliptic,” i.e., not corresponding to the action of Galois on torsion points of any elliptic curve defined over $\mathbb{Q}$. We will show this by giving concrete examples of nonelliptic representations. For any prime $\ell > 7$, the example will be constructed starting from a weight-4 classical modular form, corresponding to a rigid Calabi-Yau threefold. The case of $\ell = 7$ will be treated separately in the next section.

We consider the cuspidal modular form $f \in S_4(25)$ (i.e., of weight $4$, level $25$, and trivial nebentypus) which has all eigenvalues in $\mathbb{Z}$ and whose attached Galois representations $\rho_{f,\ell}$ agree (see [Schoen 86, Yui 03]) with the Galois representations on the third étale cohomology groups of the Schoen rigid Calabi-Yau threefold. This threefold is obtained (after resolving the singularities) from

$$Y : X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 - 5X_0X_1X_2X_3X_4 = 0 \subseteq \mathbb{P}^4.$$
We list the first eigenvalues $a_p$ of $f$ (for $p \neq 5$):
\[
a_2 = 1; a_3 = 7; a_7 = 6; a_{11} = -43.
\]

From now on we will assume $\ell > 5$. For any prime $\ell$ let $\overline{\rho}_\ell := \overline{\rho}_{f,\ell}$ be the residual $\ell$-representation corresponding to $\rho_{f,\ell}$: it is unramified outside $5\ell$, its conductor or Serre's level (defined as the prime-to-$\ell$ part of its Artin conductor) divides $25$, and it has values in $\mathbb{F}_\ell$ and determinant $\chi^3$ ($\chi$ denotes the mod $\ell$ cyclotomic character). For every prime $p \nmid 5\ell$, we have $\text{trace}(\rho_\ell(\text{Frob } p)) \equiv a_p \pmod{\ell}$.

Let us show that for any $\ell > 5$, $\overline{\rho}_\ell$ is (absolutely) irreducible. As explained in [Dieulefait and Manoharmayum 03], since $\rho_\ell$ is attached to a rigid Calabi-Yau threefold, as long as $\ell > 4$ and $\ell$ is not $5$ (so that $\ell$ is a prime of good reduction), if $\overline{\rho}_\ell$ is reducible it must hold that
\[
\overline{\rho}_\ell \cong \epsilon \oplus \epsilon^{-1} \chi^3,
\]
where $\epsilon$ is a character unramified outside $5$ (the same description follows also from the fact that the representation is attached to a weight-4 cuspform). Since
\[
\text{cond}(\epsilon)\text{cond}(\epsilon^{-1}) = \text{cond}(\epsilon^2) = \text{cond}(\overline{\rho}_\ell) \mid 25,
\]
we have $\text{cond}(\epsilon) \mid 5$. In particular, if $\ell \neq 11$, we have $\epsilon(11) = 1$, therefore
\[
-43 = a_{11} \equiv \text{trace}(\overline{\rho}_\ell(\text{Frob } 11)) \equiv 1 + 11^3 \pmod{\ell}.
\]

But no prime $\ell > 5, \ell \neq 11$ divides $11^3 + 1 + 43$, and this proves irreducibility of $\overline{\rho}_\ell$ for every $\ell > 5$ except $11$.

To show that $\overline{\rho}_{11}$ is also irreducible, observe that since it is an odd representation, irreducibility and absolute irreducibility are equivalent for it. Thus, it is enough to find a prime $p \nmid 55$ such that the reduction modulo $11$ of the characteristic polynomial $x^3 - a_p x + p^3$ is irreducible. Equivalently, we need the discriminant $\Delta_p = a_p^2 - 4p^3$ to be a nonsquare modulo $11$. For $p = 2$ we have $\Delta_2 = -31 \equiv 2 \pmod{11}$, which is a nonsquare, and this gives the irreducibility of $\overline{\rho}_{11}$.

We define $\overline{\rho}'_\ell := \overline{\rho}_\ell \otimes \chi^{(\ell-3)/2}$, for any $\ell > 5$. It is also irreducible and odd, but the advantage is that its determinant is $\chi$.

We ask the following: is there any elliptic curve $E$ defined over $\mathbb{Q}$ such that the Galois representation $\overline{\rho}_{E,\ell}$ corresponding to its $\ell$-torsion points gives $\overline{\rho}'_\ell$ for some $\ell$?

Let us show that this cannot happen for any $\ell > 7$.

Suppose the opposite. Then, since $\overline{\rho}'_\ell$ is unramified at $2$ and $\ell = 1 \pmod{\ell}$, if $\overline{\rho}'_\ell \cong \overline{\rho}_{E,\ell}$ it is known (see [Carayol 89] and [Ribet 91]) that $\rho_{E,\ell}$, the $\ell$-adic representation corresponding to the $\ell$-adic Tate module of $E$,

must be unramified or semistable at $2$. If it is unramified at $2$, let us call $c_2$ the trace of $\rho_{E,\ell}(\text{Frob } 2)$. Since $\abs{c_2} \leq 2\sqrt{2}$, it should be $c_2 = 0, \pm 1$ or $\pm 2$.

Comparing the traces of $\overline{\rho}'_\ell$ and $\overline{\rho}_{E,\ell}$ at $\text{Frob } 2$ we obtain
\[
a_2 2^{(\ell-3)/2} \equiv 0, \pm 1, \pm 2 \pmod{\ell}.
\]

If $\rho_{E,\ell}$ is semistable at $2$, since $\overline{\rho}'_\ell$ is modular and $\rho_{E,\ell}$ is also modular (because all elliptic curves over $\mathbb{Q}$ are modular) then we obtain from $\overline{\rho}'_\ell \cong \rho_{E,\ell}$ by level raising (see [Ghate 02])
\[
\text{trace}(\overline{\rho}'_\ell(\text{Frob } 2)) \equiv \pm(2+1) \equiv \pm 3 \pmod{\ell}.
\]

Thus
\[
a_2 2^{(\ell-3)/2} \equiv \pm 3 \pmod{\ell}.
\]

We conclude from (1–1) and (1–2) that if for some $\ell > 5$, $\overline{\rho}'_\ell$ comes from an elliptic curve, it must hold that (recall that $a_2 = 1$)
\[
2^{(\ell-3)/2} \equiv 0, \pm 1, \pm 2, \pm 3 \pmod{\ell}.
\]

Thus $2^{\ell-3} \equiv 1, 4, 9 \pmod{\ell}$.

Applying Fermat’s little theorem, this gives $2^{-2} \equiv 1, 4, 9 \pmod{\ell}$, and this is false for every prime $\ell > 7$.

Remark 1.1. It is natural that our result does not apply to $\ell = 7$ since independently of the value of $a_2$, we would never get a contradiction for $\ell = 7$ because $0, \pm 1, \pm 2, \pm 3$ cover all possible values modulo $7$.

We conclude that for any prime $\ell > 7$ the representation $\overline{\rho}'_\ell$ is nonelliptic.

2. THE CASE $\ell = 7$

We will consider the example of a mod $7$ representation attached to a weight-2 cuspform $f$ such that the field $\mathbb{Q}_f$ generated by its eigenvalues is not $\mathbb{Q}$, there is a prime in $\mathbb{Q}_f$ dividing 7 of residue class degree 1, and the representation is irreducible but it cannot come from any elliptic curve for the following simple reason: the conductor of the representation is too large, compared with the universal bounds for conductors (see [Silverman 94]) of elliptic curves defined over $\mathbb{Q}$. Recall that the $p$-part of the conductor of any elliptic curve over $\mathbb{Q}$ must divide $256$ if $p = 2$, $243$ if $p = 3$, and $p^2$ if $p > 3$.

Concretely, we take the following example: let $f \in S_2(512)$ be the cuspform with $\mathbb{Q}_f = \mathbb{Q}(\sqrt{2})$ and eigenvalues.
$a_3 = \sqrt{2}$, \quad $a_5 = -2\sqrt{2}$,

$a_7 = -4$, \quad $a_{11} = \sqrt{2}$,

$a_{13} = 2\sqrt{2}$, $\ldots$, \quad $a_{29} = 6\sqrt{2}$

(we obtain these values from the web site [Stein 00]).

The corresponding mod 7 representation $\overline{\rho}_7$ has values in $\mathbb{F}_7$ and it is irreducible because the discriminant $\Delta_{29}$ is a nonsquare modulo 7.

The conductor of any of the representations $\rho_\lambda := \rho_{f,\lambda}$ in the family attached to $f$ ($\lambda \nmid 2$), is equal to 512, the level of $f$. Therefore, (see [Carayol 89], page 789) the conductor of $\overline{\rho}_7$ is also 512.

Since the 2-part of the conductor of any elliptic curve is at most 256, this implies that $\overline{\rho}_7$ cannot correspond to any elliptic curve. Thus $\overline{\rho}_7$, whose determinant is the cyclotomic character, is nonelliptic.

Remark 2.1. We have computed another example, using [Stein 00], with $f \in S_2(2560)$, with the same properties: $\overline{\rho}_7$ irreducible, valued in $\mathbb{F}_7$, but nonelliptic for the same reason. The field $\mathbb{Q}_f$ corresponds to a root of the polynomial $x^4 - 316x^2 + 8836$ (in [Stein 00] one can obtain a list of eigenvalues of $f$); it is a quadratic extension of $\mathbb{Q}(\sqrt{7})$ in which $\sqrt{7}$ splits.

Remark 2.2. Observe that from the “bounds for conductors” in [Serre 87], since $7 \not \equiv \pm 1 (\mod 9)$ and $7 \not \equiv \pm 1$ (mod $p$) for any $p > 3$, every odd, irreducible Galois representation valued in $\mathbb{F}_7$ must have the $p$-part of its conductor bounded with the same bound holding for elliptic curves, for any $p > 2$. Thus, it is only by searching for representations with “large 2-part of the conductor” that one can obtain a representation valued in $\mathbb{F}_7$ not satisfying the universal bounds for conductors of elliptic curves.

On the other hand, since $7 \equiv -1 (\mod 8)$, the bound for the 2-part of conductors given in [Serre 87] does not apply to the case of representations with values in $\mathbb{F}_7$.

REFERENCES


