A method to prove that a modular Galois representation has large image

Nicolas Mascot*

May 30, 2022

Abstract

Let ρ be a mod ℓ Galois representation attached to a newform f. Explicit methods such as [Ann13] are sometimes able to determine the image of ρ, or even [Mas22] the number field cut out by ρ, provided that ℓ and the level N of f are small enough; however these methods are not amenable to the case where ℓ or N are large. The purpose of this short note is to establish a sufficient condition for the image of ρ to be large and which remains easy to test for moderately large ℓ and N.

Acknowledgements

We express our thanks to B. S. Banwait for motivating us to write this short note by asking about the image of the representation discussed in Example 10 below.

Keywords: Modular form, Galois representation, Large image.

Let $f = q + \sum_{n \geqslant 2} a_n(f) q^n$ be a newform of weight $k \in \mathbb{N}$, level $N \in \mathbb{N}$, and nebentypus $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$. Let λ be a prime of residual degree 1 of the field K_f spanned by the Hecke eigenvalues of f, let $\ell \in \mathbb{N}$ be the prime below λ, and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$ be the Galois representation attached to f mod λ. Since ρ also arises from a form of level prime to ℓ, we assume that $\ell \nmid N$ from now on.

2020 *Mathematics subject classification:* 11F80, 11F11.

*Trinity College Dublin, mascotn@tcd.ie

Definition 1. Let $p \in \mathbb{N}$ be a prime dividing N. We say that $f \bmod \lambda$ is *old at p* if ρ also arises from a form of level dividing N/p.

Equivalently, $f \bmod \lambda$ is old at p if it is congruent to a newform f' whose level divides N/p; in particular, ε must actually arise from a character mod N/p. In fact, [Edi92, 3.4, 7.2] even show that this is equivalent to the existence of an integer $i \in \mathbb{N}$, of a newform $q + \sum_{n \geqslant 2} b_n q^n$ of weight k' satisfying $2 \leqslant k' \leqslant \ell + 2$, level dividing N/p, and same nebentypus ε as f, and of a prime λ' above ℓ of the field spanned by the b_n such that

$$a_n(f) \bmod \lambda = n^i b_n \bmod \lambda' \tag{2}$$

for all n coprime to ℓN. Therefore, given f, λ, and p, it is possible (and usually not too difficult) to explicitly determine whether $f \bmod \lambda$ is old at p; see Examples 10 and 12 below for concrete cases.

Definition 3. We say that ρ has *large* image if its image contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.

The purpose of this note is to establish an efficient one-way criterion for ρ to have large image. The key argument is established by the following Lemma.

Lemma 4. *Suppose that ρ is irreducible, and that there exists a prime $p \mid N$ such that $p^2 \nmid N$ and that the p-part of ε is trivial. Then either*

- $f \bmod \lambda$ *is old at p, or*
- ρ *is ramified but not wildly ramified at p, and the image by ρ of the inertia at p is cyclic of order ℓ.*

Proof. As ρ is irreducible, Serre's conjecture (now a theorem thanks to [KW09]) assigns to ρ a level $N(\rho) \mid N$ and a weight $k(\rho) \leqslant \ell^2 - 1$ such that ρ also arises from an newform f_ρ of level $N(\rho)$ and weight $k(\rho)$. While $k(\rho)$ is defined in terms of the action of the inertia at ℓ, $N(\rho)$ is defined in terms of the action of inertia at primes $r \neq \ell$, viz

$$N(\rho) = \prod_{r \neq \ell} r^{n_r}, \quad n_r = \operatorname{codim} V^{I_r} + \mathrm{Swan}_r,$$

where $V \simeq \mathbb{F}_\ell^2$ is the representation space of ρ, V^{I_r} is the subspace of V fixed by the inertia I_r at r, and

$$\mathrm{Swan}_r = \sum_{i=1}^{+\infty} \frac{1}{[I_r : I_r^{(i)}]} \operatorname{codim} V^{I_r^{(i)}}$$

is a non-negative integer defined in terms of the action on V of the higher inertia groups $I_r^{(i)}$ at q.

Therefore, if $f \bmod \lambda$ is *not* old at p, then $p \mid N(\rho)$. As $N(\rho) \mid N$, it follows that

$$1 = n_p = \operatorname{codim} V^{I_p} + \mathrm{Swan}_p \, .$$

In particular, $\operatorname{codim} V^{I_p} \leqslant 1$; but we cannot have $\operatorname{codim} V^{I_p} = 0$ lest I_p, and a fortiori the $I_p^{(i)}$, act trivially on V, which would also force $\mathrm{Swan}_p = 0$. Therefore we must have $\operatorname{codim} V^{I_p} = 1$ and $\mathrm{Swan}_p = 0$, meaning that up to conjugacy

$$\rho_{|I_p} = \begin{pmatrix} 1 & \xi \\ 0 & \chi \end{pmatrix}$$

for some morphism $\chi : I_p \longmapsto \mathbb{F}_\ell^\times$ and cocycle $\xi : I_p \longmapsto \mathbb{F}_\ell$, and that ρ is ramified, but only moderately ramified, at p. More specifically, χ is the restriction to I_p of $\det \rho$, and is therefore trivial: Indeed, $\det \rho$ is the product of ε, which is trivial on I_p by our assumption that its p-part is trivial, and of the $(k-1)$-th power of the mod ℓ cyclotomic character χ_ℓ (the one that expresses the Galois action on the ℓ-th roots of unity), which is also trivial on I_p.

We deduce that actually

$$\rho_{|I_p} = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$$

for some morphism $\xi : I_p \longmapsto \mathbb{F}_\ell$, which cannot be trivial since $\operatorname{codim} V^{I_p} \neq 0$. □

Theorem 5. *Suppose that there exists a prime $p \mid N$ such that $p^2 \nmid N$ and that the p-part of ε is trivial, and another prime $r \nmid \ell N$ such that the polynomial $x^2 - a_r(f)x + r^{k-1}\varepsilon(r) \bmod \lambda \in \mathbb{F}_\ell[x]$ is irreducible over $\mathbb{F}_\ell$. Then either*

- *$f \bmod \lambda$ is old at p, or*
- *ρ has large image.*

Proof. As the image of the Frobenius at r has irreducible characteristic polynomial $x^2 - a_r(f)x + r^{k-1}\varepsilon(v) \bmod \lambda \in \mathbb{F}_\ell[x]$, ρ must be irreducible. Therefore, unless $f \bmod \lambda$ is old at p, Lemma 4 shows that that $\rho(I_p)$ is cyclic of order ℓ, so ℓ divides the order of $\operatorname{Im} \rho$. Proposition 15 of [Ser72] then shows that the image of ρ is either large or contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$, but the latter case is incompatible with ρ being irreducible. □

Remark 6. Let $G \leqslant \mathrm{GL}_2(\mathbb{F}_\ell)$ be a subgroup containing $\mathrm{SL}_2(\mathbb{F}_\ell)$. The proportion of elements of G whose characteristic polynomial is irreducible only depends on ℓ; more specifically, it is $\frac{1}{3}$ if $\ell = 2$ and $\frac{1}{2}\frac{\ell-1}{\ell+1}$ if $\ell \geqslant 3$, which is always $\geqslant \frac{1}{4}$ and close to $\frac{1}{2}$ for large ℓ.

Therefore, if ρ indeed has large image, Cebotarev ensures that it will not be difficult to find a prime $r \nmid \ell N$ such that the characteristic polynomial of $\rho(\mathrm{Frob}_r)$ is irreducible. Conversely, it is reasonable to suspect ρ is reducible if no such prime r is found after a few attempts; and if desired this suspicion may be rigorously confirmed by [Ann13, Algorithm 7.2.4].

Remark 7. Suppose one wishes to search for pairs (f, λ) with ε trivial and such that ρ has "exotic" image, meaning neither large nor contained in a Borel subgroup. One would presumably go through newforms f of increasing level N, and not be interested in representations ρ already encountered in lower level. Theorem 5 then shows that one can skip levels N having at least one non-repeated prime factor.

Remark 8. Suppose that the assumptions of Theorem 5 are satisfied, and that $f \bmod \lambda$ is not old at p, so that ρ has large image. Let k (resp. K) be the number field of degree $\ell + 1$ (resp. $\ell^2 - 1$) corresponding by ρ to the stabiliser of a point in $\mathbb{P}^1(\mathbb{F}_\ell)$ (resp. a nonzero vector in $\mathbb{F}_\ell^2$), and suppose N or ℓ are too large for methods to determine k or K such as [Mas22] to apply, but that we hope to find a model for k or K in a database such as [LMFDB].

Recall that whenever $T(x) \in \mathbb{Q}[x]$ is irreducible of degree d and $r \in \mathbb{N}$ is an at-most-tamely ramified prime in the root field $F \simeq \mathbb{Q}[x]/T(x)$ of $T(x)$, the exponent of r in the discriminant of F is $d - \omega_r$, where ω_r is the number of orbits of roots of $T(x)$ under the action of inertia I_r. Lemma 4 therefore also implies that the exponent of p in $\operatorname{disc} k$ is $\ell + 1 - 2 = \ell - 1$, and it is $\ell^2 - 1 - 2(\ell - 1) = (\ell - 1)^2$ in $\operatorname{disc} K$. In particular, the primes above p do not ramify in the extension K/k; this could already be seen in the proof of Lemma 4, which shows that $\rho(I_p)$ injects into $\mathrm{PGL}_2(\mathbb{F}_\ell)$.

Besides, when $\ell \neq 2$, the fact that ρ is odd implies that the respective signatures of k and K are $(2, \frac{\ell-1}{2})$ and $(\ell - 1, \frac{\ell(\ell-1)}{2})$. All this information, as well as the equivalence

$$\begin{aligned} a_r(f) = 0 \bmod \lambda &\iff \operatorname{Tr} \rho(\mathrm{Frob}_r) = 0 \\ &\iff \rho(\mathrm{Frob}_r) \text{ has order exactly 2 in } \mathrm{PGL}_2(\mathbb{F}_\ell) \\ &\iff T_k(x) \text{ only has factors of degree 1 or 2 over } \mathbb{F}_\ell, \\ &\qquad \text{with at least one factor of degree 2} \end{aligned}$$

whenever $T_k(x) \in \mathbb{Z}[x]$ is an irreducible polynomial defining k and $r \in \mathbb{N}$ is a prime not dividing $\operatorname{disc} T_k$, can help narrow down the search for k and K in a number field database.

Finally, if a candidate for k of K has been isolated, this identification can sometimes be proved rigorously by methods relying on Serre's conjecture, such as [Mas18, 4.2].

Furthermore, our explicit knowledge of $\det \rho$ makes it easy to explicitly determine the image of ρ when it is large:

Corollary 9. *Suppose that there exists a prime $p \mid N$ such that $p^2 \nmid N$ and that the p-part of ε is trivial, another prime $r \nmid \ell N$ such that $x^2 - a_r(f)x + r^{k-1}\varepsilon(r)$ is irreducible mod λ, and that f mod λ is not old at p. Let $\Delta \leqslant \mathbb{F}_\ell^\times$ be the subgroup spanned by the values of ε mod λ and by the $k-1$-th powers in $\mathbb{F}_\ell^\times$. Then the image of ρ is*

$$\operatorname{Im} \rho = \{g \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \det g \in \Delta\} \leqslant \mathrm{GL}_2(\mathbb{F}_\ell).$$

In particular, if $\ell \neq 2$, then the image of the projective representation attached to ρ is $\mathrm{PSL}_2(\mathbb{F}_\ell)$ iff. k is odd and the values assumed by ε mod λ are squares in $\mathbb{F}_\ell^\times$; else it is $\mathrm{PGL}_2(\mathbb{F}_\ell)$. (If $\ell = 2$, then either way it is $\mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2)$, and $\operatorname{Im} \rho = \mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2)$.)

Proof. By Theorem 5, $\operatorname{Im} \rho$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$, whence

$$\operatorname{Im} \rho = \{g \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \det g \in \operatorname{Im} \det \rho\},$$

so it remains to prove that $\Delta = \operatorname{Im} \det \rho$.

We have $\det \rho = \chi_\ell^{k-1}\varepsilon$, where χ_ℓ is the mod-ℓ cyclotomic character. But for $r \nmid \ell N$ prime, $\chi_\ell(\mathrm{Frob}_r) = r$ mod ℓ only depends on r mod ℓ, whereas $\varepsilon(\mathrm{Frob}_r) = \varepsilon(r)$ only depends on r mod N. As ℓ and N are coprime by assumption, the conclusion follows by Chinese remainders. □

Example 10. Let $f = q - 2q^4 + (3 + \sqrt{2})q^5 + O(q^6)$ be the newform of [LMFDB] label 9099.2.a.g. Its level is $N = 9099 = 3^3 \cdot p$ where $p = 337$ is prime, its weight is $k = 2$, its nebentypus is trivial, and its coefficient field is $K_f = \mathbb{Q}(\sqrt{2})$. Let λ be the prime $(7, \sqrt{2} - 3)$ of K_f, and let ρ be the corresponding representation.

Already for $r = 2$ we find that

$$x^2 - a_r(f)x + r = x^2 + 2$$

is irreducible over $\mathbb{F}_7$, which proves that ρ is irreducible.

If f mod λ were old at p, there would exist a newform $f' = q + \sum_{n\geqslant 2} b_n q^n$ of level $\Gamma_0(3^v)$, $v \leqslant 3$ and weight $2 \leqslant k' \leqslant 9$, and an integer i such that (2) holds. As the [LMFDB] informs us that $a_r(f) \equiv 0 \bmod \lambda$ for $r \in \{2, 11, 31, 73\}$, we run a computer search for such forms f' also satisfying that the b_r have norm divisible by 7 for all $r \in \{2, 11, 31, 73\}$, which takes a couple of minutes and results in only possible form f'. However, this f' also has $b_5 \equiv 0 \bmod 7$ whereas $a_5(f) \not\equiv 0 \bmod \lambda$, which proves that f is not old at p.

As $k-1 = 1$, we conclude by Corollary 9 that the representation attached to f mod λ is surjective. This answers a question of B. S. Banwait's, and which was our motivation for writing this short note.

The observations made in Remark 8 show that in this example, the field k is a number field of signature $(2, 3)$, unramified away form $\{3, 7, 337\}$ and certainly ramified at 7 (by $\det \rho$) and tamely ramified 337, the exponent of 337 in $\operatorname{disc} k$ being 6; and the Galois group of the Galois closure of $k/\mathbb{Q}$ is $\mathrm{PGL}_2(\mathbb{F}_7)$. This information is more than enough to determine that this field is not present in the [LMFDB] as of May 2022.

Remark 11. On the other hand, f is old at p modulo the conjugate prime $\lambda' = (7, \sqrt{2}+3)$, as f mod λ' is congruent to the newform of weight 2, level 27, and trivial nebentypus. In fact, this form of weight 2 happens to have CM, and accordingly the image of the projective representation attached to f mod λ' is dihedral according to [Ban21, Table 2].

Example 12. This time, let $f = q + \sum_{n\geqslant 2} a_n(f) q^n$ be the newform of [LMFDB] label 71.3.b.a. It has prime level $N = 71$, weight $k = 3$, quadratic nebentypus $\varepsilon = \left(\frac{\cdot}{71}\right)$, and coefficient field $K_f = \mathbb{Q}(\beta)$ where $\beta^4 + 108\beta^2 - 40\beta + 2825 = 0$. Let us take for instance $\lambda = (41, \beta - 11)$, a prime of K_f of degree 1 above $\ell = 41$, and let ρ be the corresponding mod ℓ Galois representation.

First of all, we check that for $r = 2$, the characteristic polynomial

$$x^2 - a_r(f)x + r^{k-1}\varepsilon(r) \bmod \lambda = x^2 - 16x + 4$$

is irreducible over $\mathbb{F}_\ell$, so ρ is irreducible.

Let us thus apply Theorem 5 with $p = N$. If f mod λ were old at p, there would exist a newform $f' = q + \sum_{n\geqslant 2} b_n q^n$ of level 1 and weight at most $\ell + 2 = 43$ and an integer i such that (2) holds. However, a computer search reveals in less than one second that $a_{101}(f) = 0 \bmod \lambda$ whereas all these forms f' have that the norm of b_{101} is not a multiple of ℓ. Therefore f mod λ is not old at p, so ρ has large image.

In fact, as $k-1=2$ and as the values ± 1 of ε are squares mod λ, Corollary 9 shows that the image of ρ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_{41})$ formed of matrices whose determinant is a square mod 41, so the corresponding projective representation has image $\mathrm{PSL}_2(\mathbb{F}_{41})$. In particular, in this example, the Galois closure of $k/\mathbb{Q}$ has Galois group the simple group $\mathrm{PSL}_2(\mathbb{F}_{41})$, and ramifies exactly at ℓ and at p, tamely at p, and probably wildly at ℓ.

References

[Ann13] Samuele Anni, **Images of Galois representations**. PhD thesis, `https://tel.archives-ouvertes.fr/tel-00903800`. General Mathematics. Université Sciences et Technologies - Bordeaux I; Universiteit Leiden, 2013. NNT : 2013BOR14869. tel-00903800.

[Ban21] Banwait, Barinder Singh, **Examples of abelian surfaces failing the local–global principle for isogenies**. Res. number theory 7, 55 (2021). `https://doi.org/10.1007/s40993-021-00283-9`.

[Edi92] Edixhoven, Bas, **The weight in Serre's conjectures on modular forms**. Invent. Math. 109 (1992), no 3, 563–594.

[KW09] Khare, Chandrashekhar; Wintenberger, Jean-Pierre, **Serre's modularity conjecture (I and II)**. Invent. Mathemat. 178 (3), 485–504 and 505–586.

[LMFDB] The LMFDB Collaboration, **The L-functions and Modular Forms Database**. `http://www.lmfdb.org`

[Mas18] Mascot, Nicolas, **Companion forms and explicit computation of PGL_2-number fields with very little ramification**, Journal of Algebra, Vol. 509, 2018, pp. 476–506, ISSN 0021-8693, `https://doi.org/10.1016/j.jalgebra.2017.10.027`

[Mas22] Mascot, Nicolas, **Moduli-friendly Eisenstein series over the p-adics and the computation of modular Galois representations**. To appear in Res. number theory.

[Ser72] Serre, Jean-Pierre, **Propriétés galoisiennes des points d'ordre fini des courbes elliptiques**. Invent Math 15, 259–331 (1971). `https://doi.org/10.1007/BF01405086`