Companion forms and explicit computation of PGL_2 number fields with very little ramification

Nicolas Mascot*

University of Warwick, Coventry CV4 7AL, UK.

September 10, 2017

Abstract

In previous works [Mas13] and [Mas16], we described algorithms to compute the number field cut out by the mod ℓ representation attached to a modular form of level $N = 1$. In this article, we explain how these algorithms can be generalised to forms of higher level N.

As an application, we compute the Galois representations attached to a few forms which are supersingular or admit a companion mod ℓ with $\ell = 13$ and $\ell = 41$, and we obtain previously unknown number fields of degree $\ell + 1$ whose Galois closure has Galois group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and a root discriminant that is so small that it beats records for such number fields.

Finally, we give a formula to predict the discriminant of the fields obtained by this method, and we use it to find other interesting examples, which are unfortunately out of our computational reach.

Acknowledgements

The author thanks Noam Elkies, Benedict Gross and David Roberts for their suggestion to compute Galois representations attached to forms admitting a companion mod ℓ, David Roberts for providing the author with a few examples of such forms that were especially amenable to computation, and Ariel Pacetti and Aurel Page for stimulating discussions about the arithmetic of the fields cut out by mod ℓ Galois representations.

The computer algebra packages used for the computations presented in this paper were [SAGE], [Pari/GP] and [Magma], and we were able to evaluate root discriminants of Galois closures of wildly ramified fields thanks to John Jones's and David Roberts's page [JR]. The computations were carried out on the Warwick mathematics institute computer cluster provided by the EPSRC Programme Grant EP/K034383/1 "LMF: L-Functions and Modular Forms".

This research was supported by the aforementioned grant.

Keywords: Galois representation, modular form, number field tabulation, ramification, discriminant, inverse Galois problem

2010 *Mathematics subject classification:* 11F80, 11R21, 11Y40, 11F11, 11F30.

*n.a.v.mascot@warwick.ac.uk

1 Introduction

Let $f = \sum_{n\geqslant 1} a_n q^n$ be a classical cusp form of level $N \geqslant 1$, weight $k \geqslant 2$ and nebentypus ε. We suppose that f is an *newform*, that is to say that f is a new eigenform which is normalised so that $a_1 = 1$. The *Hecke field* of f is the number field generated by the coefficients a_n; it also contains the values of ε. For all finite primes $\mathfrak{l}$ of this field, there exists a unique (up to equivalence) semisimple mod $\mathfrak{l}$ Galois representation

$$\rho_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}),$$

which sends any Frobenius element at $p \nmid \ell N$ to a matrix of characteristic polynomial

$$T^2 - a_p T + p^{k-1}\varepsilon(p) \in \mathbb{F}_\mathfrak{l}[T]$$

where $\mathbb{F}_\mathfrak{l}$ is the residue field of $\mathfrak{l}$, $\ell \in \mathbb{N}$ is the prime below $\mathfrak{l}$, and the coefficients of the characteristic polynomial are considered mod $\mathfrak{l}$.

Let L be the field *cut out* by $\rho_{f,\mathfrak{l}}$, that is to say the unique number field that fits in the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_{f,\mathfrak{l}}} & \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}). \\ \downarrow & \nearrow & \\ \mathrm{Gal}(L/\mathbb{Q}) & & \end{array}$$

The ramification properties of L are well-understood in terms of f and $\mathfrak{l}$. In particular, L is unramified at p if $p \nmid \ell N$, and L is at most tamely ramified at every $p \neq \ell$ such that $p \parallel N$. At ℓ, the field L is usually wildly ramified, but not always. More precisely, it is tamely ramified when f admits a *companion form* mod ℓ in the sense of [Gro90], or when f is *supersingular* at $\mathfrak{l}$. Assuming for the clarity of the exposition that that $k < \ell$, the first case means that there exists another eigenform $g = \sum_{n\geqslant 1} b_n q^n$, of the same level as f but of weight $\ell + 1 - k$, such that

$$\sum_{n\geqslant 1} n a_n q^n \bmod \mathfrak{l} = \sum_{n\geqslant 1} n^k b_n q^n \bmod \mathfrak{l}'$$

for some prime $\mathfrak{l}'$ above ℓ in the Hecke field of g. The second case means that the ℓ-th Fourier coefficient a_ℓ of f is 0 mod $\mathfrak{l}$; in this case, there also exists another eigenform $g = \sum_{n\geqslant 1} b_n q^n$, of the same level as f but of weight $\ell + 3 - k$ this time, such that

$$\sum_{n\geqslant 1} n^2 a_n q^n \bmod \mathfrak{l} = \sum_{n\geqslant 1} n^k b_n q^n \bmod \mathfrak{l}'.$$

Therefore, Galois representations attached to such forms are a valuable source of number fields of Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$ or $\mathrm{PGL}_2(\mathbb{F}_\ell)$ whose ramification is extremely restricted, and that thus deserve a particular place in tables of number fields, provided of course that we are able to find them explicitly. This was pointed out to the author by David Roberts. A quantitative statement of this fact is achieved by theorem 6.1.2.

In previous works [Mas13] and [Mas16], we described algorithms to compute explicitly the number field cut out by the mod $\mathfrak{l}$ representation attached to a form of level $N = 1$. In this article, we show how these algorithms can be generalised

efficiently to forms of higher level N, provided for simplicity that ℓN is squarefree. We lose no generality by assuming that ℓ and N are coprime since every mod ℓ representation attached to a form of level ℓN is also attached to a form of level N; besides, the hypothesis that N is squarefree could probably be suppressed without great difficulty.

As an application, we compute the Galois representations attached to a few forms which admit a companion or are supersingular mod ℓ, and we obtain very lightly ramified number fields of degree $\ell+1$ that were, as far as the author knows, previously unknown, and whose Galois closure has Galois group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ and a particularly small root discriminant, thus beating the record for such number fields.

For the same reasons as in [Mas13], the output of this algorithm is not certified. We therefore explain how our certification method [Mas16] can be extended to the case of forms of higher level.

Finally, we establish formulas to predict the discriminant of the number fields cut out by such representations and we use these formulas to single out an interesting example, even though we are unable to compute the corresponding fields explicitly at the moment.

This article is organised as follows. First, in section 2, we derive formulas describing the action of the Atkin-Lehner operators on a space of modular forms of given level and weight, including on the old subspace and on the Eisenstein subspace. These formulas are needed for the generalisation of our modular Galois representation computation algorithm [Mas13], and we present this generalisation in section 3. In section 4, we explain how the output of this new algorithm may be certified thanks to a generalisation of the methods presented in [Mas16]. Finally, in section 5 we present the results of our computations, and we explain in section 6 what results can be obtained with our techniques in general.

Notation

The letter $\mathbb{N}$ denotes the set of positive integers; in particular, $0 \notin \mathbb{N}$. We let $G_\mathbb{Q}$ denote the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of the rationals, and we write $\mathrm{Frob}_p \in G_\mathbb{Q}$ for a Frobenius element at the prime $p \in \mathbb{N}$. Since all the Galois representations considered in this article are mod ℓ (as opposed to ℓ-adic), we will denote them by ρ (as opposed to $\overline{\rho}$). We will also frequently consider projective mod ℓ Galois representations, which we will denote by the letter π. This should not cause any confusion, as we will not consider any automorphic representation in this article.

We write $e(x)$ as a shorthand for $e^{2i\pi x}$.

Let ε be a Dirichlet character modulo $N \in \mathbb{N}$. We write

$$\mathfrak{g}(\varepsilon) = \sum_{x \bmod N} \varepsilon(x) e(x/N)$$

for the Gauss sum of ε. Given a factorisation $N = Q_1 \cdots Q_r$ of N into pairwise coprime factors Q_i, we will denote by $\varepsilon_{Q_1} \cdots \varepsilon_{Q_r}$ the corresponding decomposition of ε into characters of respective moduli Q_i.

We normalise the weight k action on functions on the upper half-plane as

$$f\big|_k \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right](\tau) = \frac{(ad-bc)^{k/2}}{(c\tau+d)^k} f\left(\frac{a\tau+b}{c\tau+d}\right).$$

This is an action of $\mathrm{PGL}_2^+(\mathbb{R})$.

For $k, N \in \mathbb{N}$ and ε a Dirichlet character mod N, we let $\mathcal{M}_k(N,\varepsilon)$ $\big($resp. $\mathcal{S}_k(N,\varepsilon)$, $\mathcal{E}_k(N,\varepsilon)\big)$ be the $\mathbb{C}$-vector space of modular forms (resp. cuspforms, Eisenstein series) of level N and nebentypus ε, and we let $\mathcal{N}_k(N,\varepsilon)$ be the finite set of newforms in $\mathcal{S}_k(N,\varepsilon)$.

When $N \mid N'$, we write $I_N^{N'}$ for the "identity" injection map from $\mathcal{M}_k(N,\varepsilon)$ to $\mathcal{M}_k(N',\varepsilon)$. Also, for $t \in \mathbb{N}$, we let B_t denote the operator $f(\tau) \mapsto f(t\tau)$, in other words

$$f\big|B_t = t^{-k/2} f\big|_k \left[\begin{smallmatrix} t & \\ & 1 \end{smallmatrix}\right]$$

for f of weight k.

Finally, we write $\langle d \rangle$ for the Hecke operator that acts as multiplication by $\varepsilon(d)$ on $\mathcal{M}_k(N,\varepsilon)$. In particular, $\langle d \rangle$ is the 0 operator if $\gcd(d,N) > 1$.

2 Explicit formulas for Atkin-Lehner operators acting on the whole space of modular forms

In order to compute mod ℓ Galois representations attached to eigenforms of level $N > 1$, we will need to be able to compute the action of the Atkin-Lehner operators on the space $\mathcal{M}_k\big(\Gamma_1(\ell N)\big)$, including its old part and its Eisenstein part. The purpose of this section is to establish explicit formulas for this.

2.1 Atkin-Lehner operators on the new part of the cuspidal subspace

The explicit action of the operators W_Q on newforms is well-understood. Indeed, we have the following formula (cf. [AL78, section 2] and [Asa76, theorem 2]):

Theorem 2.1.1. *Let $f = q + \sum_{n\geqslant 2} a_n q^n \in \mathcal{N}_k(N,\varepsilon)$ be a newform, and let $Q \parallel N$. For all positive integers $n \in \mathbb{N}$, write $n_Q = \gcd(n, Q^\infty)$ for the part of n that is supported by the primes dividing Q. Then there exists an algebraic number $\lambda_{f,Q} \in \mathbb{C}^*$ of absolute value 1 such that*

$$f\big|W_Q = \lambda_{f,Q} \sum_{n\geqslant 1} b_n q^n,$$

where $b_n = \varepsilon_{N/Q}(n_Q)\bar{\varepsilon}_Q(n/n_Q)\overline{a_{n_Q}} a_{n/n_Q}$ for all $n \in \mathbb{N}$.

Let $Q = \prod_{i=1}^r q_i^{e_i}$ be the complete factorisation of Q, and write $Q_i = q_i^{e_i}$. Then the following conditions are equivalent:

- *$a_Q \neq 0$,*
- *$a_{Q_i} \neq 0$ for all i,*
- *$a_{q_i} \neq 0$ for all i,*

and if these equivalent conditions are satisfied, then $\lambda_{f,Q}$ is given by

$$\lambda_{f,Q} = \prod_{i=1}^r \varepsilon_{Q_i}(Q/Q_i)\lambda'_{f,Q_i} \qquad \text{where} \qquad \lambda'_{f,Q_i} = Q_i^{k/2-1}\mathfrak{g}(\varepsilon_{Q_i})/a_{Q_i}.$$

Remark 2.1.2. Note that according to [Li75, theorem 3], $a_{q_i} = 0$ if and only if $e_i \geqslant 2$ and ε_{Q_i} is not a primitive character. When this case occurs, the only method to determine $\lambda_{f,Q}$ known to the author consists in evaluating numerically the functional equation defining $f\big|W_Q$ at a point; however this requires knowing a large number of coefficients a_n in order to get a reasonably accurate approximation of $\lambda_{f,Q}$.

2.2 Atkin-Lehner operators on the new part of the Eisenstein subspace

Fix an integer $k \geqslant 1$, let ψ and φ be *primitive* characters of respective moduli u and v, and let $M = uv$. If $k = 2$, also suppose that $M > 1$. Consider the eigenform for the whole Hecke algebra

$$E_k^{\psi,\varphi} = -\mathbb{1}_{u=1}\frac{B_{k,\varphi}}{k} + 2\sum_{n=1}^{+\infty}\sum_{0<m|n}\psi(n/m)\varphi(m)m^{k-1}q^n \in \mathcal{E}_k\big(\Gamma_1(M)\big),$$

where $B_{k,\varphi}$ is the k-th Bernoulli number attached to φ. If $k = 2$, also define $E_2(\tau) = 1 - 24\sum_{n=1}^{+\infty}\sigma_1(n)q^n$, which is *not* a modular form, and

$$E^{(M)}(\tau) = E_2(\tau) - ME_2(M\tau) \in \mathcal{E}_2\big(\Gamma_0(M)\big),$$

which is a modular form and also an eigenform for the Hecke operators T_p such that $p \nmid M$.

Let now ε by a character modulo N of the same parity as k. It is well-known (cf. for instance [DS05, theorems 4.5.2 and 4.6.2]) that for $k \neq 2$, the series $E_k^{\psi,\varphi}\big|B_t$ for (ψ, φ, t) such that $\psi\varphi = \varepsilon$ and $tuv \mid N$ form a basis of the Eisenstein space $\mathcal{E}_k(N, \varepsilon)$. The same remains true for $k = 2$ provided that ψ and φ are not both trivial, and that we include the series $E^{(t)}$ for $1 < t \mid N$ if ε is trivial.

The series $E_k^{\psi,\varphi}$ with $uv = N$, as well as $E^{(N)}$ if $k = 2$, thus play in $\mathcal{E}_k(N, \varepsilon)$ a rôle that is analogous to the newforms in $\mathcal{S}_k(N, \varepsilon)$. We now establish formulas describing the action of W_Q on them.

Theorem 2.2.1. *Let ψ and φ be as above, and let $Q \parallel N$. Write $R = N/Q$, $u = u_Q u_R$ and $v = v_Q v_R$, where $u_Q = \gcd(u, Q)$, $u_R = \gcd(u, R)$, and similarly for v_Q and v_R. Finally, let $\varepsilon = \psi\varphi$, a character modulo N. Then*

$$E_k^{\psi,\varphi}\big|W_Q = \frac{\varphi_Q(-1)(v_Q/u_Q)^{k/2}\mathfrak{g}(\psi_Q\varphi_R)}{\varepsilon_Q(v_R)\varepsilon_R(v_Q)\mathfrak{g}(\overline{\varphi})}E_k^{\bar{\varphi}_Q\psi_R,\bar{\psi}_Q\varphi_R}$$

where $\psi_Q\varphi_R$ is of course understood as a character modulo $u_Q v_R$.

The case of the series $E^{(N)}$ is simpler:

Theorem 2.2.2. *Let $Q \parallel N$, and let $R = N/Q$. Then $E^{(N)}\big|W_Q = E^{(R)} - E^{(Q)}$. In particular, $E^{(N)}\big|W_N = -E^{(N)}$.*

These formulas both follow from direct computations.

2.3 Atkin-Lehner operators on the old subspace

We now derive formulas for the action of W_Q on the old subspace of $\mathcal{M}_k(N,\varepsilon)$. This involves computing the action of W_Q (as an operator of level N) on forms which are new of level $M \mid N$ on the one hand, and deriving commutation relations between W_Q and B_t on the other hand. In order to make the notation precise, we will specify the level at which W_Q acts whenever necessary, by writing $W_Q^{(M)}$ for the operator W_Q acting on a space of forms of level M.

Theorem 2.3.1. *Let $M \in \mathbb{N}$, let ε be a Dirichlet character modulo M, and let $f \in \mathcal{M}_k(M,\varepsilon)$. Let N be a multiple of M, and let t divide N/M, so that $N = tMR$ for some integer $R \in \mathbb{N}$ and that $f\big|B_t$ may be seen as a form of level N.*

Let $Q \parallel N$, and define $M_Q = \gcd(M,Q)$, $t_Q = \gcd(t,Q)$, $R_Q = \gcd(R,Q)$, so that $Q = t_Q M_Q R_Q$, and then let $M' = M/M_Q$ and $t' = t/t_Q$. Then the form $f\big|B_t\big|I_{tM}^N\big|W_Q^{(N)}$ depends on Q but not on N (as long as N is such that $tM \mid N$ and that $Q \parallel N$ of course), so we may write it as $f\big|B_t\big|W_Q$. Explicitly, we have

$$f\big|B_t\big|W_Q = (R_Q/t_Q)^{k/2}\overline{\varepsilon}_{M'}(t_Q)\overline{\varepsilon}_{M_Q}(t')f\big|W_{M_Q}^{(M)}\big|B_{t'R_Q}.$$

Proof. Let $w_Q = \left[\begin{smallmatrix} Qa & b \\ Nc & Qd \end{smallmatrix}\right]$ where $a,b,c,d \in \mathbb{Z}$ are such that $a \equiv 1 \bmod N/Q$, $b \equiv 1 \bmod Q$, and $\det w_Q = Q$. Then we have

$$\begin{aligned}
f\big|B_t\big|I_{tM}^N\big|W_Q^{(N)} &= t^{-k/2} f\big|_k \left[\begin{smallmatrix} t & \\ & 1 \end{smallmatrix}\right] w_Q \\
&= t^{-k/2} f\big|_k \left[\begin{smallmatrix} t_Q & \\ & 1 \end{smallmatrix}\right] \left[\begin{smallmatrix} t' & \\ & 1 \end{smallmatrix}\right] w_Q \left[\begin{smallmatrix} t'^{-1} & \\ & 1 \end{smallmatrix}\right] \left[\begin{smallmatrix} t' & \\ & 1 \end{smallmatrix}\right] \\
&= t_Q^{-k/2} f\big|_k \begin{bmatrix} t_Q Qa & t_Q t'b \\ \frac{N}{t'}c & Qd \end{bmatrix} \big|B_{t'} \\
&= t_Q^{-k/2} f\big|_k \begin{bmatrix} Qa & t'b \\ \frac{N}{t}c & \frac{Q}{t_Q}d \end{bmatrix} \big|B_{t'} \\
&= t_Q^{-k/2} f\big|_k \begin{bmatrix} \frac{Q}{R_Q}a & t'b \\ \frac{N}{tR_Q}c & \frac{Q}{t_Q}d \end{bmatrix} \left[\begin{smallmatrix} R_Q & \\ & 1 \end{smallmatrix}\right] \big|B_{t'} \\
&= (R_Q/t_Q)^{k/2} f\big|_k \begin{bmatrix} M_Q t_Q a & t'b \\ MR'c & M_Q R_Q d \end{bmatrix} \big|B_{t'R_Q},
\end{aligned}$$

where $R' = R/R_Q \in \mathbb{N}$. As $w_{M_Q} = \left[\begin{smallmatrix} M_Q t_Q a & t'b \\ MR'c & M_Q R_Q d \end{smallmatrix}\right]$ is of the form $\left[\begin{smallmatrix} M_Q x & y \\ Mz & M_Q w \end{smallmatrix}\right]$ where $x,y,z,w \in \mathbb{Z}$ are such that $x \equiv t_Q \bmod M'$, $y \equiv t' \bmod M_Q$ and $\det w_{M_Q} = M_Q$, the result follows from [AL78, proposition 1.1]. □

This formula, along with those for newforms and Eisenstein series presented above, allow us to compute the action of W_Q on the whole space $\mathcal{M}_k(N,\varepsilon)$.

3 Computation of modular Galois representations

In this section, we fix a prime $\ell \in \mathbb{N}$, a newform

$$f = q + \sum_{n \geqslant 2} a_n q^n \in \mathcal{N}_k(N, \varepsilon)$$

of weight $2 \leqslant k \leqslant \ell$, where ε is a Dirichlet character mod N, and a prime $\mathfrak{l}$ above $\ell \in \mathbb{N}$ of the Hecke field of f. We want to compute the Galois representation

$$\rho_{f,\mathfrak{l}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$$

attached to f mod $\mathfrak{l}$.

We are especially interested in the case where f mod $\mathfrak{l}$ admits a companion form or is supersingular, but the algorithms that we describe do not require that this is the case.

For simplicity, we will assume that ℓN is squarefree. This is mainly so as to simplify statements pertaining to the q-expansion of modular forms at all the cusps or such as proposition 3.2.3 below, and this hypothesis could be suppressed without much difficulty.

Later on, we will focus on the case when the nebentypus ε of f is trivial. This is only for the sake of exposition, and this hypothesis may also be removed very easily.

3.1 The modular curve $X_H(\ell N)$

Just as in [Mas13], the idea of our algorithm is to "catch" the representation $\rho_{f,\mathfrak{l}}$ in the torsion of the jacobian of a modular curve. More precisely, according to [Gro90, theorem 9.3 part 2], there exists an eigenform f_2 of weight 2 and level $\Gamma_1(\ell N)$, a prime $\mathfrak{l}_2 \mid \ell$ of the Hecke field of f_2 and an identification of residue fields $\mathbb{F}_{\mathfrak{l}} \simeq \mathbb{F}_{\mathfrak{l}_2}$ such that

$$f \bmod \mathfrak{l} = f_2 \bmod \mathfrak{l}_2.$$

Let ε_2 be the nebentypus of f_2, which is a Dirichlet character modulo ℓN. The same reference also tells us that f_2 may be chosen so that the N-part of ε_2 agrees with ε, in equations

$$(\varepsilon_2)_N = \varepsilon. \tag{3.1.1}$$

As a consequence, $\rho_{f,\mathfrak{l}} \sim \rho_{f_2,\mathfrak{l}_2}$ appears in the ℓ-torsion of the jacobian of the modular curve $X_1(\ell N)$.

However, the genus of $X_1(M)$ is roughly $M^2/24$ by Riemann-Hurwitz and hence grows quickly with M, and unfortunately the algorithm [Mas13] cannot reasonably cope with genera higher than 30. As a result, we are limited to $\ell \leqslant 31$ when $N = 1$, and to even smaller values of ℓ when N is larger.

Nevertheless, the representation we are interested in occurs in the abelian variety A_{f_2} corresponding to the Galois orbit of the eigenform f_2, which is a factor (up to isogeny) of the jacobian $J_1(\ell N)$ of $X_1(\ell N)$, and it is quite possible that A_{f_2} is much smaller than $J_1(\ell N)$. Unfortunately, we do not know how to compute explicitly with abelian varieties, unless they are provided to us as the jacobian of some curve. We thus want to find a curve whose jacobian contains A_{f_2} and is not much larger than it.

A natural solution, which we owe to [DvHZ14], is to introduce the modular curve $X_H(\ell N)$ corresponding to the congruence subgroup

$$\Gamma_H(\ell N) = \left\{ \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \mid \ell N \text{ and } a, d \bmod \ell N \in H \right\},$$

where $H \leqslant (\mathbb{Z}/\ell N\mathbb{Z})^*$ is the kernel of the nebentypus ε_2 of f_2. As $\Gamma_H(\ell N)$ is an intermediate congruence subgroup between $\Gamma_1(\ell N)$ and $\Gamma_0(\ell N)$, this modular curve is defined over $\mathbb{Q}$ and is intermediate between $X_0(\ell N)$ and $X_1(\ell N)$. In some cases, its genus is significantly smaller than that of $X_1(\ell N)$, and so we save a lot of computational effort by replacing $X_1(\ell N)$ with it, but in other cases we have $H \leqslant \{\pm 1\}$ so that $\Gamma_H(\ell N) = \Gamma_1(\ell N)$ and $X_H(\ell N) = X_1(\ell N)$.

More precisely, note that

$$p^{k-1}\varepsilon(p) \bmod \mathfrak{l} = \det \rho_{f,\mathfrak{l}}(\mathrm{Frob}_p) = \det \rho_{f_2,\mathfrak{l}_2}(\mathrm{Frob}_p) = p\varepsilon_2(p) \bmod \mathfrak{l}_2$$

for all $p \nmid \ell N$ prime, so the character ε_2 must satisfy

$$\varepsilon_2(x) \bmod \mathfrak{l}_2 = x^{k-2}\varepsilon(x) \bmod \mathfrak{l}$$

for all $x \in \mathbb{Z}$ by Dirichlet's theorem on arithmetic progressions.

To simplify, **we suppose from now on that the nebentypus ε of f is trivial**. By (3.1.1), ε_2 is then a Dirichlet character modulo ℓN of conductor ℓ or 1, and it satisfies

$$\varepsilon_2(x) \equiv x^{k-2} \bmod \mathfrak{l}_2$$

for all $x \in \mathbb{Z}$, so that the subgroup $H \leqslant (\mathbb{Z}/\ell N\mathbb{Z})^*$ is the pull-back to $(\mathbb{Z}/\ell N\mathbb{Z})^*$ of the subgroup K of $(\mathbb{Z}/\ell\mathbb{Z})^*$ formed of the $(k-2)$-torsion elements. The lower the additive order of $k-2 \bmod \ell - 1$, the larger H, hence the smaller $X_H(\ell N)$ and the more efficient our computation of $\rho_{f,\mathfrak{l}}$ will be.

3.2 The periods of $X_H(\ell N)$

As in [Mas13], in order to compute $\rho_{f,\mathfrak{l}}$ we begin by computing the periods of the modular curve $X_H(\ell N)$, which will allow us to view its jacobian as an explicit complex torus.

Proposition 3.2.1. *Let $n \in \mathbb{N}$ be any integer, and let T_n be the corresponding Hecke operator at level $\Gamma_H(\ell N)$. Let $f = q + \sum_{m \geqslant 2} a_m q^m \in \mathcal{N}_k(M, \varepsilon)$ be a newform of weight k whose level M divides ℓN and whose nebentypus ε factors through H, and let t be a divisor of $\ell N/M$. Write $n = n_1 n_2$, where $n_1 = \gcd(n, (\ell N)^\infty)$, and factor n_1 as $\prod_i p_i^{e_i}$. Then*

$$f\big|B_t\big|I_{tM}^{\ell N}\big|T_n = a_{n_2} f\big|B_t\big| \prod_i U_{p_i}^{e_i},$$

where $\left(\sum_m b_m q^m\right)\big|U_p = \sum_m b_{pm} q^m$, and furthermore

$$f\big|B_t\big|U_p = \begin{cases} a_p f\big|B_t - p^{k-1}\varepsilon(p) f\big|B_{pt} & \text{if } p \nmid t, \\ f\big|B_{t/p} & \text{if } p \mid t \end{cases}$$

for all primes $p \in \mathbb{N}$. Note that in the first case, $\varepsilon(p) = 0$ if $p \mid M$, since ε is a character mod M.

Proof. Immediate from the formulas

$$F\big|T_{n_1}T_{n_2} = F\big|T_{n_2}T_{n_1} \quad \text{if } \gcd(n_1,n_2)=1,$$

$$F\big|U_{p^e} = F\big|U_p^e \quad \text{for } p \mid \ell N \text{ prime and } e \in \mathbb{N},$$

and

$$F\big|T_p = \sum_m b_{pm}q^m + p^{k-1}\chi(p)\sum_m b_m q^{pm}$$

valid for all $F = \sum_m b_m q^m \in \mathcal{S}_k(\ell N, \chi)$. □

The space of holomorphic differentials on $X_H(\ell N)$ is

$$\mathcal{S}_2\big(\Gamma_H(\ell N)\big) = \bigoplus_{\substack{\varepsilon \bmod \ell N \\ \operatorname{Ker}\varepsilon \geqslant H}} \mathcal{S}_2(\ell N, \varepsilon). \tag{3.2.2}$$

A natural basis of this space is formed of the $f\big|B_t$, where f and t are as above and f has weight $k=2$.

For each primitive Dirichlet character χ, define the modular symbol

$$s_\chi = \sum_{a \bmod m} \bar\chi(-a)\{\infty, a/m\},$$

where m is the modulus of χ. The reason why we introduce these symbols is the following formula:

Proposition 3.2.3. *Fix a squarefree integer $N \in \mathbb{N}$, consider a newform $f = q + \sum_{n\geqslant 2} a_n q^n \in \mathcal{N}_2(M,\varepsilon)$ of weight 2 and an integer t as above, and let $\lambda \in \mathbb{C}^*$ be such that*

$$f\big|W_M = \lambda \sum_{n\geqslant 1} \bar a_n q^n.$$

Then for all primitive *Dirichlet characters χ whose modulus m is prime to N, we have*

$$\int_{s_\chi} f\big|B_t = \frac{\chi(t)}{t}\frac{m}{2\pi i \mathfrak{g}(\chi)} \sum_{n\geqslant 1} \frac{\chi(n)a_n - \lambda_\chi \bar\chi(n)\bar a_n}{n} R^n,$$

where $\lambda_\chi = \chi(-M)\varepsilon(m)\frac{\mathfrak{g}(\chi)}{\mathfrak{g}(\bar\chi)}\lambda$ and $R = e^{-2\pi/m\sqrt{M}}$.

Proof. We have

$$\int_{s_\chi} f\big|B_t = \sum_{x \bmod m} \bar\chi(-x)\int_\infty^{x/m} f(t\tau)d\tau = \frac{\chi(t)}{t}\sum_{x \bmod m}\bar\chi(-x)\int_\infty^{x/m} f(\tau)d\tau$$

by the changes of variable $\tau' = t\tau$ and $x' = tx$, which is legitimate since t and m are coprime.

Next, note that $\chi(y) = \frac{1}{m}\sum_{x \bmod m}\hat\chi(x)e\left(\frac{xy}{m}\right)$ where $\hat\chi(x) = \bar\chi(-x)\mathfrak{g}(\chi)$ since χ is primitive. Therefore,

$$\sum_{x \bmod m}\bar\chi(-x)\int_\infty^{x/m} f(\tau)d\tau = \frac{m}{\mathfrak{g}(\chi)}\int_\infty^0 f\otimes\chi,$$

where $f \otimes \chi = q + \sum_{n \geqslant 2} \chi(n) a_n q^n$ is a newform of weight 2, level $M' = m^2 M$ and character $\varepsilon\chi^2$ by [AL78, p. 228]. Furthermore, according to the same reference, we have

$$f \otimes \chi \big| W_{M'} = \lambda_\chi \left(q + \sum_{n \geqslant 2} \bar{\chi}(n) \bar{a_n} q^n \right).$$

The result follows by splitting the integration path at $i/\sqrt{M'}$ and using $W_{M'}$ to move the endpoint 0 to ∞. □

Thanks to the previous propositions, we can compute efficiently the integrals of the form

$$\int_{s_\chi} f \big| B_t \big| T$$

where f and t are as above and T is a Hecke operator, and thus the periods of $X_H(\ell N)$, by choosing a family of characters χ such that the s_χ generate the homology as a Hecke-module.

The point of using the Hecke-module structure of the homology is that this reduces our task to computing integrals along modular symbols that generate the homology as a Hecke-module, as opposed to a $\mathbb{Z}$-module. This results in smaller generating families, formed of symbols s_χ that lead via proposition 3.2.3 to series that converge faster, thus requiring the computation of fewer q-expansion coefficients a_n to reach the desired accuracy.

3.3 High-precision q-expansion of the forms of weight 2

We are thus able to compute the periods of $X_H(\ell N)$ to very high precision, provided that we first compute enough terms of the q-expansion of the newforms of weight 2 appearing in (3.2.2). This is a non-trivial task since we typically need a few hundred thousands terms. We do so thanks to an improved version of the mod p modular equation method which we described in [Mas13, section 3.1].

Suppose for the simplicity of the exposition that the dimension g_0 of $\mathcal{S}_2\big(\Gamma_0(\ell N)\big)$ is at least 2, and let $f_1, \ldots, f_{g_0} \in \mathcal{S}_2\big(\Gamma_0(\ell N)\big)$ be a basis made of forms whose Fourier coefficients are rational, where g_0 is thus the genus of $X_0(\ell N)$. Thanks to the Sturm bound, we may easily rescale these forms so that their Fourier coefficients are integers. As in [Mas13, section 3.1], we then begin by computing a polynomial equation relating the functions f_1/du and u on $X_0(\ell N)$ modulo a large enough prime $p \in \mathbb{N}$, where $u = 1/j \in q\mathbb{Z}[[q]]$ is the multiplicative inverse of the j-invariant. The degrees of this equation are respectively d_0 and at most $d_0 + s_0 + 2g_0 - 2$, where d_0 is the index of $\Gamma_0(\ell N)$ in $\mathrm{SL}_2(\mathbb{Z})$ and s_0 is the number of cusps of $X_0(\ell N)$. We then compute a lot of terms of the q-expansion of u mod p. This can be done quickly thanks to the formulas

$$u = \frac{E_4^3 - E_6^2}{(12E_4)^3}, \quad E_4 = 1 + 240 \sum_{n \geqslant 1} \sigma_3(n) q^n, \quad E_6 = 1 - 504 \sum_{n \geqslant 1} \sigma_5(n) q^n$$

where $\sigma_h(n) = \sum_{0<d|n} d^h$, and an Eratosthenes sieve, as long as we use fast series arithmetic and we do all the computations mod p. Next, we use Newton iteration in $\mathbb{F}_p[[q]]$ on the bivariate polynomial equation so as to recover the coefficients mod p of f_1/du, and hence of f_1. Finally, we lift these coefficients back to $\mathbb{Z}$, which we can do unambiguously thanks to Deligne's bounds if p is large enough.

This is rather slow, as the degrees of the polynomial equation tend to be high, so for f_2 we proceed a bit differently, by computing a polynomial equation relating f_2/f_1 and u modulo a (possibly different) large prime p. We then use Newton iteration to recover the coefficients of f_2. This time, the degrees of this equation are d_0 and at most $2g_0-2$, which is already much better, so this is much faster than for f_1.

Then, for all the other forms f_i in the basis of $\mathcal{S}_2\big(\Gamma_0(\ell N)\big)$, we compute an equation relating f_i/f_1 to f_2/f_1 modulo a (possibly again different) large prime p, and we use Newton iteration to deduce the coefficients of f_i. This is very fast, as the degree of this equation is at most $2g_0-2$ in each variable; besides, all the forms f_i may be treated in parallel.

Finally, let ε be a non-trivial character appearing in (3.2.2), let $r>1$ be its order, and fix a basis $F_1,\dots,F_d$ of $\mathcal{S}_2(\ell N,\varepsilon)$ made up of forms whose Fourier coefficients lie in the value field $K=\mathbb{Q}(\varepsilon)$ of ε. Such a basis always exists and may easily be computed thanks to [CF96, theorem p. xiii]. Again, thanks to the Sturm bound, we may effortlessly arrange for the F_i to have integral coefficients. Then, for each F_i, we choose a large enough prime p such that $p\equiv 1 \bmod r$, so that p splits completely in K, and we compute an equation relating $(F_i/f_1)^r \bmod \mathfrak{p}$ to $f_2/f_1 \bmod p$ for each prime $\mathfrak{p}$ of K above p. By definition of r, the function $(F_i/f_1)^r$ descends to $X_0(\ell N)$, so this equation has degrees at most $2g_0-2$ and $2g-2$, where g is the genus of $X_H(\ell N)$, and so the computation is still reasonably fast. We then use Newton iteration to recover the coefficients of $F_i \bmod \mathfrak{p}$, and finally lift these coefficients back to K thanks to Chinese remainders over the primes $\mathfrak{p}\mid p$. Note that the various forms F_i and primes $\mathfrak{p}$ may easily be processed in parallel.

As in [Mas13, section 3.1], we thus obtain a method to expand a basis of $\mathcal{S}_2\big(\Gamma_H(\ell N)\big)$ to q-adic accuracy $O(q^B)$ in time quasilinear in B. However, this new method performs much better in practice, since it relies on modular equations of degrees much smaller than in [Mas13] for all but the first form.

3.4 The rest of the computation

Once we have computed a very precise approximation of the periods of $X_H(\ell N)$ over $\mathbb{C}$, we may proceed essentially as in [Mas13], by inverting the Abel-Jacobi map at ℓ-torsion points thanks to Kamal Khuri-Makdisi's algorithms [KM07].

In order to adapt these algorithms to $X_H(\ell N)$, we need to compute the Riemann-Roch space

$$V_2 \simeq H^0\big(X_H(\ell N), D_0\big) \tag{3.4.1}$$

attached to a divisor D_0 defined over $\mathbb{Q}$ whose degree d_0 is at least $2g+1$, where g is the genus of $X_H(\ell N)$. As in [Mas13], we let D_0 be the sum of a canonical divisor of $X_H(\ell N)$ and of a divisor D_∞ of degree 3 supported by three distinct cusps; we thus set $d_0=2g+1$ exactly, which is good since higher values of d_0 would just slow Khuri-Makdisi's algorithms down. The space V_2 is then the space of meromorphic differentials that have at most simple poles at the 3 cusps supporting D_∞ and are holomorphic elsewhere. As a result, V_2 is contained in the space $\mathcal{M}_2\big(\Gamma_H(\ell N)\big)$ of modular forms of weight 2; more precisely, we have

$$V_2 = \mathcal{S}_2\big(\Gamma_H(\ell N)\big) \oplus E,$$

where E is the subspace of the Eisenstein space $\mathcal{E}_2\big(\Gamma_H(\ell N)\big)$ formed of the series that vanish at all the cusps except those 3 that support D_∞.

Remark 3.4.2. The dimension of E is 2. This is a consequence of the Riemann-Roch theorem and of (3.4.1); alternatively, this can be seen directly since the map that evaluates the modular forms at all of the cusps induces an isomorphism between the Eisenstein subspace and the trace zero subspace.

In order for D_0 to be defined over $\mathbb{Q}$, we need D_∞ itself to be defined over $\mathbb{Q}$. Since we assumed that N is squarefree, say $N = p_1 \cdots p_r$, this is not difficult. Indeed, the moduli interpretation of cusps as generalised elliptic curves with level structure (cf. [DI95, section 9.3]) yields an identification of $G_\mathbb{Q}$-sets

$$\mathrm{Cusps}\big(X_H(\ell N)\big) = \mathrm{Cusps}\big(X_K(\ell)\big) \times \mathrm{Cusps}\big(X_0(p_1)\big) \times \cdots \times \mathrm{Cusps}\big(X_0(p_r)\big).$$

This moduli interpretation also makes the action of $G_\mathbb{Q}$ on the cusps of $X_K(\ell)$ and of $X_0(p_i)$ transparent, so constructing D_∞ poses no difficulty.

Since the level ℓN is squarefree, the group spanned by the operators W_Q and $\langle d \rangle$ acts transitively on the cusps, so the formulas established in section 2 allow us to deduce the q-expansion of any modular form in $\mathcal{M}_2\big(\Gamma_H(\ell N)\big)$ at each of the cusps from its q-expansion at the cusp ∞. In particular, it is easy to compute a basis of E by linear algebra. Therefore, we choose to represent the elements of V_2 by their q-expansion at all the cusps, with enough q-adic accuracy to ensure that Khuri-Makdisi's algorithms perform correctly.

Now that we are able to compute in the jacobian $J_H(\ell N)$ of $X_H(\ell N)$, we may proceed just as in [Mas13], by identifying the 2-dimensional subspace $V_{f,\mathfrak{l}}$ of $J_H(\ell N)[\ell]$ that affords $\rho_{f,\mathfrak{l}}$ as the space where T_n acts as the coefficient $a_n \bmod \mathfrak{l}$ of f for all n, inverting the Abel-Jacobi map at the points of $V_{f,\mathfrak{l}}$, and evaluating a rational map $\alpha \in \mathbb{Q}\big(J_H(\ell N)\big)$ at these points; we do all this with high-accuracy approximations over $\mathbb{C}$ as in sections 3.5 and 3.6 of [Mas13]. Finally, we use these complex approximations to identify the coefficients of

$$F(x) = \prod_{\substack{P \in V_{f,\mathfrak{l}} \\ P \neq 0}} \big(x - \alpha(P)\big)$$

as rational numbers. If these identifications are correct and if α is one-to-one on $V_{f,\mathfrak{l}}$, then the polynomial thus obtained describes the representation $\rho_{f,\mathfrak{l}}$ since the Galois action on its roots mimicks the Galois action on the points of $V_{f,\mathfrak{l}}$.

4 Certification of the results

We now wish to certify that the data computed in the previous section does define the representation $\rho_{f,\mathfrak{l}}$. This is very likely, but not completely certain, as these data were produced by identifying rational numbers from floating point approximations.

The certification method we present here is a generalisation of the one presented in [Mas16]. We still focus on the case where the level N of f is squarefree, although it is probably not difficult to drop this hypothesis, possibly at the expense of slowing down the computations. For simplicity, we also assume that the representation $\rho_{f,\mathfrak{l}}$ is surjective; it is easy to modify our arguments when this is not the case.

In order to completely certify our data, we will eventually have to restrict to the case where the nebentypus ε of f is trivial; unlike in section 3, this is a real requirement which the author does not know how to remove. It is however not necessary to make this assumption if one is only interested in the *projective* representation attached to $f \bmod \mathfrak{l}$, which is the case if one just wants to construct explicitly $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$-number fields with small discriminants.

4.1 Reduction of the polynomials

The polynomial $F(x)$ computed above tends to have a very large arithmetic height. More precisely, in [Mas16, section 2] where we computed in $X_1(\ell)$ instead of $X_H(\ell N)$, we conjectured that the number of decimal digits of the typical denominator of the coefficients of $F(x)$ was approximately $g^{5/2}$, where g is the genus of $X_1(\ell)$.

We have computed two representations (cf. the results section) mod $\ell = 13$ in the jacobian of modular curves X_H of respective levels $5 \cdot 13$ and $7 \cdot 13$ which both happen to have genus $g = 13$. The denominator of the polynomial $F(x)$ thus obtained has 458 decimal digits for the first representation, and 586 for the second one, which seems to indicate that our conjecture extends to the modular curves $X_H(\ell N)$; this was expected, as our prediction is governed by the genus and not by the level. However, we have also computed a mod $\ell = 41$ representation in a modular curve X_H of genus $g = 25$, and this yielded a polynomial $F(x)$ whose denominator has 4582 decimal digits! A bit of extra experimentation with modular curves $X_H(\ell)$ of small genus but large values of ℓ have confirmed that the height of $F(x)$ get much larger than the predicted $g^{5/2}$ when ℓ gets really large, which indicates that our conjecture is wrong and must be modified to take the value of ℓ (but not N) into account.

Anyhow, it is extremely inconvenient to work with polynomials of such height, so we want to apply [Pari/GP]'s function `polredbest` to them, as this function computes a nicer polynomial defining the same number field. As noted in [Mas16], very often the polynomial $F(x)$ is simply too large for this to be possible; however, we may form the polynomials

$$F_i(x) = \prod_{S_i \cdot P \in V_{f,\mathfrak{l}}^{S_i}} \left(x - \sum_{s \in S_i} \alpha(s \cdot P) \right)$$

that ought to correspond to the quotient representations

$$\rho_{f,\mathfrak{l}}^{S_i} : G_\mathbb{Q} \xrightarrow{\rho_{f,\mathfrak{l}}} \mathrm{GL}_2(\mathbb{F}_\mathfrak{l}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{l})/S_i$$

for $0 \leqslant i \leqslant r$, and identify their coefficients as rationals, where $S_i = \{s^{2^i},\ s \in \mathbb{F}_\mathfrak{l}^*\}$, $V_{f,\mathfrak{l}}^{S_i} = (V_{f,\mathfrak{l}} - \{0\})/S_i$, and r is the 2-adic valuation of $\#\mathbb{F}_\mathfrak{l}^*$; we may then reduce these polynomials inductively on i as explained in section 2 of [Mas16].

The point of this is that the polynomial $F_r(x)$ ought to correspond to the quotient representation $\rho_{f,\mathfrak{l}}^{S_r}$, which contains enough information to recover $\rho_{f,\mathfrak{l}}$ itself while being much easier to deal with, as explained in section 2 of [Mas16].

4.2 Certification of the data

Now that the polynomials have been reduced, we begin as in [Mas16] by proving that the Galois group of $F_0(x)$ over $\mathbb{Q}$ is $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$, for instance thanks to the "unordered cross-ratio" method presented in section 3.3.1 of [Mas13]. If we are only interested in the construction of $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$-number fields with small discriminant, we may stop here, check that the root field of $F_0(x)$ has as little ramification as expected, and add $F_0(x)$ to our collection; in fact, we did not need to compute and reduce the polynomials $F_i(x)$ for $i > 0$ in the first place.

However, if we are interested in the representation $\rho_{f,\mathfrak{l}}$, then we need to certify that the polynomial $F_r(x)$ corresponds in the sense of [Mas16] to the quotient representation $\rho_{f,\mathfrak{l}}^{S_r}$. In order to do this, we now introduce a generalisation of the methods presented in [Mas16].

The reason why we need to modify these methods is that theorem 4 from [Mas16], which was used to certify the modularity of the projective representation defined by $F_0(x)$, only applies to representations attached to forms of level 1, which is not the case in this article, and which are wildly ramified at ℓ, which is precisely not the case we are most interested in. As a result, we present a new, more general method to certify that a projective Galois representation is modular and comes from a form of squarefree level.

We begin by recalling a well-known result about projective Galois representations.

Lemma 4.2.1. *Let $\mathbb{F}$ be a topological field, $p \in \mathbb{N}$ a prime, and let $W_p \lhd I_p \leqslant G_\mathbb{Q}$ be the wild inertia and inertia subgroups attached to some prime of $\overline{\mathbb{Q}}$ above p. Every continuous character $\chi : I_p \longrightarrow \mathbb{F}^*$ may be extended to a continuous character $G_\mathbb{Q} \longrightarrow \mathbb{F}^*$ which is unramified away from p. Similarly, every continuous character $\chi : W_p \longrightarrow \mathbb{F}^*$ may be extended to a continuous character $G_\mathbb{Q} \longrightarrow \mathbb{F}^*$ which is unramified away from p.*

Proof. Let $\chi : I_p \longrightarrow \mathbb{F}^*$ be a continuous character. As $\mathbb{F}^*$ is abelian, χ factors through the abelianisation I_p^{ab} of I_p.

By class field theory, we have a compatible system of isomorphisms of topological groups

$$\begin{array}{ccccccc} W_p^{\mathrm{ab}} & \subset & I_p^{\mathrm{ab}} & \subset & D_p^{\mathrm{ab}} & \subset & G_\mathbb{Q}^{\mathrm{ab}} \\ \wr| & & \wr| & & \wr| & & \wr| \\ 1+p\mathbb{Z}_p & \subset & \mathbb{Z}_p^* & \subset & p^{\hat{\mathbb{Z}}} \times \mathbb{Z}_p^* & \subset & \prod_p \mathbb{Z}_p^* \end{array}$$

where $D_p^{\mathrm{ab}} \subset G_{\mathbb{Q}_p}^{\mathrm{ab}}$ is the decomposition group of $G_\mathbb{Q}^{\mathrm{ab}}$. We may thus extend χ by composing it with the continuous projections $G_\mathbb{Q} \longrightarrow G_\mathbb{Q}^{\mathrm{ab}} \longrightarrow I_p^{\mathrm{ab}}$, and the resulting character is unramified away from p.

Similarly, since $1 + p\mathbb{Z}_p$ is a direct factor of $\mathbb{Z}_p^*$, we may extend any continuous character on W_p to I_p, and thus to $G_\mathbb{Q}$. □

Our result on the lifting of projective Galois representations is the following:

Theorem 4.2.2 (Serre, Tate)**.** *Let $\pi : G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\overline{\mathbb{F}_\ell})$ be a projective Galois representation. There exists a lift $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ such that for all primes $p \in \mathbb{N}$,*

$$\pi \text{ is unramified at } p \implies \rho \text{ is unramified at } p$$

and

$$\pi \text{ is tamely ramified at } p \implies \rho \text{ is tamely ramified at } p.$$

Remark 4.2.3. The field of definition of ρ may be larger than that of π.

Proof. J.-P. Serre proves in [Ser77, pp. 332–336] that

$$H^2(G_{\mathbb{Q}}, \mathbb{Q}_p/\mathbb{Z}_p) = 0$$

for all primes $p \in \mathbb{N}$. Since $\overline{\mathbb{F}_\ell}^* \simeq \bigoplus_{p \neq \ell} \mathbb{Q}_p/\mathbb{Z}_p$, this implies that every projective representation $\pi : G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\overline{\mathbb{F}_\ell})$ can be lifted to a linear representation $\rho' : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$. However, this lift may not have the required ramification behaviour.

If p is a prime such that π is unramified, then $\rho'|_{I_p} = \left[\begin{smallmatrix} \chi_p & \\ & \chi_p \end{smallmatrix}\right]$, where $\chi_p : I_p \longrightarrow \overline{\mathbb{F}_\ell}^*$ is a character which we may extend to $G_{\mathbb{Q}}$ by lemma 4.2.1.

Similarly, if p is a prime such that π is tamely ramified, then $\rho'|_{W_p} = \left[\begin{smallmatrix} \chi_p & \\ & \chi_p \end{smallmatrix}\right]$, where $\chi_p : W_p \longrightarrow \overline{\mathbb{F}_\ell}^*$ may be extended to $G_{\mathbb{Q}}$ by lemma 4.2.1.

Finally, if π is wildly ramified at p, let χ_p denote the trivial character on $G_{\mathbb{Q}}$.

For each prime p, we thus have a character χ_p on $G_{\mathbb{Q}}$ which is unramified away from p. By compactness of $G_{\mathbb{Q}}$, $\operatorname{Im}\rho'$ is finite, so ρ' ramifies at finitely many primes p and so only finitely many of the χ_p are nontrivial. We may thus define $\chi = \prod_p \chi_p$, and it is clear that $\rho = \rho' \otimes \chi^{-1}$ has the required properties. □

Thanks to this result, we may lift projective representations to linear ones, to which we may apply Serre's modularity conjecture so as to prove that the original projective representation is modular. This is very useful for us as we want to certify that our data correspond to modular Galois representations; however, this is not enough, as we want to prove that the representation corresponding to our data is attached to the eigenform f and not a different one. In this view, we establish the following theorem, which allows us to prove that our data define a representation attached to a form of the same level as f with very little computational effort.

Theorem 4.2.4. *Let $\pi : G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\overline{\mathbb{F}_\ell})$ be a projective Galois representation, and K be the number field corresponding via π to the stabiliser of a point of $\mathbb{P}^1(\overline{\mathbb{F}_\ell})$. Let R be the set of primes $p \neq \ell$ at which π ramifies. Suppose that π is irreducible and odd*[1]*, and that for all $p \in R$, π is tamely ramified at p, and there exists an unramified prime $\mathfrak{p}$ of K above p. Then there exists a newform $f \in \mathcal{S}_k\big(\Gamma_1(N)\big)$ with $N = \prod_{p \in R} p$ and $2 \leqslant k \leqslant \ell + 2$ such that π is equivalent to the projective representation $\pi_{f,\mathfrak{l}}$ attached to f modulo a prime $\mathfrak{l}$ above ℓ.*

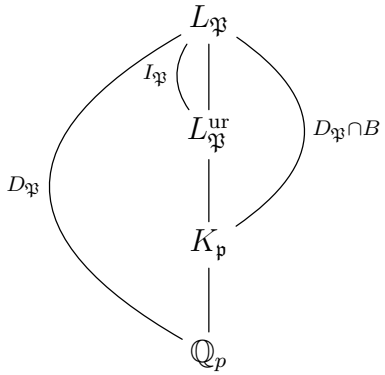
[1]These conditions respectively mean that π does not fix any point of $\mathbb{P}^1(\overline{\mathbb{F}_\ell})$, and that the image of complex conjugation is similar to $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$.

Proof. By theorem 4.2.2, there exists a lift $\rho : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ of π which is irreducible, odd, unramified at the primes at which π is unramified, and tamely ramified at all primes $p \neq \ell$. Therefore, Serre's modularity conjecture, which was proved by Khare and Wintenberger in [KW09], implies that there exists a newform $f \in \mathcal{S}_k\big(\Gamma_1(N)\big)$ such that ρ is equivalent to the representation attached to f mod $\mathfrak{l}$, where $N = \prod_{p \in R} p^{n_p}$ is the Serre conductor of ρ and $\mathfrak{l}$ is a prime above ℓ. Besides, according to [RS01, theorem 2.7], after twisting by a character of ℓ-power conductor (which does not affect π), we may suppose that $2 \leqslant k \leqslant \ell + 2$, so to conclude we only have to prove that $n_p = 1$ for all $p \in R$.

Let $p \in R$, so that by our hypothesis there exists an unramified prime $\mathfrak{p}$ of K above p. Let $\mathfrak{P}$ be a prime of $\overline{\mathbb{Q}}$ above $\mathfrak{p}$, and let $I_{\mathfrak{P}} \leqslant D_{\mathfrak{P}} \leqslant G_{\mathbb{Q}}$ be its inertia and decomposition subgroups. Since ρ is tamely ramified at p, the local exponent of its conductor is just

$$n_p = \operatorname{codim} V^{\rho(I_{\mathfrak{P}})},$$

where $V \simeq \overline{\mathbb{F}_\ell}^2$ is the space of the representation. As π ramifies at p, so does ρ, so $\rho(I_p)$ is not trivial and $n_p \geqslant 1$. Let L be the Galois number field cut out by ρ, and let $B = \mathrm{Gal}(L/K)$, so that $\rho(B)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ by definition of K. As $\mathfrak{p}$ is unramified, we have a tower of local extensions



where $L_{\mathfrak{P}}^{\mathrm{ur}}$ is the maximal unramified subextension of $L_{\mathfrak{P}}$. Therefore, $I_{\mathfrak{P}}$ is contained in B, so $\rho|_{I_{\mathfrak{P}}} \sim \left[\begin{smallmatrix} \chi_p & * \\ 0 & * \end{smallmatrix}\right]$ for some character $\chi_p : I_{\mathfrak{P}} \longrightarrow \overline{\mathbb{F}_\ell}^*$, which we may extend to $G_{\mathbb{Q}}$ by lemma 4.2.1. After replacing ρ with $\rho \otimes \prod_{p \in R} \chi_p^{-1}$, which does not affect the weight since $\ell \notin R$, we may thus suppose that $\rho|_{I_{\mathfrak{P}}} \sim \left[\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right]$, so that $n_p \leqslant 1$. This concludes the proof. □

Remark 4.2.5. Conversely, let $\rho = \rho_{f,\mathfrak{l}}$ be a mod ℓ representation attached to an eigenform $f \in \mathcal{S}_k\big(\Gamma_1(N)\big)$. We may suppose that N is minimal, that is to say that it is the Serre conductor $\prod_{p \neq \ell} p^{n_p}$ of ρ, where

$$n_p = \operatorname{codim} V^{\rho(I_p)} + \sum_{n \geqslant 1} \frac{1}{[I_p : I_p^{(n)}]} \operatorname{codim} V^{\rho(I_p^{(n)})} \tag{4.2.6}$$

and the $I_p^{(n)} \leqslant W_p$ are the higher ramification groups for $n \geqslant 1$. Then if $p \in \mathbb{N}$ is a prime such that $p \parallel N$ so that $n_p = 1$, the equation (4.2.6) implies that ρ is tamely ramified at p and that the inertia at p fixes a dimension 1 subspace of V, so that the number field K corresponding by ρ to the stabiliser of a point in $\mathbb{P}^1(\mathbb{F}_{\mathfrak{l}})$ has an unramified prime $\mathfrak{p}$ above p. Therefore, the implication between the existence of an unramified prime $\mathfrak{p}$ and the fact that $n_p = 1$ is actually an equivalence, so that

theorem 4.2.4 yields a very efficient and general-purpose criterion that we can use to prove that a polynomial with Galois group a subgroup of $\mathrm{PGL}_2(\mathbb{F}_{\ell^m})$ defines a projective representation which is modular of squarefree level.

Thanks to this criterion, we are able to prove that the polynomial $F_0(x)$ that we have computed defines a projective representation π_F attached to an eigenform f' of the same level N as f and of weight $2 \leqslant k \leqslant \ell+2$ modulo a prime $\mathfrak{l}'$. We now want to ensure that this representation is actually attached to f modulo the prime $\mathfrak{l}$. We will prove this by listing all the possible candidate forms, and eliminating them one by one. Of course, the fact that we have already determined the level narrows down this search considerably.

To do so, we apply a generalisation of the technique presented in the second half of section 3.3.2 of [Mas16]: for each prime p such that

$$\begin{gathered} F_0(x) \bmod p \text{ is squarefree and splits as a product of} \\ \text{linear or quadratic factors, but does not split completely,} \end{gathered} \tag{4.2.7}$$

we know that $\pi_F(\mathrm{Frob}_p)$ is of order exactly 2, so that its trace is zero. As a result, any eigenform f' such that $\pi_F \sim \pi_{f',\mathfrak{l}'}$ for some $\mathfrak{l}'$ must satisfy $a_p(f') \equiv 0 \bmod \mathfrak{l}'$.

We thus form the list of pairs $(f', \mathfrak{l}')$, where f' is a newform of level $\Gamma_1(N)$ and weight between 2 and $\ell+2$, and $\mathfrak{l}'$ is a prime of the Hecke field of f' of the appropriate degree above ℓ; then we start looking for primes p satisfying the condition (4.2.7), and for each such prime we eliminate the pairs $(f', \mathfrak{l}')$ that fail to satisfy the condition $a_p(f') \equiv 0 \bmod \mathfrak{l}'$. This is very efficient, as each such prime p divides the size of the list roughly by $\#\mathbb{F}_{\mathfrak{l}}$. Besides, in order to speed up the computation, we can replace the condition $a_p(f') \equiv 0 \bmod \mathfrak{l}'$ by $N_{\mathbb{Q}}^{K'_f}\big(a_p(f')\big) \equiv 0 \bmod \ell$ where $N_{\mathbb{Q}}^{K'_f}$ is the norm from the Hecke field of f' to $\mathbb{Q}$, which is weaker but just as discriminating in practice, and allows us to barely have to deal with the different possible primes $\mathfrak{l}'$ above ℓ at all.

We stop when all the remaining pairs $(f', \mathfrak{l}')$ correspond to the same projective representation. In general, this happens when the only couple left on the list is $(f, \mathfrak{l})$ itself, except of course when f admits a companion mod $\mathfrak{l}$, in which case we wait for the list to reduce to the couple $(f, \mathfrak{l})$ and the companion couple. Typically, it is enough to consider the primes $p \leqslant 100$ to achieve this.

We are thus able to certify that $F_0(x)$ defines the projective representation attached to f mod $\mathfrak{l}$. If the nebentypus ε of f is trivial, we may then apply without any modification the "group cohomology method" presented in section 3.6 of [Mas16] to certify that the polynomial $F_r(x)$ defines the quotient representation $\rho_{f,\mathfrak{l}}^{S_r}$ attached to f mod $\mathfrak{l}$, and to compute the image of Frobenius elements in a certified way. Unfortunately, the author does not know at present how to do the same thing if ε is not trivial.

Remark 4.2.8. In principle, we could also have used the range $1 \leqslant k \leqslant \ell+1$ throughout this section. We prefer the interval $2 \leqslant k \leqslant \ell+2$ because cuspforms of weight 1 are difficult to compute, so that using the range $1 \leqslant k \leqslant \ell+1$ would make the generation of the list of the $(f', \mathfrak{l}')$ unnecessarily delicate.

5 Results

We have used the above algorithms to compute the mod 13 Galois representations attached to the primitive newforms

$$q + 2q^2 - 4q^3 + O(q^4) \in \mathcal{N}_6\big(\Gamma_0(5)\big)$$

and

$$q - 6q^2 - 42q^3 + O(q^4) \in \mathcal{N}_8\big(\Gamma_0(7)\big)$$

of respective LMFDB labels 5.6.1.a and 7.8.1.a. The former is supersingular mod 13, whereas the latter admits 7.6.1.a as a companion mod 13. The reason for the choice of these forms is that the corresponding Galois representations occur in the torsion of Jacobian of modular curves $X_H(\ell N)$ whose genus is moderate, namely $g = 13$ in both cases; in particular, working with 7.6.1.a instead of 7.8.1.a would have led to computing the same projective representation but a different linear representation in a different curve of higher genus. Similarly, the projective representation attached to 5.6.1.a also comes from 5.10.1.a mod 13, but using the former leads to a modular curve of lower genus than with the latter.

In both cases, the computation of the Galois representations mod 13 took about 12 hours, after which the reduction of the polynomials by the inductive method took just a few minutes (as a comparison, the direct reduction of the polynomial $F_r(x)$ takes about 90 hours), and finally the whole certification process took less than a minute.

We then computed the mod 41 representation attached to the form

$$q + 1728q^2 - 59049q^3 + O(q^4) \in \mathcal{N}_{22}\big(\Gamma_0(3)\big)$$

of LMFDB label 3.22.1.b that admits 3.20.1.b as a companion. The genus of the modular curve $X_H(3 \cdot 41)$ is $g = 25$ in this case, which is at the very top of the range of genera that are reasonably amenable to computation with our method. The computation took three months and was parallelised on several dozens of cores, after which the reduction of the polynomials by the inductive method took about 10 days.

5.1 The polynomials for the projective representations

Recall that under GRH, we have

$$\liminf_{n\to\infty} \inf_{\substack{[K:\mathbb{Q}]=n \\ \operatorname{sign}(K)=(r_1,r_2)}} |\operatorname{disc} K|^{1/n} \geqslant 8\pi e^{\gamma+\frac{\pi}{2}\frac{r_1}{n}} = 44.763\cdots \times (4.810\cdots)^{r_1/n},$$

cf. [Ser75].

We have computed and certified that the field corresponding to the stabiliser of a point of $\mathbb{P}^1(\mathbb{F}_{13})$ via the projective representation attached to 5.6.1.a mod 13 is defined by the polynomial

$$x^{14} - x^{13} - 26x^{11} + 39x^{10} + 104x^9 - 299x^8 - 195x^7 + 676x^6 + 481x^5 - 156x^4 - 39x^3 + 65x^2 - 14x + 1.$$

This polynomial has thus signature $(2, 6)$ and a Galois group that is permutation-isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{13}) \circlearrowleft \mathbb{P}^1(\mathbb{F}_{13})$. Besides, the root discriminant of its root field is

$$(5^{12}13^{13})^{1/14} = 43.002\ldots,$$

which is significantly lower than the estimation

$$8\pi e^{\gamma+\pi/14} = 56.024\cdots$$

for a field of this signature, and even lower than the estimation

$$8\pi e^{\gamma} = 44.763\cdots$$

for any number field of any signature.

Nevertheless, our field is beaten by the record (as of June 2017) from the [LMFDB], namely the $\mathrm{PGL}_2(\mathbb{F}_{13})$-field 14.2.203256043372850100305921 computed by Noam Elkies, whose root discriminant is

$$(2^{26}13^{13})^{1/14} = 39.213\cdots,$$

and by that from the database [KM] (as of June 2017) whose root discriminant is only

$$(2^{8}13^{17})^{1/14} = 33.470\cdots.$$

However, if we move to Galois closures, then our field beats both the aforementioned field from [KM] and Elkies's. Indeed, the root discriminant of the Galois closure of our field is

$$5^{12/13}13^{13/14} = 47.816\cdots,$$

which incidentally is close to $8\pi e^{\gamma}$, whereas it is

$$2^{13/6}13^{167/156} = 69.939\cdots$$

for Elkies's field, and

$$2^{2/3}13^{215/156} = 54.441\cdots$$

for the above field from [KM], and even worse for the other $\mathrm{PGL}_2(\mathbb{F}_{13})$-fields from [KM] and the [LMFDB]. This is due to the fact that our field is tamely ramified at all primes, whereas the others are not. According to [Rob16, p. 14], it is possible that our field is the $\mathrm{PGL}_2(\mathbb{F}_{13})$ field whose Galois closure has the smallest root discriminant.

Similarly, we have computed and certified that the polynomial corresponding to the projective representation attached to 7.8.1.a mod 13 is

$$x^{14} - 52x^7 + 91x^6 + 273x^5 - 364x^4 - 1456x^3 - 455x^2 + 1568x + 1495.$$

This polynomial has the unexpected and intriguing property that all 6 terms from x^{13} to x^8 included are missing; the author does not know of any convincing explanation for this behaviour.

The root discriminant of the root field is

$$(7^{12}13^{11})^{1/14} = 39.775\cdots$$

which is even better than our previous example and narrowly misses beating Elkies's; theorem 6.1.2 below explains that this is because we are dealing with a form which admits a companion, whereas the form was supersingular in the previous example. However, the root discriminant of the Galois closure is

$$7^{12/13}13^{11/12} = 63.271\cdots,$$

which is not as good as our previous example (this is due to the fact that the level is higher) but still beats Elkies's, again thanks to the fact that it is only tamely ramified.

Finally, we have computed and certified that the polynomial

$$x^{42} - 13x^{41} + 70x^{40} - 209x^{39} + 395x^{38} - 1235x^{37} + 8745x^{36} - 32673x^{35} + 41466x^{34} + 23047x^{33} + 117494x^{32} - 1473749x^{31} + 3432505x^{30} + 2534861x^{29} - 8121350x^{28} - 46053615x^{27} + 55119882x^{26} + 3771513x^{25} + 926108685x^{24} + 222895020x^{23} - 7775139729x^{22} - 13813042275x^{21} + 57369301467x^{20} + 104177173023x^{19} - 235503859068x^{18} - 631349403945x^{17} + 789220697001x^{16} + 2415426085387x^{15} - 1368495524968x^{14} - 7976148397256x^{13} + 2486419230610x^{12} + 18312969605213x^{11} - 3490664476058x^{10} - 33337073689065x^{9} + 9634206834816x^{8} + 38121337992357x^{7} - 8827768624685x^{6} - 35949940921273x^{5} + 19912312531x^{4} + 24698337243313x^{3} + 7457815492250x^{2} - 8123634511724x - 4296658258197$$

corresponds to the projective representation attached to 3.22.1.b mod 41; in particular, we have proved its Galois group is permutation-isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{41})$. The computations required for this proof took only 8 hours and required 50GB of RAM thanks to the "unordered cross-ratios" method presented in section 3.3.1 of [Mas16]; as a comparison, on a computer with 512GB of RAM, [Magma]'s function `GaloisProof` hangs after about one hour while attempting to allocate 400GB of RAM when we asked it to perform the same task.

The root discriminant of the root field is

$$(3^{40}41^{39})^{1/42} = 89.533\cdots,$$

whereas its Galois closure has root discriminant

$$3^{40/41}41^{39/40} = 109.131\cdots.$$

These numbers are not as nice as in the previous two examples due to the fields being ramified at the "large" prime $\ell = 41$.

Remark 5.1.1. Polynomials defining a fixed number field are of course never unique; however, the polynomials that we display in this section and in the next one are the output of [Pari/GP]'s function `polredabs`, which makes them canonical.

5.2 The polynomials for the quotient representations

For both of these representations mod 13, we have also computed the polynomials $F_r(x)$ introduced in section 4, and certified that these polynomials are correct thanks to the group cohomology method presented in [Mas16]. We have then computed the Dokchitsers' resolvents, which may be used to determine the image in $\mathrm{GL}_2(\mathbb{F}_{13})$ (up to similarity of course) of Frobenius elements, and in particular to recover the value mod 13 of the coefficients a_p of these forms for huge primes p. All these data are available for download on the author's web page [Mas].

For the representation attached to 5.6.1.a mod 13, the polynomial $F_r(x)$ is

$$\begin{aligned}F_2(x) = {} & x^{56} - 19\,x^{55} + 176\,x^{54} - 1099\,x^{53} + 5292\,x^{52} - 19916\,x^{51} + 53755\,x^{50} - 82979\,x^{49} - 11609\,x^{48} + 418938\,x^{47} - 1351519\,x^{46} + 3570307\,x^{45} \\ & -8104499\,x^{44} + 9946931\,x^{43} + 5331934\,x^{42} - 12684220\,x^{41} - 180933386\,x^{40} + 956990587\,x^{39} - 2345057533\,x^{38} + 2930653050\,x^{37} \\ & -366740868\,x^{36} - 2647967569\,x^{35} - 10686690040\,x^{34} + 66782657110\,x^{33} - 169078436150\,x^{32} + 261459165916\,x^{31} - 253975820897\,x^{30} \\ & +159187764447\,x^{29} - 272743393068\,x^{28} + 1165595337221\,x^{27} - 3256037467741\,x^{26} + 6113796826345\,x^{25} - 8131597368544\,x^{24} \\ & +7180532683571\,x^{23} - 2160263809470\,x^{22} - 5641397045687\,x^{21} + 12758000383973\,x^{20} - 15558252071934\,x^{19} + 12690172501916\,x^{18} \\ & -6215260751330\,x^{17} + 180457670019\,x^{16} + 2797189991937\,x^{15} - 3474577634674\,x^{14} + 4227913001201\,x^{13} - 5838445844387\,x^{12} \\ & +6919193824400\,x^{11} - 5805277968711\,x^{10} + 2648204866489\,x^{9} + 369252764894\,x^{8} - 1933374840137\,x^{7} + 1819874305834\,x^{6} \\ & -1245647904878\,x^{5} + 908803702639\,x^{4} - 675346876626\,x^{3} + 345380525276\,x^{2} - 96857560911\,x + 7979838361.\end{aligned}$$

For the one attached to 7.8.1.a mod 13, it is

$$\begin{aligned}F_2(x) = {} & x^{56} - 14\,x^{55} + 69\,x^{54} - 82\,x^{53} - 396\,x^{52} + 823\,x^{51} + 3351\,x^{50} - 11931\,x^{49} + 8522\,x^{48} - 35835\,x^{47} + 186446\,x^{46} - 8847\,x^{45} - 854460\,x^{44} \\ & -743676\,x^{43} + 4590031\,x^{42} + 7212191\,x^{41} - 22038546\,x^{40} - 38957922\,x^{39} + 49157879\,x^{38} + 243902411\,x^{37} - 180717704\,x^{36} \\ & -988889224\,x^{35} + 704374598\,x^{34} + 4859375083\,x^{33} - 3763415241\,x^{32} - 16386779936\,x^{31} + 21701597191\,x^{30} + 46834006724\,x^{29} \\ & -85332561468\,x^{28} - 70138311949\,x^{27} + 302231735974\,x^{26} - 10052385427\,x^{25} - 632464301217\,x^{24} + 556951211889\,x^{23} + 1081393994453\,x^{22} \\ & -1845293759824\,x^{21} - 358646925616\,x^{20} + 3673731123829\,x^{19} - 1686600977427\,x^{18} - 4103844332008\,x^{17} + 5303152415742\,x^{16} \\ & +2644700341946\,x^{15} - 8175629100848\,x^{14} + 3069957630241\,x^{13} + 5747922498716\,x^{12} - 4528557603372\,x^{11} - 3341692089599\,x^{10} \\ & +6603867688269\,x^{9} - 2399016765221\,x^{8} - 1314878616927\,x^{7} + 1252052945123\,x^{6} - 5862989822\,x^{5} - 159810157800\,x^{4} - 23334202447\,x^{3} \\ & +35386045540\,x^{2} + 9146004182\,x + 973774019.\end{aligned}$$

Finally, we have also managed to obtain a reduced version of the polynomial $F_r(x)$ attached to 3.22.1.b mod 41, thanks to an improvement of our inductive reduction method which we pushed to its limits. This polynomial has degree 336 and its coefficients have about 1000 decimal digits, so we do not reproduce it here. We are currently certifying that this polynomial corresponds to 3.22.1.b mod 41 and computing the Dokchitser resolvents; all these data will also be available on the author's web page [Mas].

6 What to expect in general

6.1 Computation of the root discriminant

We now want to establish a formula that will allow us to predict the value of the root discriminant of the fields that we obtain when we compute the projective representation attached to a form of squarefree level and which admits a companion or is supersingular.

We begin by recalling some well-known relations between the discriminant of a number field, the ramification and splitting behaviour of primes in this field, and the Galois action.

Lemma 6.1.1. *Let $T(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n, $Z = \{z_1, \cdots, z_n\}$ be the set formed by its roots in $\overline{\mathbb{Q}}$, $K = \mathbb{Q}(z_1)$ be the associated number field of degree n, $L = \mathbb{Q}(z_1, \cdots, z_n)$ its Galois closure, and $G = \mathrm{Gal}(L/\mathbb{Q})$ its Galois group. Fix a prime $p \in \mathbb{N}$ and a prime $\mathfrak{P}$ of L above p, and let $I_{\mathfrak{P}} \trianglelefteq D_{\mathfrak{P}} \leqslant G$ be the inertia and decomposition groups of $\mathfrak{P}$. Then the map*

$$\begin{array}{ccc} D_{\mathfrak{P}}\backslash Z & \longrightarrow & \{\text{primes of } K \text{ above } p\} \\ D_{\mathfrak{P}}(g \cdot z_1) & \longmapsto & (g^{-1} \cdot \mathfrak{P}) \cap K \end{array} \qquad (g \in G)$$

is well-defined and bijective. Furthermore, given an orbit $\omega \in D_{\mathfrak{P}}\backslash Z$, the inertial degree $f_{\mathfrak{p}/p}$ of the corresponding prime $\mathfrak{p}$ of K is the number of orbits of ω under $I_{\mathfrak{P}}$, and these orbits all have the same size, which agrees with the ramification index $e_{\mathfrak{p}/p}$ of $\mathfrak{p}$. Finally, if the ramification is tame at p, then the p-adic valuation of the root discriminant of K is $1 - \frac{1}{n}\#(I_{\mathfrak{P}}\backslash Z)$, and that of the root discriminant of L is $1 - \frac{1}{\mathrm{lcm}_{\omega \in I_{\mathfrak{P}}\backslash Z} \#\omega}$.

Examining the action of inertia through a modular Galois representation then leads to the following formulas:

Theorem 6.1.2. *Let $\pi_{f,\mathfrak{l}}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_{\mathfrak{l}})$ be the projective representation attached to a newform $f = q + \sum_{n\geqslant 2} a_n q^n \in \mathcal{N}_k(N,\varepsilon)$ of weight $2 \leqslant k \leqslant \ell+1$, where $\mathfrak{l}$ is a prime of the Hecke field of f above an odd prime ℓ. Suppose that the image of $\pi_{f,\mathfrak{l}}$ is not too small, in that it acts transitively on $\mathbb{P}^1(\mathbb{F}_{\mathfrak{l}})$. Let m be the degree of $\mathfrak{l}$, let K be the number field of degree ℓ^m+1 corresponding via $\pi_{f,\mathfrak{l}}$ to the stabiliser of a point of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{l}})$, and let L be its Galois closure, which is thus the field cut out by $\pi_{f,\mathfrak{l}}$. Assume that N is squarefree and that $\ell \nmid N$. Let M be the conductor of $\varepsilon \bmod \mathfrak{l}$, and for each prime $p \mid M$, let $r_p \in \mathbb{N}$ denote the multiplicative order of the p-part of $(\varepsilon \bmod \mathfrak{l})$. Finally, let N' be the product of the primes $p \neq \ell$ such that the* linear *representation attached to $f \bmod \mathfrak{l}$ is ramified at p, so that $M \mid N' \mid N$. Then the root discriminant of K is*

$$d_K = \ell^{\alpha}\left(\frac{N'}{M}\right)^{\frac{1-1/\ell}{1+1/\ell^m}}\left(\prod_{p\mid M} p^{1-1/r_p}\right)^{\frac{\ell^m-1}{\ell^m+1}}$$

for some $\alpha \in \mathbb{Q}_{>0}$, whereas the root discriminant of L is

$$d_L = \ell^{\beta}\left(\frac{N'}{M}\right)^{1-1/\ell}\prod_{p\mid M} p^{1-1/r_p}$$

for some $\beta \in \mathbb{Q}_{>0}$. Furthermore, if the coefficient a_ℓ of f is not $0 \bmod \mathfrak{l}$ and if $f \bmod \mathfrak{l}$ admits a companion form, then $\pi_{f,\mathfrak{l}}$ is tamely ramified at ℓ and we have

$$\beta = 1 - \frac{\gcd(k-1,\ell-1)}{\ell-1}, \quad \alpha = \frac{\ell^m-1}{\ell^m+1}\beta,$$

whereas if the coefficient a_ℓ of f is $0 \bmod \mathfrak{l}$, then $\pi_{f,\mathfrak{l}}$ is again tamely ramified at ℓ and we have

$$\beta = 1 - \frac{\gcd(k-1,\ell+1)}{\ell+1}, \quad \alpha = \begin{cases} \beta & \text{if } m \text{ is odd,} \\ \frac{\ell^m-1}{\ell^m+1}\beta & \text{if } m \text{ is even.} \end{cases}$$

Remark 6.1.3. The value of N' is not difficult to determine in practice. Indeed, a prime p divides N/N' if and only if there exists an eigenform f' of level N/p such that $f' \bmod \mathfrak{l}' = f \bmod \mathfrak{l}$ for some prime $\mathfrak{l}'$ above ℓ; as a consequence, N' is the product of the primes p such that no such form f' exists.

Remark 6.1.4. The case when the ramification at ℓ is wild is treated in [MT03].

Remark 6.1.5. The image of complex conjugation by $\pi_{f,\mathfrak{l}}$ is similar to $\left[\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right]$ as ℓ is odd, so the signature of K is $\left(2, \frac{\ell^m-1}{2}\right)$ and that of L is $(0, \frac{\#\operatorname{Im}\pi_{f,\mathfrak{l}}}{2})$. This allows us to determine the sign of the discriminants of K and L, should we want to do so.

Proof. Let $\rho = \rho_{f,\mathfrak{l}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$ be the linear representation attached to $f \bmod \mathfrak{l}$, and write d_K and d_L for the root discriminants of K and L.

Let $p \neq \ell$ be a prime dividing N'. By hypothesis, $p \parallel N$ and ρ ramifies at p, so $\rho(I_p)$ fixes a line pointwise by (4.2.6). We thus have

$$\rho|_{I_p} \sim \begin{bmatrix} 1 & \xi \\ & \varepsilon_p \end{bmatrix},$$

where $\varepsilon_p = \det \rho|_{I_p}$ is the p-part of ε mod $\mathfrak{l}$. We now distinguish two cases.

On the one hand, if ε_p is non-trivial, that is to say if $p \mid M$, then by section 2 of [Dia97] we may arrange that $\xi = 0$, so I_p acts on $\mathbb{P}^1(\mathbb{F}_\mathfrak{l})$ via ε_p, whence two orbits formed of a single point (namely 0 and ∞), and $\frac{\ell^m-1}{r_p}$ orbits of size r_p.

On the other hand, if ε_p is trivial, that is to say if $p \mid \frac{N'}{M}$, then ξ is an additive character on I_p with values in $\mathbb{F}_\mathfrak{l}$. As $p \neq \ell$, ξ factors through the tame quotient of I_p; since this quotient is cyclic, the image of ξ is either cyclic of order ℓ or trivial. But ξ cannot be trivial as ρ ramifies at p; therefore, I_p acts on $\mathbb{P}^1(\mathbb{F}_\mathfrak{l})$ by a cyclic group of translations of order ℓ, whence one orbit of size 1 (the point at infinity) and ℓ^{m-1} orbits of size ℓ.

Either way, the ramification is tame at p (which we already knew by the formula (4.2.6) for the Artin conductor), so we can compute the exponent of p in d_K and in d_L thanks to lemma 6.1.1.

We now focus on the image of the inertia at ℓ. We distinguish again two cases.

On the one hand, if f mod $\mathfrak{l}$ is *ordinary*, that is to say if $a_\ell \not\equiv 0 \bmod \mathfrak{l}$, then by [Gro90, proposition 12.1], we have

$$\rho|_{D_\ell} \sim \begin{bmatrix} \chi_\ell^{k-1}\alpha & \xi \\ & \beta \end{bmatrix},$$

where χ_ℓ is the mod ℓ cyclotomic character (the one that tells the action of Galois on the ℓ-th roots of unity), and α and β are unramified characters. Besides, $\xi = 0$ by [Gro90] if f mod $\mathfrak{l}$ admits a companion form. Therefore,

$$\rho|_{I_\ell} \sim \begin{bmatrix} \chi_\ell^{k-1} & \\ & 1 \end{bmatrix}.$$

Therefore, I_p acts on $\mathbb{P}^1(\mathbb{F}_\mathfrak{l})$ by multiplication by the $(k-1)$-th powers of $\mathbb{F}_\ell^*$, so we have two orbits of size 1 and $\frac{\ell^m-1}{\gcd(k-1,\ell-1)}$ orbits of size $\gcd(k-1,\ell-1)$.

On the other hand, if f mod $\mathfrak{l}$ is *supersingular*, that is to say if $a_\ell \equiv 0 \bmod \mathfrak{l}$, then according to section 2.1.2 of [RS01], we have

$$\rho|_{I_\ell} \sim \begin{bmatrix} \psi^{k-1} & \\ & \psi'^{k-1} \end{bmatrix}$$

over $\overline{\mathbb{F}}_\mathfrak{l}$, where ψ and $\psi' = \psi^\ell$ are the two fundamental characters of level 2, which take values in $\mathbb{F}_{\ell^2}^*$.

If m is odd, then this splitting does not occur over $\mathbb{F}_\mathfrak{l}$, so $\rho|_{I_\ell}$ is similar to m copies of

$$\begin{array}{ccccc} \mathbb{F}_{\ell^2}^* & \longrightarrow & \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}) & \simeq & \mathrm{GL}_2(\mathbb{F}_\ell) \\ x & \longmapsto & (y \mapsto xy). & & \end{array} \tag{6.1.6}$$

restricted to the $(k-1)$-th powers of $\mathbb{F}_{\ell^2}^*$. Here, we are using the fact that $\mathbb{F}_{\ell^2}^*$ is cyclic and that two matrices with coefficients in $\mathbb{F}_\mathfrak{l}$ which are similar over $\overline{\mathbb{F}}_\mathfrak{l}$ are already similar over $\mathbb{F}_\mathfrak{l}$. In (6.1.6), the $(\ell+1)$-th powers of $\mathbb{F}_{\ell^2}^*$ act as scalars since they lie in $\mathbb{F}_\ell^*$, so the action of I_ℓ on $\mathbb{P}^1(\mathbb{F}_\ell)$ is equivalent to the action of the $(k-1)$-th powers of copies of an $(\ell+1)$-cycle. We thus have $\frac{\ell^m+1}{(\ell+1)/\gcd(k-1,\ell+1)}$ orbits, all of size $\frac{\ell+1}{\gcd(k-1,\ell+1)}$.

If m is even, then we have the decomposition

$$\rho|_{I_\ell} \sim \psi^{k-1} \otimes \begin{bmatrix} 1 & \\ & \psi^{(\ell-1)(k-1)} \end{bmatrix}$$

over $\mathbb{F}_\mathfrak{l}$. The character $\psi^{(\ell-1)(k-1)}$ is of order $r = \frac{\ell^2-1}{\gcd\left((\ell-1)(k-1),\ell^2-1\right)} = \frac{\ell+1}{\gcd(k-1,\ell+1)}$, and the action of I_ℓ on $\mathbb{P}^1(\mathbb{F}_\mathfrak{l})$ yields two orbits of size 1 and $\frac{\ell^m-1}{r}$ orbits of size r.

Either way, the ramification is tame, and we can again determine the valuation of ℓ in d_K and d_L thanks to lemma 6.1.1. □

Remark 6.1.7. One sees easily that same formulas remain valid for $k = 1$, in which case one has $\alpha = \beta = 0$. Furthermore, the same reasoning can also be used to derive formulas for the discriminant of the fields attached to the *linear* representation $\rho_{f,\mathfrak{l}}$ attached to a newform of any weight $k \leqslant \ell + 1$ if desired.

Of course, we are mainly interested in the cases when the image of $\pi_{f,\mathfrak{l}}$ is $\mathrm{PGL}_2(\mathbb{F}_\ell)$ or $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Given an explicit choice of $f \in \mathcal{N}_k(N,\varepsilon)$ and $\mathfrak{l}$, it is easy to ensure this. Indeed, if it were not the case, then according to Dixon's classification of finite subgroups of $\mathrm{PGL}_2(\overline{\mathbb{F}_\ell})$, either the image of the linear representation $\rho_{f,\mathfrak{l}}$ attached to $f \bmod \mathfrak{l}$ would be contained in a Borel subgroup or in the normaliser of a split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_\ell)$, or the image of $\pi_{f,\mathfrak{l}}$ would be isomorphic to a subgroup of the symmetric group $\mathfrak{S}_4$ or of the alternating group $\mathfrak{A}_5$. In order to rule these cases out, we use the same technique as in section 2 of [Swi72]: The Borel (resp. normaliser of Cartan) case can be ruled out by computing the Fourier coefficients a_p of f for a few primes p, and finding at least one $p \nmid \ell N$ such that $x^2 - a_p x + p^{k-1}$ is irreducible in $\mathbb{F}_\mathfrak{l}[x]$ (resp. a few primes $p \nmid \ell N$ which span $(\mathbb{Z}/\ell N\mathbb{Z})^* \otimes \mathbb{Z}/2\mathbb{Z}$ and such that $a_p \not\equiv 0 \bmod \mathfrak{l}$). Similarly, if $\ell \geqslant 7$, the $\mathfrak{S}_4$ or $\mathfrak{A}_5$ case may be ruled out by exhibiting a prime $p \neq \ell$ such that $a_p^2/p^{k-1} \bmod \mathfrak{l}$ is not a root of $x(x-1)(x-2)(x-4)(x^2-3x+1)$. One then sees if the image of $\pi_{f,\mathfrak{l}}$ is $\mathrm{PSL}_2(\mathbb{F}_\ell)$ or $\mathrm{PGL}_2(\mathbb{F}_\ell)$ by checking whether the values of the mod ℓN character $x \mapsto x^{k-1}\varepsilon(x) \bmod \mathfrak{l}$ are all squares in $\mathbb{F}_l^*$ or not.

6.2 A few examples with trivial nebentypus

In the case where $f \bmod \mathfrak{l}$ has trivial nebentypus, is ordinary, and admits a companion, we get especially small root discriminants when N' is small and $k-1$ and $\ell-1$ have a large common factor. If they do not, for large ℓ the root discriminant of both K and L is asymptotically ℓN. This condition should not be confused with the condition from section 3.1 that $\gcd(k-2,\ell-1)$ be large for $X_H(\ell N)$ to be much smaller than $X_1(\ell N)$. Sadly, these two conditions are rather contradictory (unless $k = 2$ of course, since we do not have to raise the level from N to ℓN in this case), so unfortunately the most interesting examples are the hardest to compute. For instance, of all the examples of newforms with trivial nebentypus, rational coefficients, and which admit a companion listed by David Roberts in table 3.2 of [Rob16], the only case for which we are able to compute the associated Galois representation is for 7.8.1.a mod 13, which we presented in section 5.

When $f \bmod \mathfrak{l}$ is supersingular and has trivial nebentypus, the condition for the root discriminant to drop from the ℓN asymptotic is that $k-1$ and $\ell+1$ have a large common factor, and this seems more compatible with the condition for $X_H(\ell N)$ to have moderate genus. However, for $11 \leqslant \ell \leqslant 41$ we have found no examples of forms of weight $2 \leqslant k \leqslant \ell+1$, squarefree level $N \leqslant 20$ corpime to ℓ and trivial nebentypus which are supersingular mod a prime above ℓ, whose mod ℓ projective representation has big image, and such that $\gcd(k-1,\ell+1) > 1$. This is partly

because having a trivial nebentypus forces $k-1$ to be odd, which makes it harder for its gcd with the even number $\ell+1$ to be nontrivial. We have still found two examples of surjective representations attached to supersingular forms leading to small root discriminants, even though $\gcd(k-1,\ell+1)=1$ in each case:

- The mod $\ell=19$ projective representation attached to

$$3.10.1.b = q + 18q^2 + 81q^3 + O(q^4) \in \mathcal{N}_{10}\big(\Gamma_0(3)\big)$$

  is surjective and this form is supersingular mod 19, whence an example of $\mathrm{PGL}_2(\mathbb{F}_{19})$-field with

$$d_K = (3^{18}19^{19})^{1/20} = 44.078\cdots$$

  and

$$d_L = 3^{18/19}19^{19/20} = 46.432\cdots .$$

  This projective representation also comes from the newform

$$3.12.1.a = q + 78q^2 - 243q^3 + O(q^4) \in \mathcal{N}_{12}\big(\Gamma_0(3)\big).$$

- The mod $\ell=29$ projective representation attached to

$$2.14.1.a = q - 64q^2 - 1836q^3 + O(q^4) \in \mathcal{N}_{14}\big(\Gamma_0(2)\big)$$

  is surjective and this form is supersingular mod 29, whence an example of $\mathrm{PGL}_2(\mathbb{F}_{29})$-field with

$$d_K = (2^{28}29^{29})^{1/30} = 49.500\cdots$$

  and

$$d_L = 2^{28/29}29^{29/30} = 50.617\cdots .$$

  This projective representation also comes from the newform

$$2.18.1.a = q + 256q^2 + 6084q^3 + O(q^4) \in \mathcal{N}_{18}\big(\Gamma_0(2)\big).$$

The corresponding degree $\ell+1$ fields are not part of [KM] nor of the [LMFDB]; according to [Rob16, p.14], it is possible that these fields are the ones of smallest root discriminant with this Galois group, and similarly for their Galois closures. Unfortunately, the genus of the modular curve $X_H(\ell N)$ is respectively $g=43$ and $g=36$ in these examples (no matter which of the two possible newforms we look at), which keeps them out of computational reach at present.

6.3 Supersingular forms with nontrivial nebentypus

As supersingularity is very easy to test, we have run a search for newforms of nontrivial nebentypus that are supersingular modulo at least one prime $\mathfrak{l}$ (of any degree) above ℓ for $\ell \leqslant 41$. We have restricted our search to forms whose level is squarefree, coprime to ℓ, and at most 20 for $\ell \leqslant 13$ and at most 10 for $17 \leqslant \ell \leqslant 41$, and whose (possibly odd) weight ranges from 2 to ℓ included; according to theorem 2.8 of [Edi92], this is equivalent to searching for weights between 2 and $\ell+1$. We have kept the cases for which $d_K \leqslant 8\pi e^\gamma$ or $d_L \leqslant 70$, where as before d_K is the root

discriminant of the field corresponding to the stabiliser of a point of $\mathbb{P}^1(\mathbb{F}_\mathfrak{l})$ and d_L is the root discriminant of its Galois closure.

In most cases, imposing these tight bounds on the root discriminants leads to representations with small image (a similar phenomenon is reported in section 4.5 of [Rob16]), the most frequent case being that the image is contained in the normaliser of a Cartan subgroup. After eliminating these cases, we are left with only two projective representations whose image is either $\mathrm{PGL}_2(\mathbb{F}_\mathfrak{l})$ or $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{l})$:

Galois group	d_K	d_L	Newforms	Genus
$\mathrm{PGL}_2(\mathbb{F}_7)$	$27.269\cdots$	$46.531\cdots$	13.2.4.a, 13.8.4.a	2
$\mathrm{PSL}_2(\mathbb{F}_{37})$	$51.483\cdots$	$52.993\cdots$	3.13.2.b, 3.27.2.a	385

In this table, each line corresponds to a projective representation, and we indicate which supersingular forms found in our search yield this representation. To each form, we associate as in section 3.1 a modular curve $X_H(\ell N)$ whose jacobian contains the corresponding mod $\mathfrak{l}$ linear representation, and we indicate the smallest of the genera of these curves. It is of course not impossible that the projective representation appears in a curve of smaller genus, but we do not know how to construct such a curve, nor if it exists. Sadly, we have not found any example with a prime of degree higher than 1 satisfying the root discriminant bounds.

The first representation is the one attached to the newform

$$13.2.2.a = q + (\zeta_3 - 1)q^2 - (2\zeta_3 - 2)q^3 + O(q^4) \in \mathcal{N}_2(13, \varepsilon)$$

modulo any[2] of the two primes above 7 in $\mathbb{Q}(\zeta_3)$, where ζ_3 is a primitive cube root of 1 and ε sends 2 mod 13 to $-\zeta_3$. As the weight of this form is 2, this representation occurs in the 13-torsion of the genus 2 curve $X_1(13)$, so it is extremely easy to compute it with our algorithms. In fact, the corresponding degree 8 field is already part of [KM].

On the other hand, as far as we know the second example is completely out of computational reach, which is a real pity as it is the first PSL_2 example that we have encountered, and the value of d_L is quite small.

[2]Changing the prime is tantamount to twisting the linear representation in this case.

References

[Asa76] Asai, Tetsuya, **On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution**. Journal of the Mathematical Society of Japan, 1976, vol. 28, no 1, pp. 48–61.

[AL78] Atkin, A. O. L.; Li, Wen Ch'ing Winnie, **Twists of newforms and pseudo-eigenvalues of W-operators**. Invent. Math. 48 (1978), no 3, 221–243.

[CF96] Cassels, J. W. S.; Flynn, E. V., **Prolegomena to a middlebrow arithmetic of curves of genus 2**. London Mathematical Society Lecture Note Series, 230. Cambridge University Press, Cambridge, 1996.

[DvHZ14] Derickx, Maarten; van Hoeij, Mark; Zeng, Jinxiang, **Computing Galois representations and equations for modular curves $X_H(\ell)$**. arXiv:1312.6819

[Dia97] Diamond, Fred; **An extension of Wiles' results**. In **Modular forms and Fermat's last theorem**, 475–489, Springer, New York, 1997.

[DI95] Diamond, Fred; Im, John, **Modular forms and modular curves**. Seminar on Fermat's Last Theorem (Toronto, ON, 19931994), 39–133, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[DS05] Diamond, Fred; Shurman, Jerry, **A First Course in Modular Forms**. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.

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

[Gro90] Gross, Benedict H., **A tameness criterion for Galois representations associated to modular forms (mod p)**. Duke Math. J. 61 (1990), no. 2, 445–517.

[JR] Jones, John W.; Roberts, David P., **Database of local fields**. `https://math.la.asu.edu/~jj/localfields/`

[JR07] Jones, John W.; Roberts, David P., **Galois number fields with small root discriminant**. J. Number Theory 122 (2007), no. 2, pp. 379–407.

[KM] Klüners, Jürgen and Malle, Gunter, **A Database for Number Fields**. `http://galoisdb.math.upb.de/`

[KM07] Khuri-Makdisi, Kamal, **Asymptotically fast group operations on Jacobians of general curves**. Math. Comp. 76 (2007), no 260, 2213–2239.

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

[Li75] Li, Wen-Ch'ing Winnie, **Newforms and functional equations**. Math. Ann., vol 212, no 4, 285–315.

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

[Magma] Bosma, Wieb; Cannon, John; Playoust, Catherine, **The Magma algebra system. I. The user language** J. Symbolic Comput., 24 (1997), 235–265.

[Mas] Mascot, Nicolas, **Modular Galois representations data**. Personal web page, https://www2.warwick.ac.uk/fac/sci/maths/people/staff/mascot/galreps/.

[Mas13] Mascot, Nicolas, **Computing modular Galois representations**. Rendiconti del Circolo Matematico di Palermo, Volume 62, Number 3, 451–476.

[Mas16] Mascot, Nicolas, **Certification of modular Galois representations**. To appear in Mathematics of Computation. arXiv:1312.6418

[MT03] Moon, Hyunsuk; Taguchi, Yuichiro, **Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations**. Doc. Math. Extra Vol. (2003), 641–654.

[Pari/GP] The PARI Group, PARI/GP development version 2.8.0, Bordeaux, 2015, http://pari.math.u-bordeaux.fr/

[RS01] Ribet, Kenneth; Stein, William, **Lectures on Serre's conjectures**. pp. 143–232 in **Arithmetic algebraic geometry**, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI, 2001.

[Rob16] Roberts, David P., $\mathrm{PGL}_2(\mathbb{F}_\ell)$ **number fields with rational companion forms**. arXiv:1611.06628

[SAGE] **SageMath, the Sage Mathematics Software System** (Version 7.3), The Sage Developers, 2016, http://sagemath.org/

[Ser75] Serre, Jean-Pierre, **Minorations de discriminants**. Note of October 1975 published in **Œuvres**, vol. III, pp. 240–243.

[Ser77] Serre, Jean-Pierre, **Modular forms of weight one and Galois representations**, In **Algebraic number fields: L-functions and Galois properties** (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 193–268. Academic Press, London, 1977.

[Swi72] Swinnerton-Dyer, H. P. F., **On ℓ-adic representations and congruences for coefficients of modular forms**. In **Modular functions of one variable, III** (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 155. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.