Compositio Mathematica **118:** 103–122, 1999.

Serre's Conjecture for Imaginary Quadratic Fields

L. M. FIGUEIREDO
Universidade Federal Fluminese, Instituto de Mathematica, Departamento de Geometria, Rua Ma'rio Santos Braza, S/N Valonguinho, CEP 24020-005, Niteroi, RJ, Brazil
e-mail: lmsf@impa.br

(Received: 17 June 1997; accepted in final form: 11 September 1998)

Abstract. We study an analog over an imaginary quadratic field K of Serre's conjecture for modular forms. Given a continuous irreducible representation $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ we ask if ρ is modular. We give three examples of representations ρ obtained by restriction of even representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. These representations appear to be modular when viewed as representations over K, as shown by the computer calculations described at the end of the paper.

Mathematics Subject Classifications (1991): 11F30, 11F67, 11F11, 11R32.

Key words: modular forms, Serre's conjecture.

1. Introduction

In his 1987 article ([8]) Serre conjectured that a continuous irreducible odd representation $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ arises from a normalised cuspidal eigenform f, in the sense that trace $\rho(\mathrm{Frob}_p) = a_p$ and det $\rho(\mathrm{Frob}_p) = \varepsilon(p)p^{k-1}$ for all $p \nmid Nl$, where N, k, ε are respectively the level, weight and character of f. Representations arising in this way are called modular.

He also asserts that ρ should arise from a form of level $N(\rho)$, weight $k(\rho)$ and character $\varepsilon(\rho)$, where the triple $(N(\rho), k(\rho), \varepsilon(\rho))$ is defined by Serre solely in terms of the representation ρ.

Let K be an imaginary quadratic field. We can define mod l cusp forms over K. In view of Serre's conjecture, one might ask whether a continuous irreducible representation $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ is modular.

This is an interesting question when one considers that a necessary condition for a representation ρ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to be modular is that ρ must be odd, but that there is no odd/even distinction for representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

One can also ask if a modular representation ρ of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ arises with the level and weight obtained in a manner similar to that of Serre's conjecture.

An interesting class of examples is provided by continuous representations ρ_K of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ obtained by restriction of representations $\rho_{\mathbb{Q}}$ of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. If $\rho_{\mathbb{Q}}$ is odd then it is (conjecturally) modular and so ρ_K is modular by base change. If $\rho_{\mathbb{Q}}$ is even then it is not modular but nothing is known about ρ_K.

In this paper we give three examples of even Galois representations of $\rho_{\mathbb{Q}}$ to $\mathrm{SL}_2(\bar{\mathbb{F}}_3)$. We calculate the space of cusp forms of weight 2 of suitable level over the fields $K = \mathbb{Q}(\sqrt{-d})$, where $d = 1, 2, 3,$ and 7 for one of the examples and $d = 1$ and 3 for all three examples.

In all cases the representations appear to be modular when viewed as representations over K. Moreover, the level and character of the corresponding cuspidal eigenforms are the values expected in analogy to Serre's conjecture.

2. Reducing to Weight 2

We use the modular symbols method to calculate cusp forms over an imaginary quadratic field K for a given level. This method can only calculate cusp forms of weight 2.

For representations ρ of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ it is a direct consequence of a theorem of A. Ash and G. Stevens that if ρ is modular then it arises with weight 2. More precisely we have the following.

Let $N(\rho)$ and $k(\rho)$ denote, respectively, the level and weight assigned to ρ by Serre (see [8] for the precise definition) and denote by χ the mod l cyclotomic character. The representation ρ will always be assumed continuous and irreducible.

LEMMA 1. *If ρ is modular arising from $S_{k(\rho)}(N(\rho))$ then there is an integer α such that $\rho \otimes \chi^{\alpha}$ arises from $S_{k'}(N(\rho))$ for some k' satisfying* $2 \leqslant k' \leqslant l + 1$.

Proof. It follows from Serre's definition of the weight that there is always a power χ^{α} such that $\rho' = \rho \otimes \chi^{\alpha}$ has weight $2 \leqslant k(\rho') \leqslant l + 1$. Now it suffices to show that ρ' is modular of the same level N.

Let $f \in S_{k(\rho)}(N(\rho))$ be the eigenform giving rise to ρ. Twisting ρ by χ corresponds to applying the operator θ on f and so ρ' is modular arising from $\theta^{\alpha} f$.

The eigenform $\theta^{\alpha} f$ has some weight k', which is probably large, but since ρ' is modular and $k(\rho') \leqslant l + 1$ then there is an eigenform g of weight $k(\rho')$ and level $N(\rho)$ giving rise to ρ' with the same system of eigenvalues as $\theta^{\alpha} f$. This follows from Edixhoven's theorem on the minimality of the weight (Theorem 4.5 of [4]). $\square$

Now using Theorem 3.5 of [1] we have that

LEMMA 2. *If ρ is modular arising from $S_{k(\rho)}(N(\rho))$ then ρ also arises from* $S_2(N(\rho)l^2)$.

Proof. Let $N = N(\rho)$. There is an integer α such that $\rho' = \rho \otimes \chi^{\alpha}$ arises from level N and weight satisfying $2 \leqslant k(\rho') \leqslant l + 1$. This implies that ρ' arises from some eigenform g in $S_2(Nl)$.

We can view the twist operator on modular forms as the twist of a modular form by the character χ. This does not change the weight, but changes the level and the character of the form (see [9, Prop. 3.64]).

Twisting g by $\chi^{-\alpha}$ we get an eigenform $g \otimes \chi^{-\alpha}$ of level $\operatorname{lcm}(N, l^2) = Nl^2$. This form corresponds to $\rho' \otimes \chi^{-\alpha} = \rho$. □

This lemma only guarantees that a modular representation ρ arises with weight 2 and level Nl^2. The following proposition shows exactly when ρ arises with level Nl. We already know this to be the case when $2 \leqslant k(\rho) \leqslant l+1$.

Let us fix some notation first. The notation is the same used in the article [1]. Let $\mathcal{H}$ denote the classical Hecke algebra, which acts on the space $\mathcal{M}_k(\Gamma_1(N))$ of weight k modular forms over $\Gamma_1(N)$.

For $k \geqslant 2$ let $\widetilde{\Omega}_k(\Gamma_1(N))$ be the systems of eigenvalues $\Phi\colon \mathcal{H} \to \bar{\mathbb{F}}_l$ occurring in $\tilde{\mathcal{M}}_k(\Gamma_1(N))$, the space of mod l modular forms of weight k (see [1] for the precise definition).

PROPOSITION 1. *A modular representation ρ arises with weight* 2 *and level Nl if and only if*

$$2 \leqslant k(\bar{\rho}) \leqslant l+1 \quad \text{or} \quad 2 \leqslant k(\bar{\rho} \otimes \chi(\det \bar{\rho})^{-1}) \leqslant l+1,$$

where $\bar{\rho}$ is the restriction of ρ to the inertia group at l.

Proof. Let g be an integer such that $\det \bar{\rho} = \chi^{g+1}$ and let us normalize g such that $1 \leqslant g \leqslant l-1$. We have that $k(\bar{\rho}) \equiv g+2 \bmod (l-1)$.

Let Φ denote the system of eigenvalues corresponding to $\bar{\rho}$. Then ρ arises with weight 2 and level Nl when $\Phi \in \widetilde{\Omega}_2(\Gamma_1(Nl), \chi^g)$. By Theorem 3.5 of [1] we have that

$$\Phi \in \widetilde{\Omega}_2(\Gamma_1(Nl), \chi^g) \Leftrightarrow \Phi \in \widetilde{\Omega}_k(\Gamma_1(N)) \text{ or } \Phi \in \widetilde{\Omega}_{l+1-g}(\Gamma_1(N))^{(g)}$$

where $k = g+2$.

But $\Phi \in \widetilde{\Omega}_k(\Gamma_1(N))$ implies that either $k = l+1$ and $k(\rho) = 2$ or $k(\rho) = k$, by the minimality of the weight. Hence this happens if and only if $2 \leqslant k(\bar{\rho}) \leqslant l+1$.

If $\Phi \in \widetilde{\Omega}_{l+1-g}(\Gamma_1(N))^{(g)}$ then Φ is the gth-twist of a system of eigenvalues in $\widetilde{\Omega}_{l+1-g}(\Gamma_1(N))$. Since twisting Φ corresponds to tensoring ρ by χ, it follows that

$$\Phi \in \widetilde{\Omega}_{l+1-g}(\Gamma_1(N))^{(g)} \Leftrightarrow \rho \otimes \chi^{-g} \quad \text{occurs in } \widetilde{\Omega}_{l+1-g}(\Gamma_1(N)).$$

This is equivalent, by the minimality of the weight, to $k(\bar{\rho} \otimes \chi^{-g}) = l+1-g$, which is equivalent to $k(\bar{\rho} \otimes \chi(\det \bar{\rho})^{-1}) = l+1-g$. Since $1 \leqslant g \leqslant l-1$ it follows that this is equivalent to $2 \leqslant k(\bar{\rho} \otimes \chi(\det \bar{\rho})^{-1}) \leqslant l+1$. □

3. Modular Symbols for $\Gamma_1(N)$

Let K be an imaginary quadratic field and let N be an ideal in $\mathcal{O}_K$. Let

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_K) \mid c \in N,\ d \equiv \varepsilon \bmod N, \ \text{ for some } \ \varepsilon \in \mathcal{O}_K^* \right\}.$$

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

The space of weight 2 cusp forms over K for $\Gamma_1(N)$ is equivalent to the homology space $H_1(\Gamma_1(N)\backslash(\mathcal{H}_3 \cup K \cup \infty), \mathbb{C})$ which can be effectively calculated using modular symbols. For a description of cusp forms of weight 2 over K see [2], Chapter 3.

The modular symbols method was developed in the seventies by Manin, Birch, Swinnerton–Dyer and others. It is described for the rational case in [6]. Grunewald, Mennicke and others extended the method to calculate the homology of the space $H_1(\Gamma_0(N)\backslash(\mathcal{H}_3 \cup K \cup \infty), \mathbb{C})$ when $K = \mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-3})$ and N a prime ideal of degree 1. John Cremona (in [2]) and [3]) extended these calculations for arbitrary ideals in all five Euclideans: $K = \mathbb{Q}(\sqrt{-d})$, where $d = 1, 2, 3, 7$ and 11.

We are interested in calculating mod l cusp forms of weight 2 for $\Gamma_1(N)$ and a given character of $\Gamma_1(N)\backslash\Gamma_0(N)$. These cannot be defined as corresponding to cuspidal harmonic differentials as in characteristic 0 because not all classes lift to characteristic 0 (see comments on section 8). We define here the mod l cusp forms of weight 2 as the homology classes in the homology space $H_1(X^*, \bar{\mathbb{F}}_l)$, where X^* is the manifold with cusps $\Gamma_1(N)\backslash(\mathcal{H}_3 \cup K \cup \infty)$.

In order to do the calculations in this thesis I have rewritten Cremona's program to work with $\Gamma_1(N)$ and arbitrary character and to work over a finite field.

3.1. THE MODULAR SYMBOLS METHOD

In this section we will recall the modular symbols algorithm for $\Gamma_0(N)$. This is described in [6] for cusp forms over $\mathbb{Q}$ and in [2] and [3] for cusp forms over K.

Let K be one of the class number one fields $\mathbb{Q}(\sqrt{-d})$, with $d = 1, 2, 3, 7$ or 11. Let $\mathcal{O}_K$ denote its ring of integers.

Let $\Gamma \subset \mathrm{PGL}_2(\mathcal{O}_K)$ be a subgroup of finite index. Let $X = \Gamma\backslash\mathcal{H}_3$ and denote by X^* its compactification obtained by adjoining the cusps $X^* = \Gamma\backslash(\mathcal{H}_3 \cup K \cup \infty)$. We want to calculate the homology group $H_1(X^*, \bar{\mathbb{F}}_l)$. The algorithm is basically the same as the algorithm to calculate the homology with rational coefficients.

The set of all geodesic paths between cusps form the one-skeleton of a tessellation of X^* by a hyperbolic polyhedra (see [2]). Therefore the homology $H_1(X^*, \partial X, \bar{\mathbb{F}}_l)$ is generated by such paths. Denote by $\{\alpha, \beta\}_\Gamma$ the class in the homology of the path between the two cusps α, β. By abuse of notation we use the same symbol to denote a path and its class in the homology.

Given any $\gamma \in \mathrm{PGL}_2(\mathcal{O}_K)$ denote by (γ) the path $\{\gamma(0), \gamma(\infty)\}_\Gamma$. We call these the distinguished classes. Not all paths $\{\alpha, \beta\}$ are of this form. But any class $\{\alpha, \beta\}$ is a sum of distinguished classes and therefore the homology is generated by the distinguished classes. This is proved in [6] in the rational case. The proof over K is very similar (see [5]). The proof also tells us how to convert arbitrary classes to sums of distinguished classes.

The polyhedra of the tessellation of X^* obtained by geodesic paths between cusps are all transforms of a basic polyhedron B, a Dirichlet fundamental domain for $\mathrm{PGL}_2(\mathcal{O}_K)$.

The subgroup of $\mathrm{PGL}_2(\mathcal{O}_K)$ identifying in pairs the faces of B form a group G_P. The precise shape of B and the group G_P obviously depends on the field K and it has been determined for a number of fields (see [10]).

There are several relations which hold for all paths (γ). These relations come from two different considerations: the indeterminacy in the notation (γ) and the cycles along the faces of B, i.e. by moding out by boundaries of 2-cells.

If a matrix M identifies $\{0, \infty\}$ to $\{0, \infty\}$ we must have $(\gamma) = (\gamma M)$ since these two denote the same path. Analogously if M identifies $\{0, \infty\}$ to $\{\infty, 0\}$ we must have $(\gamma) = -(\gamma M)$.

But

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \{0, \infty\} = \{0, \infty\} \Rightarrow b = 0 \quad \text{and} \quad c = 0.$$

Fix some fundamental unit ε of $\mathcal{O}_K$. The matrices satisfying the equation above are generated by $\left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let us denote this matrix by J.

On the other hand

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \{0, \infty\} = \{\infty, 0\} \Rightarrow a = 0 \quad \text{and} \quad d = 0.$$

These matrices are generated by $\left(\begin{smallmatrix} 0 & 1 \\ \varepsilon & 0 \end{smallmatrix}\right)$, which we will call S.

Thus the first set of relations is

$$(\gamma) + (\gamma S) = 0, \qquad (\gamma) - (\gamma J) = 0.$$

The second set of relations come from moding out the set of (γ) by the boundaries of 2-cells, which correspond to the faces of B. Each face of B determine a relation. For example the triangle with vertices at 0, 1 and ∞ is a face of B for all the fields considered. The edges of this triangle consist of $\{\gamma(0), \gamma(1)\}$ for $\gamma = I$, $\gamma = L$ and $\gamma = L^2$, where $L = \left(\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. It follows that the relation $(\gamma) + (\gamma L) + (\gamma L^2)$ holds for all symbols γ. In general, since the edges of B are the transforms of $\{0, \infty\}$ by the group G_P, then we can determine all such relations by calculating the orbits of G_P on the edges of B.

Let $G = \mathrm{PGL}_2(\mathcal{O}_K)$. Let $C(\Gamma)$ be the $\bar{\mathbb{F}}_l$-vector space with basis the symbols (γ) for each γ in $[G : \Gamma]$. The natural right coset action of G extends by linearity to an action of the group ring $\mathbb{Z}G$ on $C(\Gamma)$.

Let $\mathcal{R}_0$ be the left ideal of $\mathbb{Z}G$ generated by $I + S$, $I - J$ and $I + L + L^2$. Then the symbols (γ) generating the homology are in the kernel of the action of $\mathcal{R}_0$. We are going to consider the ideal $\mathcal{R}$ generated by the union of $\mathcal{R}_0$ and the rest of the

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

relations coming from the faces of B. The exact definition of $\mathcal{R}$ depends on the field.

In order to determine $\mathcal{R}$ one has to describe the group G_P for each field. For a description of $\mathcal{R}$ for the fields considered here see [3]. In the particular case of $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$ we have $\mathcal{R} = \mathcal{R}_0$.

Let Cusp(Γ) be the free abelian group on the cusps of Γ. We have a map $\partial\colon C(\Gamma) \to$ Cusp(Γ) defined by $\partial\colon(\gamma) \mapsto [\gamma(\infty)] - [\gamma(0)]$, where $[\alpha]$ denote the equivalence class of the cusp α.

Now let $B(\Gamma) = C(\Gamma)\mathcal{R}$. Then it is easy to check that $B(\Gamma)$ is in the kernel of ∂. Denote by $Z(\Gamma)$ the kernel of ∂ and by $H(\Gamma)$ the quotient group $Z(\Gamma)/B(\Gamma)$. The algorithm to calculate the homology comes from the following theorem.

THEOREM 1. *The group $H(\Gamma)$ is isomorphic to $H_1(X^*, \bar{\mathbb{F}}_l)$, the isomorphism being given by*

$$\sum n_\gamma(\gamma) \mapsto \sum n_\gamma\{\gamma(0), \gamma(\infty)\}_\Gamma.$$

3.2. MODULAR SYMBOLS FOR $\Gamma_1(N)$

We first need to identify the cosets of $\Gamma_1(N)$ in $\mathrm{PGL}_2(\mathcal{O}_K)$.

LEMMA 3. *Let $\gamma_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} \in \mathrm{PGL}_2(\mathcal{O}_K)$ for $i = 1, 2$. Then γ_1 and γ_2 are in the same left coset of $\Gamma_1(N)$ in $\mathrm{GL}_2(\mathcal{O}_K)$ if and only if there is a $s \in \mathcal{O}_K$ congruent mod N to a unit in $\mathcal{O}_K^*$ and such that $c_1 \equiv sc_2 \bmod N$, $d_1 \equiv sd_2 \bmod N$.*

Proof. Let $\begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \Gamma_1(N)$ such that $\begin{pmatrix} p & q \\ r & s \end{pmatrix}\gamma_2 = \gamma_1$. Then s is congruent mod N to some $\varepsilon \in \mathcal{O}_K^*$ and we have $c_1 \equiv c_2 s \bmod N$, $d_1 \equiv d_2 s \bmod N$.

Conversely, assume $c_1 \equiv c_2 u \bmod N$, $d_1 \equiv d_2 u \bmod N$ for some $u \equiv \varepsilon \bmod N$, $\varepsilon \in \mathcal{O}_K^*$. Let p, q be a solution to the system $pa_2 + qc_2 = a_1$, $pb_2 + qd_2 = b_1$. This has a solution, since γ_2 is invertible. Now let x, y be a solution to the system

$$c_2Nx + a_2Ny = c_1 - uc_2, \qquad d_2Nx + b_2Ny = d_1 - ud_2.$$

Then take $r = yN$ and $s = u + xN$. The matrix $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ is in $\Gamma_1(N)$ and takes γ_2 to γ_1. □

Now consider cosets of $\Gamma_1(N)$ in $\Gamma_0(N)$. Clearly the map from $\Gamma_1(N)\backslash\Gamma_0(N)$ to $(\mathcal{O}_K/N)^*/\mathcal{O}_K^*$ defined by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d$ is an isomorphism. For any $u \in (\mathcal{O}_K/N)^*/\mathcal{O}_K^*$ denote by γ_u the matrix $\gamma_u = \begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}$.

The set of all γ_u with u running through $(\mathcal{O}_K/N)^*/\mathcal{O}_K^*$ is a set of coset representatives for $\Gamma_1(N)$ in $\Gamma_0(N)$.

The matrix γ_u acts on modular symbols for $\Gamma_1(N)$ by $\{\alpha, \beta\} \to \{u\alpha, u\beta\}$.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

Since the homology group $H_1(\Gamma_1(N)\backslash\mathcal{H}_3, \bar{\mathbb{F}}_l)$ is generated by paths $\{\alpha, \beta\}$ this action of γ_u extends to the homology by linearity. If δ is in the homology denote by $\gamma_u\delta$ the action of γ_u on δ.

Now let ε be a character $\varepsilon\colon \Gamma_1(N)\backslash\Gamma_0(N) \to \bar{\mathbb{F}}_l^*$.

Denote by $\mathcal{R}_\varepsilon$ the ideal of $\mathbb{Z}\Gamma_1(N)$ generated by the relations $\gamma_u - \varepsilon(u)I$, for all $u \in (\mathcal{O}_K/N)^*/\mathcal{O}_K^*$.

A cusp form of weight 2 for $\Gamma_1(N)$ with character ε will be defined as the coinvariant space of $H_1(\Gamma_1(N)\backslash\mathcal{H}_3^*, \bar{\mathbb{F}}_l)$ by the character relations. In terms of modular symbols this corresponds to the space $H(\Gamma_1(N))_\varepsilon = \mathcal{R}_\varepsilon\backslash H(\Gamma_1(N))$. This is the maximal quotient space of $H(\Gamma_1(N))$ where $\gamma_u - \varepsilon(u)I$ acts trivially for all $u \in (\mathcal{O}_K/N)^*/\mathcal{O}_K^*$.

The Hecke operators $T_\wp$ for $\wp$ not dividing N are defined as

$$T_\pi\colon \{\alpha, \beta\} \mapsto \sum_{x \bmod \pi} \left\{\frac{\alpha + x}{\pi}, \frac{\beta + x}{\pi}\right\} + \varepsilon(\pi)\{\pi\alpha, \pi\beta\},$$

for some π generating $\wp$.

As with the method for $\Gamma_0(N)$ we calculate the action of the Hecke operators $T_\wp$ on a modular symbols (γ) by first applying the operator to the path $\{\gamma(0), \gamma(\infty)\}$ and then converting the paths back to modular symbols using continued fractions.

3.3. CALCULATING THE SPACE $H(\Gamma_1(N))_\varepsilon$

We could calculate the space $H(\Gamma_1(N))_\varepsilon$ by first calculating the full space $H(\Gamma_1(N))$ and then moding out by the character relations $\mathcal{R}_\varepsilon$. In practice however the number of modular symbols for $\Gamma_1(N)$ quickly becomes astronomical and so we must use a different approach.

It is more practical from a computational point of view to first factor out the space $C(\Gamma_1(N))$ by the character relations $\mathcal{R}_\varepsilon$. This way we can map the space of all $\Gamma_1(N)$ symbols to the space of $\Gamma_0(N)$ symbols, which is much smaller.

One difficulty then is that the boundary map $\partial\colon C(\Gamma_1(N)) \to \mathrm{Cusp}\,(\Gamma_1(N))$ is not well defined on the quotient $\mathcal{R}_\varepsilon\backslash C(\Gamma_1(N))$, *i.e.*, the ideal $\mathcal{R}_\varepsilon$ is not necessarily contained in the kernel of δ.

Let $Z(\Gamma)_\varepsilon$ and $C(\Gamma)_\varepsilon$ denote the quotient by the character relations of $Z(\Gamma)$ and $C(\Gamma)$ respectively. Let $B(\Gamma)_\varepsilon = \mathcal{R}C(\Gamma)_\varepsilon$.

Denote by $\mathrm{Cusp}\,(\Gamma)_\varepsilon$ the quotient of $\mathrm{Cusp}\,(\Gamma)$ by the relations $(\varepsilon(u)[c]-[\gamma_u c])$, where $[c]$ denote the Γ equivalence class of the cusps $K \cup \infty$.

The space we want is $H(\Gamma)_\varepsilon = (Z(\Gamma)/B(\Gamma))_\varepsilon = Z(\Gamma)_\varepsilon/\mathrm{im}(B(\Gamma))$, where $\mathrm{im}(B(\Gamma))$ denotes the image of the ideal $B(\Gamma)$ in $C(\Gamma)_\varepsilon$.

Now consider the following exact sequence $0 \to K_\varepsilon \to C(\Gamma)_\varepsilon \xrightarrow{\partial} \mathrm{Cusp}\,(\Gamma)_\varepsilon$.

In my program I am really calculating the space $K_\varepsilon/B(\Gamma)_\varepsilon$. Note that $Z(\Gamma)_\varepsilon$ maps to the kernel K_ε which induces a map $Z(\Gamma)_\varepsilon/\mathrm{Im}\,(B(\Gamma)) \to K_\varepsilon/B(\Gamma)_\varepsilon$. The two spaces above are the one we want (on the left) and the one we are actually

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

calculating (on the right). Now we have to work out the difference between these two spaces.

Consider the short exact sequence $0 \to \ker \to Z(\Gamma)_\varepsilon \to K_\varepsilon \to \operatorname{coker} \to 0$ which induces

$$\begin{aligned} 0 &\to \ker/\ker \cap \mathrm{Im}\,(B(\Gamma)) \to Z(\Gamma)_\varepsilon/\mathrm{Im}\,(B(\Gamma)) \\ &\to K_\varepsilon/B(\Gamma)_\varepsilon \to \operatorname{coker}/\mathrm{Im}\,(B(\Gamma))_\varepsilon \to 0. \end{aligned}$$

So the two spaces we are considering differ by some kernel and some cokernel which we ought to calculate now.

Consider the exact sequence $0 \to Z(\Gamma) \to C(\Gamma) \to \widetilde{\mathrm{Cusp}}(\Gamma) \to 0$, where $\widetilde{\mathrm{Cusp}}(\Gamma) \subset \mathrm{Cusp}\,(\Gamma)$ is defined as the cokernel of $Z(\Gamma) \to C(\Gamma)$. This sequence induces

$$0 \to Z(\Gamma)^\varepsilon \to C(\Gamma)^\varepsilon \to \widetilde{\mathrm{Cusp}}(\Gamma)^\varepsilon \to Z(\Gamma)_\varepsilon \to C(\Gamma)_\varepsilon \to \widetilde{\mathrm{Cusp}}(\Gamma)_\varepsilon \to 0$$

where the upperscript ε indicates the invariant space by the character relations. But we also have an exact sequence

$$\begin{tikzcd} 0 \arrow[dr] & & & & \\ & K_\varepsilon \arrow[dr] & & & \\ & Z(\Gamma)_\varepsilon \arrow[u] \arrow[r] & C(\Gamma)_\varepsilon \arrow[r] \arrow[dr] & \widetilde{\mathrm{Cusp}}\,(\Gamma)_\varepsilon \arrow[r] \arrow[d] & 0 \\ & & & \mathrm{Cusp}\,(\Gamma)_\varepsilon & \end{tikzcd}$$

and so we have $\widetilde{\mathrm{Cusp}}\,(\Gamma)^\varepsilon \to Z(\Gamma)_\varepsilon \to K_\varepsilon \to \widetilde{\mathrm{Cusp}}\,(\Gamma)_\varepsilon$ which shows that

$$\begin{aligned} &\widetilde{\mathrm{Cusp}}\,(\Gamma)^\varepsilon \twoheadrightarrow \ker \\ &\operatorname{coker} \hookrightarrow \widetilde{\mathrm{Cusp}}\,(\Gamma)_\varepsilon. \end{aligned}$$

That indicates that the ker and coker are only supported on the cusps. Therefore they should correspond to Eisenstein series and we can ignore them in our calculations.

4. Galois Representations Given by Polynomials

Let P be an irreducible polynomial in $\mathbb{Q}[X]$. Let E be the splitting field of P and assume that $G_E = \mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to either $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{PGL}_2(\mathbb{F}_q)$, where q is a power of a prime p. We actually have the following possible cases: $\mathrm{PSL}_2(\mathbb{F}_3) = A_4$, $\mathrm{PGL}_2(\mathbb{F}_3) = S_4$, $\mathrm{PSL}_2(\mathbb{F}_5) = A_5$, $\mathrm{PGL}_2(\mathbb{F}_5) = S_5$, $\mathrm{PSL}_2(\mathbb{F}_9) = A_6$ and $\mathrm{PSL}_2(\mathbb{F}_7) \subset A_7$.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

Embedding $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ with $q = p^a$ into $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ we have a homomorphism $G_E \to \mathrm{PGL}_2(\bar{\mathbb{F}}_p)$, which induces a continuous representation

$$\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to G_E \to \mathrm{PGL}_2(\bar{\mathbb{F}}_p).$$

We will be constructing Galois representation into $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$ by *lifting* projective representations $\bar{\rho}$ given by polynomials. Therefore it is important to know when this representation has a lifting ρ to $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$, *i.e.*, when there is a ρ such that the following diagram is commutative:

$$\begin{tikzcd} \bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \arrow[r] \arrow[dr, "\rho"'] & \mathrm{PGL}_2(\bar{\mathbb{F}}_p) \\ & \mathrm{GL}_2(\bar{\mathbb{F}}_p) \arrow[u] \end{tikzcd}$$

Furthermore, we need to know when this lifting is an even representation.

The obstruction to lifting the representation $\bar{\rho}$ to $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ is given in terms of the Witt invariant $w_2(\mathbb{Q}_E)$ of the quadratic form $Q_E\colon E \to \mathbb{Q}$ given by $x \to \mathrm{trace}_{E/Q}(x^2)$ (see Serre's article [7]).

In this section we prove that the projective representation $\bar{\rho}$ can always be lifted to $\mathrm{GL}_2(\bar{\mathbb{F}}_p)$ and it lifts to an *even* representation if and only if all the roots of P are real numbers. This result will be crucial in our choice of polynomials to test Serre's conjecture over an imaginary quadratic field K.

Let $e\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to S_n$ denote the homomorphism giving the action of the absolute Galois group on the set of roots of P. The map e induces a map on cohomology $e^*\colon H^2(S_n) \to H^2(G_{\mathbb{Q}})$, where $H^2(G_{\mathbb{Q}}) = H^2(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z})$.

A complete description of the groups $H^k(S_n)$ and $H^k(A_n)$, $k = 1, 2$, is given by (see Serre's paper [7], Sect. 1.5):

$$H^1(S_n) = \begin{cases} 0 & \text{if } n = 1, \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } n \geqslant 2, \end{cases}$$

$$H^2(S_n) = \begin{cases} 0 & \text{if } n = 1, \\ (\mathbb{Z}/2\mathbb{Z}) & \text{if } n = 2, 3, \\ (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) & \text{if } n \geqslant 4, \end{cases}$$

$$H^1(A_n) = \begin{cases} 0 & \text{if } n \neq 4, \\ (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) & \text{if } n = 4, \end{cases}$$

$$H^2(A_n) = (\mathbb{Z}/2\mathbb{Z}) \quad \text{if } n \geqslant 4.$$

The nonzero element of $H^1(S_n)$, $n \geqslant 2$ is the signature ε_n of S_n.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

Let s_n be the element of $H^2(S_n)$ corresponding to the central extension

$$1 \to \{\pm 1\} \to \tilde{S}_n \to S_n \to 1$$

where $\tilde{S}_n$ is an extension of S_n characterized by the property that all elements of $\tilde{S}_n$ whose image in S_n are transpositions (respectively, product of transpositions) have order 2 (respectively, have order 4).

The cup product $\varepsilon_n \cdot \varepsilon_n$ is distinct from s_n. If $n = 2, 3$ then $\varepsilon_n \cdot \varepsilon_n$ is the only nonzero element of $H^2(S_n)$ (thus $s_n = 0$), while if $n \geqslant 3$ then s_n is always nonzero and $\{\varepsilon_n \cdot \varepsilon_n, s_n\}$ form a basis of $H^2(S_n)$.

We have that the image of s_n by Res: $H^2(S_n) \to H^2(A_n)$ is the only nonzero element of $H^2(A_n)$, for $n \geqslant 4$.

Both $e^* s_n$ and $w_2(Q_E)$ are elements of $H^2(G_{\mathbb{Q}})$ and we have following formula, which is the main result of [7], $w_2(Q_E) = e^* s_n + (2)(d_E)$.

Note that $(d_E) = (d_P)$, where d_E is the field discriminant and d_P is the discriminant of P, since $d_p = a^2 d_E$, for some $a \in K^*$.

To use Serre's calculation of the Witt invariant we need to know which element in $H^2(A_n)$ (respectively $H^2(S_n)$) corresponds to the central extension in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ of A_n (respectively S_n) embedded in $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$.

Let us analyze the situation in the 6 possible cases.

(1) $S_3 \cong \mathrm{PGL}_2(\mathbb{F}_2)$.
In this case the center is trivial, so $\mathrm{PGL}_2(\mathbb{F}_2) \cong \mathrm{GL}_2(\mathbb{F}_2)$.

(2) $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$, $A_5 \cong \mathrm{PSL}_2(\mathbb{F}_5)$ and $A_6 \cong \mathrm{PSL}_2(\mathbb{F}_9)$.
Let (n, p) denote one of the pairs $(4, 3)$, $(5, 5)$ or $(6, 9)$. Consider the embedding of A_n in $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$,

Denote by a_n the element in $H^2(A_n)$ corresponding to the central extension of $A_n \hookrightarrow \mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ contained in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$. We have two possibilities: a_n is trivial or $a_n = \lceil(s_n)$, as this is the only nonzero element of $H^2(A_n)$ for $n \geqslant 4$.

If $a_n = 0$ then the sequence

$$0 \to \{\pm 1\} \to \mathrm{SL}_2(\bar{\mathbb{F}}_p) \to \mathrm{PSL}_2(\bar{\mathbb{F}}_p) \to 0$$

is split in A_n and so A_n embeds into $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$. The only elements of order 2 in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ for $p \neq 2$ are $\pm I_2$ which project to identity in $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$. So elements with order 2 in A_n map to identity, contradiction with the fact that $A_n \cong \mathrm{PSL}_2(\mathbb{F}_p)$. It follows that $a_n = \mathrm{Res}(s_n)$.

(3) $\mathrm{PGL}_2(\bar{\mathbb{F}}_3) \cong S_4$ and $\mathrm{PGL}_2(\bar{\mathbb{F}}_5) \cong S_5$.
Let (n, p) be one of the pairs $(4, 3)$ or $(5, 5)$. Consider the embedding of S_n in $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$. Let l_n denote the element in $H^2(S_n)$ corresponding to the central extension of S_n in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$. There are four possibilities for l_n: 0, $\varepsilon_n \cdot \varepsilon_n$, s_n, $s_n + \varepsilon_n \cdot \varepsilon_n$, as these are the elements of $H^2(S_n)$ for $n \geqslant 4$.

The first two possibilities have trivial restriction to $H^2(A_n)$. It follows that the extension corresponding to them is trivial on A_n, which cannot be the case here, as we have already seen.

The extension of S_n corresponding to s_n is such that transpositions in S_n lift with order 2 by the description of $\tilde{S}_n$ given before. But elements of order 2 in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ project to identity and so that would imply that transpositions in S_n map to identity in $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ contradiction with $S_n \cong \mathrm{PGL}_2(\mathbb{F}_p)$.

Therefore we must have that the element in $H^2(S_n)$ corresponding to this extension is $s_n + \varepsilon_n \cdot \varepsilon_n$.

LEMMA 4. *Let $\bar{\rho}$ be the Galois representation to $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ corresponding to a polynomial P in the manner described above. In each of the cases where the Galois group of P is A_4, S_4, A_5, S_5 or A_6, where $p = 3, 3, 5, 5$ or 9, respectively, the obstruction to lifting $\bar{\rho}$ to $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ is $\mathrm{obs}(\bar{\rho}) = w_2(Q_E) + (-2)(d_E)$ where E is the splitting field of P, $w_2(Q_E)$ is the Witt invariant and d_E is the discriminant of E.*

Proof. It follows from the calculations we did above that in each of these cases the obstruction to lifting $\bar{\rho}$ is $\mathrm{obs}(\bar{\rho}) = e^*(s_n + \varepsilon_n \cdot \varepsilon_n)$. Note that this is also true in the A_n case since the term $\varepsilon_n \cdot \varepsilon_n$ is trivial in $H^2(A_n)$.

But $e^*(s_n) = w_2(Q_E) - (2)(d_E)$. So

$$\begin{aligned}\mathrm{obs}(\bar{\rho}) &= e^*(s_n) + e^*(\varepsilon_n) \cdot e^*(\varepsilon_n) = w_2(Q_E) - (2)(d_E) + (d_E)(d_E) \\ &= w_2(Q_E) + (2)(d_E) + (-1)(d_E) = w_2(Q_E) + (-2)(d_E). \qquad \square\end{aligned}$$

Now the main theorem:

THEOREM 2. *Let $p > 2$ be a prime integer and let $\bar{\rho}$ be a representation $\bar{\rho}\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ induced by the Galois group of the splitting field E of a monic irreducible polynomial $P \in \mathbb{Z}[X]$. Then $\bar{\rho}$ lifts to a representation $\rho\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ and this lifting is even if and only if E is totally real.*

Proof. Given any character $\chi\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbb{F}}_p^*$ denote by $(\bar{\rho}, \chi)$ the homomorphism

$$(\bar{\rho}, \chi)\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}\backslash \mathrm{GL}_2(\bar{\mathbb{F}}_p) = \mathrm{PGL}_2(\bar{\mathbb{F}}_p) \times \bar{\mathbb{F}}_p^*$$

defined by $(\bar{\rho}, \chi)(g) = (\bar{\rho}(g), \chi(g))$.

Now consider the exact sequence

$$1 \to \{\pm 1\} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p) \xrightarrow{\sigma} \mathrm{PGL}_2(\bar{\mathbb{F}}_p) \times \bar{\mathbb{F}}_p^* \to 1$$

where $\sigma(g) = (\pi(g), \det(g))$. We want to lift $(\bar{\rho}, \chi)$ to a representation ρ to $\mathrm{GL}_2(\bar{\mathbb{F}})$ in the sequence above.

If we can lift $\bar{\rho}$ to some representation ρ of $G_{\mathbb{Q}}$ then clearly $\bar{\rho} = \operatorname{proj}\rho$ and the map $(\bar{\rho}, \det\rho)$ lifts to ρ. Conversely, if there is a character χ such that the map $(\bar{\rho}, \chi)$ lifts to some representation ρ of $G_{\mathbb{Q}}$:

$$\begin{tikzcd}
\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \arrow[r, "(\bar{\rho},\chi)"] \arrow[dr, "\rho"'] & \mathrm{PGL}_2(\bar{\mathbb{F}}_p) \times \bar{\mathbb{F}}_p^* \\
& \mathrm{GL}_2(\bar{\mathbb{F}}_p) \arrow[u]
\end{tikzcd}$$

then ρ is a lifting for $\bar{\rho}$ with determinant χ. So the question is if we can find a character χ such that $(\bar{\rho}, \chi)$ lifts.

Now recall that the obstruction to lifting this map is a cohomology class

$$\operatorname{obs}((\bar{\rho}, \chi)) \in H^2(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Br}_2(G_{\mathbb{Q}}).$$

Denote by $\operatorname{obs}(\bar{\rho})$ the obstruction to lifting $\bar{\rho}: G_{\mathbb{Q}} \to \mathrm{PSL}_2(\bar{\mathbb{F}}_p)$ to $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ and denoted by $\operatorname{obs}(\chi)$ the obstruction to finding a square root for χ, *i.e.* finding a character ϕ such that $\chi = \phi^2$. This is the lifting problem corresponding to the diagram

$$\begin{tikzcd}
& & G_{\mathbb{Q}} \arrow[d, "\phi"'] \arrow[dr, "\chi"] & & \\
1 \arrow[r] & \{\pm 1\} \arrow[r] & \bar{\mathbb{F}}_p^* \arrow[r] & \bar{\mathbb{F}}_p^* \arrow[r] & 1. \\
& & x \arrow[r, mapsto] & x^2 &
\end{tikzcd}$$

We have that $\operatorname{obs}((\bar{\rho}, \chi)) = \operatorname{obs}(\bar{\rho}) + \operatorname{obs}(\chi)$.

It now suffices to prove that there always exist a χ such that $\operatorname{obs}(\bar{\rho}) = -\operatorname{obs}(\chi)$.

Recall that $H^2(G_{\mathbb{Q}}, \mathbb{Z}/2\mathbb{Z}) \hookrightarrow \bigoplus_q H^2(G_{\mathbb{Q}_q}, \mathbb{Z}/2\mathbb{Z})$ and that the 2-torsion of the Brauer group of $\mathbb{Q}_q$, $q \neq \infty$, is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Denote by $\operatorname{obs}_q(\bar{\rho})$ the component of $\operatorname{obs}(\bar{\rho})$ in $H^2(G_{\mathbb{Q}_q}, \mathbb{Z}/2\mathbb{Z})$. Denote by $S(\bar{\rho})$ the finite set of primes q such that $\operatorname{obs}_q(\bar{\rho}) \neq 0$.

Let $G_{\mathbb{Q}}^{\mathrm{ab}}$ denote the maximal abelian quotient of $G_{\mathbb{Q}}$. This is the quotient of $G_{\mathbb{Q}}$ by the closure of $\{aba^{-1}b^{-1} \mid a, b \in G_{\mathbb{Q}}\}$. Since the character χ is a homomorphism then χ is trivial on this set. Thus χ factors through $G_{\mathbb{Q}}^{\mathrm{ab}}$.

By class field theory one has $G_{\mathbb{Q}}^{\mathrm{ab}} \cong \prod_q \mathbb{Z}_q^*$, for all primes q. Therefore we have $\chi = \prod_q \chi_q$, where $\chi_q: \mathbb{Z}_q^* \to \bar{\mathbb{F}}_p^*$.

In terms of the local components χ_q, $\operatorname{obs}_q(\chi) = 0$ if and only if χ_q has a square root. Thus we need a character χ such that χ_q has a square root $\Leftrightarrow q \notin S(\bar{\rho})$.

For $q \notin S(\bar{\rho})$, it suffices to take χ to be trivial. Now we only need to prove that for any prime q there is a character $\chi_q: \mathbb{Z}_q^* \to \bar{\mathbb{F}}_p^*$ which does not have a square root.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

We split the proof in three cases: $q = 2$, $q \neq 2, \infty$ and $q = \infty$.

(1) $q \neq 2, \infty$.

Then $\mathbb{Z}_q^* = \left(1 + q\mathbb{Z}_q\right) \times (\mathbb{Z}/q\mathbb{Z})^*$. It suffices to choose a character χ_q trivial in $(1 + q\mathbb{Z}_q)$ and such that

$$\chi_q \mid_{(\mathbb{Z}/q\mathbb{Z})^*} \text{ does not have a square root.}$$

The set of characters $\{\chi \colon (\mathbb{Z}/q\mathbb{Z})^* \to \bar{\mathbb{F}}_p^*\}$ is a cyclic group of order divisible by 2 when $p > 2$. Choose as $\chi_q \mid_{(\mathbb{Z}/q\mathbb{Z})^*}$ any odd power of the character generating that group.

(2) $q = 2$.

In this case $\mathbb{Z}_2^* = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$. One takes χ_2 such that $\chi_2(-1) = -1$.

(3) $q = \infty$.

χ_∞ is a character $\chi_\infty \colon \{1, c\} \to \bar{\mathbb{F}}_p^*$, where c denotes complex conjugation in $G_{\mathbb{Q}}$. There are only two such characters: the trivial character and the character defined by $\chi_\infty(c) = -1$, which does not have a square root.

Note that since $S(\bar{\rho})$ is finite we only have χ_q nontrivial for a finite number of primes so that the product $\prod_q \chi_q$ makes sense. This proves the first claim of the theorem: that given $\bar{\rho}$ there always exist a character $\chi \colon G_{\mathbb{Q}} \to \bar{\mathbb{F}}_p^*$ such $(\bar{\rho}, \chi)$ lifts.

Assume $\bar{\rho}$ lifts to a representation ρ. By definition ρ is even if and only if $\det \rho(c) = 1$. This is equivalent to $\mathrm{obs}_\infty(\det \rho) = 0$, which is equivalent to $\mathrm{obs}_\infty(\bar{\rho}) = 0$ since $\mathrm{obs}_\infty(\bar{\rho}) = \mathrm{obs}_\infty(\det \rho)$.

The restriction of $\bar{\rho}$ to the decomposition group at ∞ is a homomorphism $\bar{\rho}_\infty \colon \{1, c\} \to \mathrm{PSL}_2(\bar{\mathbb{F}}_p)$, which lifts to $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$ if and only if $\bar{\rho}_\infty(c) = 1$, since if ρ_∞ is a lifting to $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$, $\rho_\infty(c)$ must have order 2, but all elements of order 2 in $\mathrm{SL}_2(\bar{\mathbb{F}}_p)$, $p \neq 2$, project to I in $\mathrm{PSL}_2(\bar{\mathbb{F}}_p)$. It follows that $\det \rho(c) = 1$ if and only if $\bar{\rho}(c) = 1$, which implies that c acts trivially on E, the splitting field of the polynomial P, or equivalently, that E is a totally real field. □

5. Examples

In this Section I describe the examples that have been worked out for testing Serre's conjecture for representations $\rho_K \colon G_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$, where $K = \mathbb{Q}(\sqrt{-d})$, $d = 1, 2, 3$ or 7.

5.1. QUESTION

Let K be an imaginary quadratic field. Let $G_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ and let l be a prime integer. Let $\rho \colon G_K \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ be a continuous irreducible representation.

Define the level $N(\rho)$ as the prime to l part of the Artin conductor of ρ.

For any prime λ of $\mathcal{O}_K$ lying above l we will multiply the level $N(\rho)$ by λ^2. We raise the level in this fashion hoping to find the eigensystem corresponding to ρ

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

with weight 2. We are using the corresponding fact in the classical case as a guide (see Lemma 2).

Let $\det\rho = \varepsilon(\rho)\chi^h$, where χ^h is some power of the mod l cyclotomic character and $\varepsilon(\rho)$ is a character $\varepsilon(\rho)\colon (\mathcal{O}_K/\tilde{N}(\rho)\mathcal{O}_K)^*/\mathcal{O}_K^* \to \bar{\mathbb{F}}_l^*$ and let $\tilde{N}(\rho) = N(\rho)\prod_{\lambda|l}\lambda^2$.

Then we ask

QUESTION 1. *Is there a homology class* $v \in H_1^*(\Gamma_1(\tilde{N}(\rho), \bar{\mathbb{F}}_l)_{\varepsilon(\rho)}$ *such that* v *is a common eigenvector for the Hecke operators and for all prime* $\wp$ *not dividing* $\tilde{N(\rho)}l$ $\operatorname{trace}\rho(\mathrm{Frob}_\wp) = a_\wp$, *where* $a_\wp$ *is the eigenvalue of* v *for the Hecke operator* $T_\wp$.

This question is an analog over K of Serre's conjecture. There are two main differences: one that we reduce the problem to weight 2. The other difference is that we define mod l cusp forms as homology classes with coefficients in $\bar{\mathbb{F}}_l$, not as mod l reduction of characteristic 0 forms.

It would be nice to work out the precise value of $\delta_\lambda = 0, 1, 2$ according to the restriction of ρ to the inertia group at λ, so that the homology class corresponding to ρ would appear with level $N(\rho)\prod_{\lambda|l}\lambda^{\delta_\lambda}$ (see the discussion in Section 2 of the classical case).

The examples worked out in this paper for the fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-7})$ seem to give evidence towards a positive answer to the question.

The examples are all of *even* continuous irreducible representations $\rho\colon G_\mathbb{Q} \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ with $l > 2$. These are guaranteed not to correspond to mod l holomorphic cusp forms over $\mathbb{Q}$. Then we consider the representation $\rho_K\colon G_K = \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$ obtained by restricting ρ to G_K and we try to check whether it corresponds to a mod l cusp form over K, for the imaginary quadratic fields listed above.

Note that *odd* continuous irreducible representations are (conjecturally) modular and so by base change there is a mod l cusp form over K with the same set of eigenvalues. Therefore testing whether the restricted representation ρ_K is modular would be nothing else then testing Serre's conjecture for $\mathbb{Q}$ itself, for which there is already a large amount of evidence. Thus we have only considered even representations ρ.

We have not considered representations into $\mathrm{GL}_2(\bar{\mathbb{F}}_2)$, the reason being that in $\mathbb{F}_2$ there is no even/odd distinction.

The representations ρ of $G_\mathbb{Q}$ are obtained in the following way. Let P be a monic irreducible polynomial with coefficients in $\mathbb{Z}$ and let E be its splitting field in $\bar{\mathbb{Q}}$. Let P have as Galois group one of the groups $\mathrm{PSL}_2(\mathbb{F}_l)$, with $l = 3, 5, 7, 9$ or $\mathrm{PGL}_2(\mathbb{F}_l)$, with $p = 3$ or 5.

We will be looking for polynomials with the following characteristics:

(1) All roots of P are real, so that the corresponding representation ρ is even.
(2) The splitting field E of P has small discriminant, so that ρ is ramified for a small number of (preferably small) primes and thus have a small conductor.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

(3) The Galois group of P is not too small. If $\mathrm{Gal}(E/\mathbb{Q}) \subset S_n$ is too small then the corresponding representation ρ is not irreducible.

In order to find such suitable polynomials a search was conducted at the tables of number fields archived at Bordeaux, available by anonymous ftp from `megrez.math.u − bordeaux.fr`.

Once we find a suitable polynomial P we can calculate the Witt invariant of P and so determine the bad primes for the problem of lifting $\bar{\rho}$. Then we can choose a character χ so that $(\bar{\rho}, \chi): G_{\mathbb{Q}} \to \mathrm{PSL}_2(\bar{\mathbb{F}}_l) \times \bar{\mathbb{F}}_l^*$ lifts to an even representation $\rho: G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_l)$, of determinant χ.

Note that this method do not give us a precise lift. The representation ρ is determined only up to twisting by a character ε such that $\varepsilon^2 = 1$. In particular, we will not be able to tell the precise lift in $\mathrm{GL}_2(\mathbb{F}_l)$ of a given conjugacy class in $\mathrm{PSL}_2(\mathbb{F}_l)$ or $\mathrm{PGL}_2(\mathbb{F}_l)$: In general there will be two possible lifts for each conjugacy class in $\mathrm{PGL}_2(\mathbb{F}_l)$, which we cannot tell apart without further calculations.

Now we need to produce a table of values of trace $\rho(\mathrm{Frob}_{\wp})$ for a number of primes $\wp \in \mathcal{O}_K$ for which ρ is not ramified. For each such prime $\wp$ we can study the ramification of p, the prime of $\mathbb{Q}$ lying below $\wp$, in the splitting field of P and from there easily guess the order of $\mathrm{Frob}_{\wp}$.

6. Examples

So far I have tested representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ arising from the 3 polynomials P_1, P_2 and P_3 listed below, for the fields $K = \mathbb{Q}(\sqrt{-1})$ and $K = \mathbb{Q}(\sqrt{-3})$. The representation coming from P_1 was also tested for the fields $K = \mathbb{Q}(\sqrt{-2})$ and $K = \mathbb{Q}(\sqrt{-7})$. More examples were tested with $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ simply because the calculations involved are smaller (The relation ideal has less relations and also these fields have more units).

In all cases the representations appear to be modular and of the level and character obtained as in Serre's conjecture.

The three polynomials considered were the following:

$$\begin{aligned} P_1 &= x^4 - 7x^2 - 3x + 1 && \mathrm{disc} = 3^2 \times 61^2 \\ P_2 &= x^4 - x^3 - 24x^2 + x + 11 && \mathrm{disc} = 3^4 \times 79^2 \\ P_3 &= x^4 - x^3 - 7x^2 + 2x + 9 && \mathrm{disc} = 163^2 \end{aligned}$$

where disc is the discriminant of the number field defined by the polynomial. All three polynomials have Galois group $\mathrm{PSL}_2(\mathbb{F}_3)$.

The conjugacy classes of the group $\mathrm{SL}_2(\mathbb{F}_3)$ are given in Table I, along with the order of each class and the dimension of the subspace of $\mathbb{F}_{3^2}$ which is fixed by an element of that class. Note that I indicated with the same roman numerals the classes of $\mathrm{SL}_2(\mathbb{F}_3)$ which project to the same class of $\mathrm{PSL}_2(\mathbb{F}_3)$.

In the three cases the calculation of the Witt invariant reveals that there is no obstruction to lifting the associated representation and so all three representations lift to $\mathrm{SL}_2(\mathbb{F}_3)$.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

Table I. Conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_3)$.

Conjugacy class	Representative	Order	Dimension of fixed subspace of $\mathbb{F}_{3^2}$
I1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	2
I2	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$	2	0
II1	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$	4	0
III1	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	3	1
III2	$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$	6	0
IV1	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$	3	1
IV2	$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$	6	0

Now we have to consider the ramification at the ramified primes to tell what the Serre conductor of the respective representations are. Let us analyze case by case.

(1) P_1. The representation is ramified at 3 and 61 and so the conductor is a power of 61. The ramification at 61 is tame and therefore the conductor is either 61 or 61^2.

The image of the decomposition group D_{61} of the prime 61 in $\mathrm{PSL}_2(\mathbb{F}_3)$ has order 3, being generated by an element of one of the two conjugacy classes whose elements have order 3. In either case the two possible lifts are a class whose elements have order 6 which has no fixed subspace and a class whose elements have order 3 and fixes a one-dimensional subspace of $\mathbb{F}_{3^2}$. The former case implies 61 has power 2 in the conductor and the latter case that 61 has power 1 in the conductor.

Despite the fact that we do not know the exact lift to $\mathrm{SL}_2(\mathbb{F}_3)$ we can ensure that there is a lift with power 1 of 61 in the conductor by a simple argument: if the element generating the image of D_{61} in $\mathrm{PSL}_2(\mathbb{F}_3)$ lifts to an element of order 6 then we twist the representation by the quadratic ramified character at 61. That will multiply the element generating D_{61} by -1 which then lies in a class with order 3.

The conductor in this case is $N = 61$.

(2) P_2. The representation is ramified at the primes 3 and 79. The decomposition group at 79 has order 3 and thus by an analogous argument to the previous case we have a lifting to $\mathrm{SL}_2(\mathbb{F}_3)$ with conductor $N = 79$.

(3) P_3. The representation is ramified at 163 only. The decomposition group at 163 has order 3 and so there is a lifting with conductor $N = 163$.

Note that in choosing these polynomials we picked the ones with discriminant p^n or $3p^n$ for some small prime p and such that the ramification at p would ensure that there is a lifting with conductor $N = p$.

All these three representations lift to $\mathrm{SL}_2(\mathbb{F}_3)$ and therefore have determinant 1. Therefore in all three cases the Serre character is $\chi_3^{-1} = \chi_3$.

In Serre's definition for the weight, the cases where a mod l representation ρ has weight 2 all have $\det \rho_{I_l} = \chi_l$.

In our 3 cases, $\det \rho = 1$, and so we would not expect to find the system of eigenvalues corresponding to these representations with weight 2 and level N, the conductor of the representation, except possibly over $\mathbb{Q}(\sqrt{-3})$, where χ_3 is trivial.

In the case of the polynomial P_3 we expect to find the system of eigenvalues with weight 2 and level $3N$, since the representation is unramified at 3, which implies weight $l + 1$.

For each representation we compiled a table with the values of $\mathrm{trace}(\mathrm{Frob}_p)$ for the unramified primes p. It turns out that with these mod 3 representations we can only distinguish two possibilities for the trace of Frobenius.

If the image of Frob_p in $\mathrm{PSL}_2(\mathbb{F}_3)$ has order 2 then it has only one possible lift to $\mathrm{SL}_2(\mathbb{F}_3)$, which has trace 0. If Frob_p has order 3 then it can lift with order 3 or 6, which have traces 1 or -1. We cannot distinguish between the two cases without fixing a precise lift. If Frob_p has order 1 then it again lifts with trace 1 or -1.

Thus in practice the values of $\mathrm{trace}(\mathrm{Frob}_p)$ is a list of zeros and ones, which we check against the eigenvalues for the eigenforms with coefficients in $\mathbb{F}_3$ that were found.

There is one more condition for a given eigenform to correspond to a representation ρ induced by a Galois group over $\mathbb{Q}$: it is that the eigenvalues of a prime p and its conjugate are the same. They must both correspond to the trace of Frobenius of the same rational prime.

In all cases an eigenform was found such that the eigenvalues correspond to the values of $\mathrm{trace}(\mathrm{Frob}_p)$ of the polynomial inducing the representation and such that the eigenvalues of each prime and its conjugate are the same.

7. Tables

Tables II and III contain the results for the three polynomials over the fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{3})$. Each table contains the following:

(1) The list of the first 18 primes $\wp$ in $\mathcal{O}_K$.
(2) The order of Frob_p in $\mathrm{PSL}_2(\mathbb{F}_3)$. This was calculated using PARI.
(3) The calculated eigenvalues of one weight 2 eigenform corresponding to the system of eigenvalues of the representation corresponding to the poynomial.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

Table II. Field $K = \mathbb{Q}(\sqrt{-1})$ and polynomials P_1, P_2 and P_3.

$\wp$	ρ_1 $o(\mathrm{Frob}_p)$	$N = 183$ $a_\wp$	$a_\wp$	ρ_2 $o(\mathrm{Frob}_p)$	$N = 237$ $a_\wp$	$a_\wp$	ρ_3 $o(\mathrm{Frob}_p)$	$N = 489$ $a_\wp$	$a_\wp$
$1+i$	3	1	−1	2	0	0	3	1	−1
$2+i$	3	1	−1	2	0	0	2	0	0
$1+2i$		1	−1		0	0		0	0
$3+2i$	3	1	1	3	−1	−1	2	0	0
$2+3i$		1	1		−1	−1		0	0
$4+i$	3	1	−1	2	0	0	2	0	0
$1+4i$		1	−1		0	0		0	0
$5+2i$	3	−1	1	3	1	−1	3	−1	1
$2+5i$		−1	1		1	−1		−1	1
$6+i$	2	0	0	3	1	1	2	0	0
$1+6i$		0	0		1	1		0	0
$5+4i$	2	0	0	3	−1	1	3	−1	1
$4+5i$		0	0		−1	1		−1	1
7	3	−1	−1	3	−1	−1	3	−1	−1
$7+2i$	2	0	0	3	1	−1	2	0	0
$2+7i$		0	0		1	−1		0	0
$6+5i$	*			3	−1	−1	2	0	0
$5+6i$					−1	−1		0	0

The level of the eigenform is indicated at the top of the column. These eigenforms have character χ_3, which is trivial in the case $K = \mathbb{Q}(\sqrt{-3})$.

The correspondence between the system of eigenvalues of the representation and the eigenform is given by

$$a_\wp = \begin{cases} 0 & \text{if order of } \mathrm{Frob}_p \text{ is } 2, \\ \pm 1 & \text{if order of } \mathrm{Frob}_p \text{ is 1 or 3.} \end{cases}$$

The tables in this paper contain the eigenvalues for the first 18 primes. I actually calculated and checked the correspondence of eigenvalues for more then 150 primes in each case. I also did the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{7})$ for the polynomial P_1.

The results for each field are:

(1) Field $K = \mathbb{Q}(\sqrt{-1})$.

In this case $(\mathcal{O}_K/3\mathcal{O}_k)^*/\mathcal{O}_K^*$ has order 2 and so there is one nontrivial character of level 3 going to $\mathbb{F}_3^*$.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

Table III. Field $K = \mathbb{Q}(\sqrt{-3})$. Notation $w = (1+\sqrt{-3})/2$.

$\wp$	ρ_1 $o(\mathrm{Frob}_p)$	$N = 61$ $a_\wp(F_1)$	ρ_2 $o(\mathrm{Frob}_p)$	$79+79w$ $a_\wp(F_2)$	ρ_3 $o(\mathrm{Frob}_p)$	$163+163w$ $a_\wp(F_3)$
2	3	−1	2	1	3	−1
$2+w$	3	−1	3	−1	3	1
$1+2w$		−1		−1		1
$3+w$	3	1	3	−1	2	0
$1+3w$		1		−1		0
$3+2w$	3	1	3	1	3	1
$2+3w$		1		1		1
5	3	−1	1	1	1	1
$5+w$	3	1	2	0	2	0
$1+5w$		1		0		0
$4+3w$	2	0	3	1	2	0
$3+4w$		0		1		0
$6+w$	3	−1	2	0	3	−1
$1+6w$		−1		0		−1
$5+4w$	$*$	1	3	−1	2	0
$4+5w$		1		−1		0
$7+2w$	3	1	3	1	3	−1
$2+7w$		1		1		−1

In all 3 cases the eigenform corresponding to the representation was found at level $3N$, where N is the Serre conductor of the representation and character χ_3.

A pair of eigenforms was found for each system of eigenvalues. I do not know why there is a pair for each representation and without fixing a precise lift both eigenforms could correspond to ρ_i.

(2) $K = \mathbb{Q}(\sqrt{-3})$.

The group $(\mathcal{O}_K/3\mathcal{O}_k)^*/\mathcal{O}_K^*$ has order 1 and so the character χ_3 is trivial.

The representation ρ_1 appears with weight 2 and level 61, ρ_2 appears with level $79+79(1+\sqrt{-3})/2$ and ρ_3 appear with level $163+163(1+\sqrt{-3})/2$. All with trivial character.

Note that $1+(1+\sqrt{-3})/2$ is the prime of $\mathbb{Q}(\sqrt{-3})$ lying above 3, which is ramified in this field.

(3) $K = \mathbb{Q}(\sqrt{-2})$ and $K = \mathbb{Q}(\sqrt{-7})$.

https://doi.org/10.1023/A:1001739825854 Published online by Cambridge University Press

The group $(\mathcal{O}_K/3\mathcal{O}_k)^*/\mathcal{O}_K^*$ has order 2 for $K = \mathbb{Q}(\sqrt{-2})$ and has order 4 for $K = \mathbb{Q}(\sqrt{-7})$ and so in both cases there is a nontrivial character χ_3.

We tested for P_1 only. The representation ρ_1 appears with level 183 and character χ_3 for both fields.

The primes marked in the tables with a $*$ are the bad primes for the corresponding level. Eigenvalues were not calculated for the bad primes.

8. Final Remarks

An interesting question is whether corresponding modular forms lift to characteristic 0. With the programs used here we cannot calculate $H_1(X^*, \mathbb{C})$ directly: the round-off errors using complex coefficients made the calculations very difficult for the levels considered. Nonetheless we can calculate $H_1(X^*, \mathbb{F}_p)$ for any prime p. I found that in the cases considered, for some values of p there are no eigenforms in $H_1^*(X^*, \mathbb{F}_p)$ with the level and character corresponding to our examples. This shows that the mod 3 eigenforms found do not lift to characteristic zero.

In the calculations above I am only computing traces of Frobenius elements up to a sign. It would be nice to remove this ambiguity by fixing a lift of the projective representation.

Acknowledgement

The work described in this paper was done for my PhD under the supervision of Richard Taylor, to whom I am very grateful.

References

1. Ash, A. and Stevens, G.: Modular forms in characteristic l and special values of their L-functions, *Duke Math. J.* **53** (1986), 849–868.
2. Cremona, J. E.: Modular symbols, PhD thesis, University of Oxford, 1981.
3. Cremona, J. E.: Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields, *Compositio Math.* **51** (1984), 275–323.
4. Edixhoven, B.: The weight in Serre's conjectures on modular forms, *Invent. Math.* **109** (1992), 563–594.
5. Figueiredo, L.: *Serre's Conjecture over Imaginary Quadratic Fields*, PhD thesis, University of Cambridge, 1995.
6. Manin, J. I.: Parabolic points and zeta functions of modular curves, *Math. USSR Izv.* **6**(1) (1972), 19–64.
7. Serre, J.-P.: L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comm. Math. Helv.* **59** (1984), 651–676.
8. Serre, J.-P.: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* **54** (1987), 179–230.
9. Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.
10. Swan, R. G.: Generators and relations for certain special linear groups, *Adv. Math.* **6** (1971), 1–77.