PROVING MODULARITY FOR A GIVEN ELLIPTIC CURVE OVER AN IMAGINARY QUADRATIC FIELD

LUIS DIEULEFAIT, LUCIO GUERBEROFF, AND ARIEL PACETTI

Abstract. We present an algorithm to determine if the L-series associated to an automorphic representation and the one associated to an elliptic curve over an imaginary quadratic field agree. By the work of Harris-Soudry-Taylor, Taylor and Berger-Harcos (cf. [HST93], [Tay94] and [BH]) we can associate to an automorphic representation a family of compatible p-adic representations. Our algorithm is based on Faltings-Serre's method to prove that p-adic Galois representations are isomorphic.

1. Introduction

Modularity for rational elliptic curves was one of the biggest achievements of last century. Little is known for general number fields. In the case of totally real number fields some techniques do apply, but the result is far from being proven. The case of not totally real fields is more intractable to Taylor-Wiles machinery. In this paper we present an algorithm to determine if the L-series associated to an automorphic representation and the one associated to an elliptic curve over an imaginary quadratic field agree or not. The algorithm is based on Faltings-Serre's method to prove isomorphism of p-adic Galois representation. By the work of Harris-Soudry-Taylor, Taylor and Berger-Harcos (cf. [HST93], [Tay94] and [BH]) we can associate to an automorphic representation a family of compatible p-adic representations, and an elliptic curve has such a family of representations as well in the natural way.

The paper is organized as follows: on the first section we present the algorithms (which depend on the residual representations). On the second section we review the results of p-adic representations attached to automorphic forms on imaginary quadratic fields. On the third section we explain Falting-Serre's method on Galois representations. On the fourth section we prove that the algorithm gives the right answer. At last we show some examples and some GP code writen for the examples.

2. Algorithm

Let K be an imaginary quadratic field, $\mathcal{E}$ be an elliptic curve over K and f an automorphic form on $\mathrm{GL}_2(\mathbb{A}_K)$ whose L-series we want to compare. This algorithm answers if the 2-adic Galois representations attached to both objects are isomorphic and if the original L-series are equal. Since these Galois representations come in compatible families, in particular the algorithm determines whether the p-adic

2000 *Mathematics Subject Classification.* Primary: 11G05; Secondary:11F80.
Key words and phrases. Elliptic Curves Modularity.
The second author was supported by a CONICET fellowship.
The third author was partially suported by PICT 2006-00312 and UBACyT X867.

Galois representations are isomorphic or not for any prime p. It depends on the residual image of the elliptic curve representation.

The input in all cases is: K, $\mathcal{E}$, $\mathfrak{n}(\mathcal{E})$ (the conductor of $\mathcal{E}$), $\mathfrak{n}(f)$ (the level of f) and $a_{\mathfrak{p}}(f)$ for some prime ideals $\mathfrak{p}$ to be determined. By $L_{\mathcal{E}}$ we denote the field obtained from K by adding the coordinates of the 2-torsion points of $\mathcal{E}$.

Notation. By $\bar{\mathbb{Q}}$ we denote an algebraic closure of $\mathbb{Q}$. Let K be an imaginary quadratic extension of $\mathbb{Q}$, and α an element of K. By $\bar{\alpha}$ we denote conjugate of α.

Let L/K be field extensions and $\mathfrak{p} \subset \mathcal{O}_K$. For $\mathfrak{q} \subset \mathcal{O}_L$ a prime ideal above $\mathfrak{p}$, we denote $e(\mathfrak{q}|\mathfrak{p})$ the ramification index.

2.1. **Residual image isomorphic to S_3.**

(1) Let $\mathfrak{m}_K \subset \mathcal{O}_K$ be given by $\mathfrak{m}_K := \prod_{\mathfrak{p}|2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)} \mathfrak{p}^{e(\mathfrak{p})}$ where
$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 6 \\ 2e(\mathfrak{p}|2)+1 & \text{if } \mathfrak{p} \mid 2 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$
Compute the ray class group $Cl(\mathcal{O}_K, \mathfrak{m}_K)$.

(2) Identify the character ψ corresponding to the unique quadratic extension of K contained on $L_{\mathcal{E}}$ on the computed basis.

(3) Extend $\{\psi\}$ to a basis $\{\psi, \chi_i\}_{i=1}^n$ of the quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m})$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{n'}$ with $\mathfrak{p}_j \subset \mathcal{O}_K$, $\mathfrak{p}_j \nmid \mathfrak{m}_K$, and with inertial degree 3 on $L_{\mathcal{E}}$ such that
$$\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \rangle_{j=1}^{n'} = (\mathbb{Z}/2\mathbb{Z})^n$$
(where we take any root of the logarithm and identify $\log(\pm 1)$ with $\mathbb{Z}/2\mathbb{Z}$).

(4) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_j}))$ is odd for $1 \le j \le n'$, $\tilde{\rho}_f$ has image isomorphic to C_3 or to S_3 with the same intermediate quadratic field as $\tilde{\rho}_{\mathcal{E}}$. If not, end with output "the two representations are not isomorphic".

(5) Compute a basis $\{\chi_i\}_{i=1}^m$ of cubic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ and a set of ideals $\{\mathfrak{p}_i\}_{i=1}^{m'}$ such that $\psi(\mathfrak{p}_i) = -1$ or $\mathfrak{p}_i$ splits completely on $L_{\mathcal{E}}$ and
$$\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_m(\mathfrak{p}_j))) \rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m.$$

(6) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_j}))$ is even for $1 \le j \le m'$, $\tilde{\rho}_f$ has S_3 image with the same intermediate quadratic field as $\tilde{\rho}_{\mathcal{E}}$. If not, end with output "the two representations are not isomorphic".

(7) Let $K_{\mathcal{E}}$ be the degree two extension of K contained in $L_{\mathcal{E}}$ and $\mathfrak{m}_{K_{\mathcal{E}}} \subset \mathcal{O}_{K_{\mathcal{E}}}$ be given by $\mathfrak{m}_{K_{\mathcal{E}}} := \prod_{\mathfrak{p}|2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)} \mathfrak{p}^{e(\mathfrak{p})}$ where
$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 3 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$
Compute the ray class group $Cl(\mathcal{O}_{K_{\mathcal{E}}}, \mathfrak{m}_{K_{\mathcal{E}}})$.

(8) Identify the character $\psi_{\mathcal{E}}$ corresponding to the cubic extension $L_{\mathcal{E}}$ on the computed basis and extend it to a basis $\{\psi_{\mathcal{E}}, \chi_i\}_{i=1}^m$ of order three characters of $Cl(\mathcal{O}_{K_{\mathcal{E}}}, \mathfrak{m}_{K_{\mathcal{E}}})$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ with $\mathfrak{p}_j \subset \mathcal{O}_K$, $\psi_{\mathcal{E}}(\mathfrak{p}_j) = 1$ and such that
$$\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$$

(where we take any identification of the cubic roots of unity with $\mathbb{Z}/3\mathbb{Z}$). If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_j})) \equiv \mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathfrak{p}_j})) \pmod 2$ for $1 \le j \le m'$, both residual representations are isomorphic. If not, end with output "the two representations are not isomorphic".

(9) Let $\mathfrak{m}_{L_\mathcal{E}} \subset \mathcal{O}_{L_\mathcal{E}}$ be the modulus $\mathfrak{m}_{L_\mathcal{E}} = \prod_{\mathfrak{q} \mid 2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)} \mathfrak{q}^{e(\mathfrak{q})}$ where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 2 \\ 2e(\mathfrak{p}|2)+1 & \text{if } \mathfrak{p} \mid 2. \end{cases}$$

Compute the ray class group $Cl(\mathcal{O}_{L_\mathcal{E}}, \mathfrak{m}_{L_\mathcal{E}})$. Let $\{\chi_i\}_{i=1}^n$ be a basis for its quadratic characters (dual to the ray class group one computed).

(10) Compute the Galois group $\mathrm{Gal}(L_\mathcal{E}/K)$.

(11) (Computing invariant subspaces) Let σ be an order 3 element of $\mathrm{Gal}(L_\mathcal{E}/K)$ and solve the homogeneous system

$$\begin{pmatrix} \log(\chi_1(\mathfrak{a}_1\sigma(\mathfrak{a}_1))) & \dots & \log(\chi_n(\mathfrak{a}_1\sigma(\mathfrak{a}_1))) \\ \vdots & & \vdots \\ \log(\chi_1(\mathfrak{a}_n\sigma(\mathfrak{a}_n))) & \dots & \log(\chi_n(\mathfrak{a}_n\sigma(\mathfrak{a}_n))) \end{pmatrix}$$

Denote by V_σ the kernel.

(12) Take τ an order 2 element of $\mathrm{Gal}(L/K)$ and compute V_τ, the kernel of the same system for τ.

(13) Intersect V_σ with V_τ. Let $\{\chi_i\}_{i=1}^m$ be a basis of the intersection. This gives generators for the $S_3 \times C_2$ extensions.

(14) Compute a set of ideals $\{\mathfrak{p}_i\}_{i=1}^{m'}$ with $\mathfrak{p}_i \subset \mathcal{O}_K$ and $\mathfrak{p}_i \nmid \mathfrak{m}_K$ such that

$$\langle(\log(\chi_1(\tilde{\mathfrak{p}}_j)), \dots, \log(\chi_n(\tilde{\mathfrak{p}}_j)))\rangle_{j=1}^{m'} = (\mathbb{Z}/2\mathbb{Z})^m,$$

where $\tilde{\mathfrak{p}}_i$ is any ideal of $L_\mathcal{E}$ above $\mathfrak{p}_i$.

(15) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(\rho_\mathcal{E}(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $1 \le i \le m$ then the two representations agree on order 6 elements, else end with output "the two representations are not isomorphic".

(16) For σ an order three element, solve the homogeneous system

$$\begin{pmatrix} \log(\chi_1(\mathfrak{a}_1\sigma(\mathfrak{a}_1)\sigma^2(\mathfrak{a}_1))) & \dots & \log(\chi_n(\mathfrak{a}_1\sigma(\mathfrak{a}_1)\sigma^2(\mathfrak{a}_1))) \\ \vdots & & \vdots \\ \log(\chi_1(\mathfrak{a}_n\sigma(\mathfrak{a}_n))\sigma^2(\mathfrak{a}_n)) & \dots & \log(\chi_n(\mathfrak{a}_n\sigma(\mathfrak{a}_n)\sigma^2(\mathfrak{a}_n))) \end{pmatrix}$$

Denote by W_σ such kernel.

(17) Intersect W_σ with V_τ. Let $\{\chi_i\}_{i=1}^t$ be a basis of such subspace. This characters give all the S_4 extensions.

(18) Compute a set of ideals $\{\mathfrak{p}_i\}_{i=1}^{t'}$ with $\mathfrak{p}_i \subset \mathcal{O}_K$ and $\mathfrak{p}_i \nmid \mathfrak{m}_K$ such that

$$\Big\langle(\log(\chi_1(\tilde{\mathfrak{p}}_j)), \dots, \log(\chi_n(\tilde{\mathfrak{p}}_j))), \dots, (\log(\chi_1(\sigma^2(\tilde{\mathfrak{p}}_j))), \dots, \log(\chi_n(\sigma^2(\tilde{\mathfrak{p}}_j))))\Big\rangle_{j=1}^{t'}$$

equals $(\mathbb{Z}/2\mathbb{Z})^t$, where $\tilde{\mathfrak{p}}_i$ is any ideal of $L_\mathcal{E}$ above $\mathfrak{p}_i$.

(19) If $\mathrm{Tr}(\rho_f(\mathfrak{p}_i)) = \mathrm{Tr}(\rho_\mathcal{E}(\mathfrak{p}_i))$ for all $1 \le i \le n$ output "$\rho_f \simeq \rho_\mathcal{E}$". If not output "the two representations are not isomorphic".

(20) If $a_\mathfrak{p}(f) = a_\mathfrak{p}(\mathcal{E})$ for $\mathfrak{p} \mid 2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)$ then $L(f,s) = L(\mathcal{E},s)$.

2.2. **Residual image trivial or isomorphic to C_2.**

(1) Chose prime ideals $\mathcal{P}_i$, $i = 1, 2$ such that 2 has no inertial degree on $\mathbb{Q}[\alpha_i]$, where α_i is a root of $\mathrm{Frob}_{\mathcal{P}_i}$. If $\mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathcal{P}_i})) \neq \mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathcal{P}_i}))$, end with output "the two representations are not isomorphic".
(2) Let $\mathfrak{m}_K \subset \mathcal{O}_K$ be given by $\mathfrak{m}_K := \prod_{\mathfrak{p} \mid 2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)} \mathfrak{p}^{e(\mathfrak{p})}$ where
$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 6 \\ 2e(\mathfrak{p}|2)+1 & \text{if } \mathfrak{p} \mid 2 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$
Compute the ray class group $Cl(\mathcal{O}_K, \mathfrak{m}_K)$.
(3) For each index two subgroup of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ (plus the whole group), take the corresponding quadratic (or trivial) extension L. In L, take the modulus $\mathfrak{m}_L = \prod_{\mathfrak{p} \mid 2\Delta(K)\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}} \mathfrak{p}^{e(\mathfrak{p})}$, where
$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 3 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$
and compute the ray class group $Cl(\mathcal{O}_L, \mathfrak{m}_L)$.
(4) Compute a set of generators $\{\chi_j\}_{j=1}^{n}$ for the cubic characters of $Cl(\mathcal{O}_L, \mathfrak{m}_L)$, and find prime ideals $\{\mathfrak{q}_j\}_{j=1}^{n'}$ of $\mathcal{O}_L$, with $\mathfrak{q}_j \nmid \mathfrak{m}_L$ and such that
$$\langle (\log(\chi_1(\mathfrak{q}_j)), \ldots, \log(\chi_n(\mathfrak{q}_j))) \rangle_{j=1}^{n'} = (\mathbb{Z}/3\mathbb{Z})^n.$$
(5) Consider the collection $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ of all prime ideals of $\mathcal{O}_K$ which are below the prime ideals found on step (3).
(6) If $\mathrm{Tr}(\tilde{\rho}_f(\mathrm{Frob}_{\mathfrak{p}_i})) \equiv 0 \pmod 2$ for each $i = 1, \ldots, m$, then $\tilde{\rho}_f$ has image trivial or isomorphic to C_2. Otherwise, output "the two representations are not isomorphic".
(7) Compute a basis $\{\chi_i\}_{i=1}^{n}$ of quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$.
(8) Compute a set of prime ideals $\{\mathfrak{p}_i \subset \mathcal{O}_K : \mathfrak{p}_i \nmid \mathfrak{m}_K\}_{i=1}^{2^n-1}$ such that
$$\{(\log(\chi_1(\mathfrak{p}_i)), \ldots, \log(\chi_n(\mathfrak{p}_i))\}_{i=1}^{2^n-1} = (\mathbb{Z}/2\mathbb{Z})^n \backslash \{0\}$$
(9) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $i = 1, \ldots, 2^n - 1$, $\rho_{\mathcal{E}}^{ss} \simeq \rho_f^{ss}$. If not, output "the two representations are not isomorphic".
(10) If $a_{\mathfrak{p}}(f) = a_{\mathfrak{p}}(\mathcal{E})$ for $\mathfrak{p} \mid 2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)$ then $L(f, s) = L(\mathcal{E}, s)$.

Remark 1. The algorithm can be slightly improved. In step (8), instead of aiming at the whole C_2^r, we can stop when we reach a *non-cubic* set.

Definition. Let V be a finite dimensional vector space. A subset T of V is called *non-cubic* if each homogeneous polynomial on V of degree 3 that is zero on T, is zero on V.

In particular, the whole space V is non-cubic.

2.3. **Residual image isomorphic to C_3.**

(1) Chose prime ideals $\mathcal{P}_i$, $i = 1, 2$ such that 2 has no inertial degree on $\mathbb{Q}[\alpha_i]$, where α_i is a root of $\mathrm{Frob}_{\mathcal{P}_i}$. If $\mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathcal{P}_i})) \neq \mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathcal{P}_i}))$, end with output "the two representations are not isomorphic".

(2) Let $\mathfrak{m}_K \subset \mathcal{O}_K$ be given by $\mathfrak{m}_K := \prod_{\mathfrak{p} | 2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)} \mathfrak{p}^{e(\mathfrak{p})}$, where

$$e(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \nmid 6 \\ 2e(\mathfrak{p}|2) + 1 & \text{if } \mathfrak{p} \mid 2 \\ \left\lfloor \frac{3e(\mathfrak{p}|3)}{2} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid 3. \end{cases}$$

Compute the ray class group $Cl(\mathcal{O}_K, \mathfrak{m}_K)$.

(3) Identify the character $\psi_{\mathcal{E}}$ corresponding to the cubic Galois extension $L_{\mathcal{E}}$ on the computed basis.

(4) Find a basis $\{\chi_i\}_{i=1}^n$ of the quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{n'}$ with $\mathfrak{p}_j \subset \mathcal{O}_K$, $\mathfrak{p}_j \nmid \mathfrak{m}$, $\psi(\mathfrak{p}_j) \neq 1$ and such that

$$\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \rangle_{j=1}^{n'} = (\mathbb{Z}/2\mathbb{Z})^n$$

(where we take any root of the logarithm and identify $\log(\pm 1)$ with $\mathbb{Z}/2\mathbb{Z}$).

(5) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_j}))$ is odd for $1 \leq j \leq n'$, $\tilde{\rho}_f$ has image isomorphic to C_3. If not, end with output "the two representations are not isomorphic".

(6) Extend $\{\psi_{\mathcal{E}}\}$ to a basis $\{\psi_{\mathcal{E}}, \chi_i\}_{i=1}^m$ of order three characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$. Compute prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ with $\mathfrak{p}_j \subset \mathcal{O}_K$, $\psi_{\mathcal{E}}(\mathfrak{p}_j) = 1$, such that

$$\langle (\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j))) \rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$$

(where we take any root of the logarithm and identify log of the cubic roots of unity with $\mathbb{Z}/3\mathbb{Z}$). If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_j})) \equiv \mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathfrak{p}_j})) \pmod 2$ for $1 \leq j \leq m'$, the two residual representations are isomorphic. If not, end with output "the two representations are not isomorphic".

(7) Apply the previous case, steps (7) to (10), with K replaced by $L_{\mathcal{E}}$.

3. Sources of two-dimensional representations of G_K

Let K be an imaginary quadratic field. We want to consider two-dimensional, irreducible, p-adic representations of the group $G_K := \mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

The first natural source of such representations comes from the action of G_K on the torsion points of an elliptic curve $\mathcal{E}$ defined over K. More precisely, we consider the Tate module $T_p(\mathcal{E})$ which is a free rank two $\mathbb{Z}_p$-module with a G_K-action, thus gives rise to a p-adic representation

$$\rho_{\mathcal{E},p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p).$$

In order to make sure that the Galois representation $\rho_{\mathcal{E},p}$ is absolutely irreducible we will assume that $\mathcal{E}$ does not have Complex Multiplication. The ramification locus of the representation $\rho_{\mathcal{E},p}$ consists of primes of K dividing p together with the set S of primes of bad reduction of $\mathcal{E}$. The family of Galois representations $\{\rho_{\mathcal{E},p}\}$ is a compatible family and has conductor equal to the conductor of the elliptic curve $\mathcal{E}$.

On the other hand, Harris-Soudry-Taylor, Taylor and Berger-Harcos (cf. [HST93], [Tay94] and [BH]) have proved that one can attach compatible families of two-dimensional Galois representations $\{\rho_p\}$ to any regular algebraic cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$, assuming that it has unitary central character ω with $\omega = \omega^c$. As in the case of classical modular forms "to be attached" means that there is a correspondence between the ramification loci of π and the representation ρ_p and also that, at unramified places, the characteristic polynomial of

$\rho_p(\mathrm{Frob}_\mathfrak{p})$ agrees with the Hecke polynomial of π at $\mathfrak{p}$. However, since the method for constructing these Galois representations depends on using a theta lift to link with automorphic forms on $\mathrm{GSp}_4(\mathbb{A}_\mathbb{Q})$, it can not be excluded that the representations ρ_p also ramify at the primes that ramify in $K/\mathbb{Q}$. The precise statement of the result, valid only under the assumption $\omega = \omega^c$, is the following (cf. [Tay94], [HST93] and [BH]):

Theorem 3.1. *Let S be the set of places in K dividing p or where $K/\mathbb{Q}$ or π or π^c ramify. Then there exists an irreducible representation:*

$$\rho_{\pi,p} : G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$$

such that if $\mathfrak{p}$ is a prime of K not in S then $\rho_{\pi,p}$ is unramified at $\mathfrak{p}$ and the characteristic polynomial of $\rho_{\pi,p}(\mathrm{Frob}_\mathfrak{p})$ agrees with the Hecke polynomial of π at $\mathfrak{p}$

Remark 2. Observe that, in particular, if for some prime $\mathfrak{p}$ ramifying in $K/\mathbb{Q}$ we happen to know that $\rho_{\pi,p}$ is unramified at $\mathfrak{p}$, the above theorem does not imply that the trace of $\rho_{\pi,p}(\mathrm{Frob}_\mathfrak{p})$ agrees with the Hecke eigenvalue of π at $\mathfrak{p}$, though it is expected that these two values should agree. It is also expected that there is a conductor for the family $\{\rho_{\pi,p}\}$, i.e., that the conductor should be independent of p as in the case of elliptic curves. The value of this conductor should also agree with the level of π.

Remark 3. Since the families of Galois representations attached to an elliptic curve $\mathcal{E}$ over K and to a cuspidal automorphic representation π by the previous result are both compatible families, if one has for one prime p that $\rho_{\mathcal{E},p} \cong \rho_{\pi,p}$ then the same holds for every prime p.

Remark 4. Even if an automorphic representation π as above has integer eigenvalues and the right weight so that the attached Galois representations "look like" those attached to some elliptic curve, one has to be careful because over imaginary fields such Galois representations may correspond to a "fake elliptic curve" instead. Namely, such a two-dimensional Galois representation of K may correspond to some abelian surface having Quaternionic Multiplication over K, i.e., the action of G_K on the p-adic Tate module of A is isomorphic to two copies of the Galois representation.

Remark 5. At first the image is defined on a finite extension of $\mathbb{Q}_p$. Actually, it can be defined on the ring of integer of an at most degree 4 extension $E_\mathcal{P}$ of $\mathbb{Q}_p$. Furthermore, let v_i, $i = 1, 2$ be two unramified paces of K and let α_i, β_i be the roots of the characteristic polynomial of Frob_{v_i}. If $\alpha_{v_i} \neq \beta_{v_i}$ and, in the case v_i is split, $\alpha_{\overline{v_i}} + \beta_{\overline{v_i}} \neq 0$ then we can take $E = \mathbb{Q}[\alpha_{v_1}, \alpha_{v_2}]$ and $E_\mathcal{P}$ as its completion at any prime above p by Corollary 1 of [Tay94].

4. Faltings-Serre's method

4.1. **First case: the image is absolutely irreducible.** On this section we review Faltings-Serre's ([Ser85]) method by stating the main ideas of [Sch06] (Section 5) on our particular case. Let

$$\rho_i : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to GL_2(\mathbb{Z}_l)$$

be representations for $i = 1, 2$ such that they satisfy:

- They have the same determinant.

- The mod l reductions are absolutely irreducible and isomorphic.
- There exists a prime $\mathfrak{p}$ such that $\mathrm{Tr}(\rho_1(\mathrm{Frob}_\mathfrak{p})) \neq \mathrm{Tr}(\rho_2(\mathrm{Frob}_\mathfrak{p}))$.

We want to give a finite set of candidates for $\mathfrak{p}$. Chose the maximal r such that $\mathrm{Tr}(\rho_1) \equiv \mathrm{Tr}(\rho_2) \pmod{l^r}$, so we obtain a non-trivial map $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_l$ given by

$$\phi(\sigma) \equiv \frac{\mathrm{Tr}(\rho_1(\sigma)) - \mathrm{Tr}(\rho_2(\sigma))}{l^r} \pmod{l}.$$

If we assume that $\tilde{\rho_1} = \tilde{\rho_2}$, we can factor ϕ through $M_2(\mathbb{F}_l) \rtimes \mathrm{Im}(\tilde{\rho_1})$. For doing this,

$$\rho_1(\sigma) = (1 + l^r\mu(\sigma))\rho_2(\sigma)$$

for some $\mu(\sigma) \in M_2(\mathbb{Z}_l)$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Define the map $\varphi : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \mapsto M_2(\mathbb{F}_l) \rtimes \mathrm{Im}(\tilde{\rho_1})$ by

$$\varphi(\sigma) = (\mu(\sigma), \tilde{\rho}_1(\sigma)) \pmod{l}.$$

Then $\phi(\sigma) \equiv \mathrm{Tr}(\mu(\sigma)\tilde{\rho}_1(\sigma)) \pmod{l}$, i.e. $\phi(A, C) = \mathrm{Tr}(AC)$ on $M_2(\mathbb{F}_l) \rtimes \mathrm{Im}(\tilde{\rho_1})$. An easy computation shows that the group structure on the semidirect product corresponds to the action by conjugation, i.e.

$$\mu(\sigma\tau) \equiv \mu(\sigma) + \tilde{\rho}_1(\sigma)^{-1}\mu(\tau)\tilde{\rho}_1(\sigma) \pmod{l}.$$

Let $\tilde{\mu}$ denote the composition of μ with reduction modulo l. The condition $\det(\rho_1) = \det(\rho_2)$ implies that $\mathrm{Im}(\tilde{\mu}) \subset M_2^0(\mathbb{F}_l) := \{M \in M_2(\mathbb{F}_l) : \mathrm{Tr}(M) \equiv 0 \pmod{l}\}$, hence it has order at most l^3.

Assume that $l = 2$ and $\mathrm{Im}(\tilde{\rho}_i) = S_3$, then

$$M_2^0(\mathbb{F}_2) \rtimes S_3 \simeq S_4 \times C_2.$$

This can be proved in different ways, we give an explicit isomorphism for latter considerations. Take the isomorphism between $M_2(\mathbb{F}_2)$ and S_3 given by

$$\begin{aligned} (12) &\mapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), \\ (13) &\mapsto \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right). \end{aligned}$$

Take $\{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\}$ as a basis for $M_2^0(\mathbb{F}_2)$. It is clear that the action of S_3 on the last element is trivial. If we denote v_1, v_2 the first two elements of the basis and v_3 their sum, the action of $\sigma \in S_3$ on the Klein group $C_2 \times C_2$ (spanned by v_1 and v_2) is $\sigma(v_i) = v_{\sigma(i)}$. Since $S_4 \simeq S_3 \ltimes (C_2 \times C_2)$ with the same action as described above we get the desired isomorphism.

Clearly the elements of $S_3 \times \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $\{1\} \times M_2^0(\mathbb{F}_2)$ and $\left\{\sigma \in S_3 \ : \ \sigma^2 = 1\right\} \times \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ go to 0 by ϕ. It can be seen that all the other elements have non-trivial image (which correspond to the elements of order 4 or 6 on $S_4 \times C_2$). So we need to compute all possible extensions of L with Galois group over K isomorphic to $S_4 \times C_2$ and primes $\mathfrak{p} \subset K$ with inertial degree 4 or 6 on each field.

Remark 6. In the proof given above one starts with a $\bmod \ell^r$ congruence between the traces of ρ_1 and ρ_2 and uses the fact that this implies that the two $\bmod \ell^r$ representations are isomorphic. This result is proved in [Ser95] (Theorem 1) but only with the assumption that the residual $\bmod \ell$ representations are absolutely irreducible. In fact, it is false in the residually reducible case, and this is one of the reasons why the above method does not extend to the case of residual image cyclic of order 3. When the residual representations are reducible there are counter-examples to this claim even assuming that they are semi-simple. We thank Professor J.-P. Serre for pointing out the following counter-example to us: take $\ell = 2$ and consider two characters χ and χ' defined $\mod 2^r$ such that they agree $\mod 2^{r-1}$ but not mod 2^r. Then $\chi \oplus \chi$ and $\chi' \oplus \chi'$ are two-dimensional Galois representations defined mod 2^r having the same trace but they are not isomorphic.

4.2. **Second case: the image is a 2-group.** This case was treated on [Liv87], where the author proves the next Theorem:

Theorem 4.1. *Let K be an imaginary quadratic field, S a finite set of primes of K and E a finite extension of $\mathbb{Q}_2$. Denote by K_S the compositum of all quadratic extensions of K unramified outside S and by $\mathcal{P}_2$ the maximal prime ideal of $\mathcal{O}_E$. Suppose $\rho_1, \rho_2 : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}_2(E)$ are continuous representations, unramified outside S, satisfying:*

1. $\mathrm{Tr}(\rho_1) \equiv \mathrm{Tr}(\rho_2) \equiv 0 \pmod{\mathcal{P}_2}$ *and* $\det(\rho_1) \equiv \det(\rho_2) \pmod{\mathcal{P}_2}$.
2. *There exists a set T of primes of K, disjoint from S, for which*
   - *(i) The image of the set* $\{\mathrm{Frob}_t\}$ *in the* ($\mathbb{Z}/2\mathbb{Z}$*-vector space*) $\mathrm{Gal}(K_S/K)$ *is non-cubic.*
   - *(ii)* $\mathrm{Tr}(\rho_1(\mathrm{Frob}_t)) = \mathrm{Tr}(\rho_2(\mathrm{Frob}_t))$ *and* $\det(\rho_1(\mathrm{Frob}_t)) = \det(\rho_2(\mathrm{Frob}_t))$ *for all* $t \in T$.

Then ρ_1 and ρ_2 have isomorphic semi-simplifications.

Proof. See [Liv87]. □

The following result is useful for identifying non-cubic subsets of ($\mathbb{Z}/2\mathbb{Z}$)-vector spaces.

Proposition 4.2. *Let V be a vector space over $\mathbb{Z}/2\mathbb{Z}$. Then a function $f : V \to \mathbb{Z}/2\mathbb{Z}$ is represented by a homogeneous polynomial of degree 3 if and only if $\sum_{I \subset \{0,1,2,3\}} f(\sum_{i \in I} v_i) = 0$ for every subset $\{v_0, v_1, v_2, v_3\} \subset V$.*

Proof. See [Liv87]. □

4.3. **Third case: the image is cyclic of order 3.** This is a mix of the previous two cases. Let E be a finite extension of $\mathbb{Q}_2$ such that its residue field is isomorphic to $\mathbb{F}_2$. Suppose $\rho_1, \rho_2 : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(E)$ are continuous representations such that the residual representations are isomorphic and have image a cyclic group of order 3. Let K_ρ be the fixed field of the residual representations kernel. If we restric the two representations to $\mathrm{Gal}(\bar{\mathbb{Q}}/K_\rho)$, we get:

$$\rho_1, \rho_2 : \mathrm{Gal}(\bar{\mathbb{Q}}/K_\rho) \to \mathrm{GL}_2(E),$$

whose residual representation have trivial image. Hence we are in 2-group case for the field K_ρ and Livne's Theorem 4.1 applies.

5. Proof of the Algorithm

Before giving a proof for each case we make some general considerations. The image of $\tilde{\rho}_{\mathcal{E}}$ is isomorphic to the Galois group $\mathrm{Gal}(L_{\mathcal{E}}/K)$. If $\mathcal{E}(K)$ has a two torsion point, its image is a 2-group. If not, assume (via a change of variables) that the elliptic curve has equation

$$\mathcal{E} : y^2 = x^3 + a_2 x^2 + a_4 x + a_6$$

and denote by α, β, γ the roots of $x^3 + a_2x^2 + a_4x + a_6$. Using elementary Galois theory it can be seen that $L_{\mathcal{E}} = K[\alpha-\beta]$. Furthermore, using elementary symmetric functions, it can be seen that $\alpha - \beta$ is a root of the polynomial

$$x^6 + x^4(6a_4 - 2a_2^2) + x^2(a_2^4 - 6a_2^2a_4 + 9a_4^2) + 4a_6a_2^3 - 18a_6a_4a_2 + 4a_4^3 - a_4^2a_2^2 + 27a_6^2.$$

If this polynomial is irreducible over K, the image of $\tilde{\rho}_{\mathcal{E}}$ is isomorphic to S_3 while if it is reducible, the image is isomorphic to C_3.

Note that under the isomorphism between S_3 and $\mathrm{GL}_2(\mathbb{F}_2)$ given on the previous section, the order 1 or 2 elements of S_3 have even trace while the order 3 ones have odd trace.

In the case where the image is not a 2-group, we need to prove that the image lies (after conjugation) on an extension E of $\mathbb{Q}_2$ with residual field $\mathbb{F}_2$.

Theorem 5.1. *If $\mathcal{E}$ has no Complex Multiplication, then we can chose split primes of K, $\mathcal{P}_i$, $i = 1, 2$ such that if $\alpha_{\mathcal{P}_i}, \beta_{\mathcal{P}_i}$ denote the roots of the characteristic polynomial of $\mathrm{Frob}_{\mathcal{P}_i}$, then the field $E = \mathbb{Q}[\alpha_{\mathcal{P}_i}]$ has inertial degree 1 at 2 and $\alpha_{\bar{\mathcal{P}}_i} + \beta_{\bar{\mathcal{P}}_i} \neq 0$. In particular, if $\mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathcal{P}_i})) = \mathrm{Tr}(\rho_{\pi,2}(\mathcal{P}_i))$ then by Taylor's argument (see Remark 5), $\mathrm{Im}(\tilde{\rho}_{\pi,2}) \subset \mathrm{GL}_2(\mathbb{F}_2)$.*

Proof. Since $\mathcal{E}$ has no Complex Multiplication, if F is any quadratic field extension of $\mathbb{Q}_2$, the set of primes $\mathcal{P}$ such that $\mathbb{Q}_2[\alpha_{\mathcal{P}}] = F$ has positive density (see for example Exercise (3) of [Ser68]). Also, the set of primes $\mathcal{P}$ such that $\alpha_{\mathcal{P}} + \beta_{\mathcal{P}} = 0$ has density zero (since $\mathcal{E}$ has no complex multiplication, see [Ser66]), so we can find primes $\mathcal{P}$ such that $\mathbb{Q}_2[\alpha_{\mathcal{P}}] = F$ and $\alpha_{\bar{\mathcal{P}}} + \beta_{\bar{\mathcal{P}}} \neq 0$. The fields F_1 and F_2 obtained adding the roots of the polynomials $x^2 + 14$ and $x^2 + 6$ to $\mathbb{Q}_2$ are two ramified extensions of $\mathbb{Q}_2$. Their composition is a degree 4 field extension (since the prime 2 is totally ramified on the composition of these extensions over $\mathbb{Q}$). Since the set of primes innert on K have density zero, we can chose prime ideals $\mathcal{P}_1$ and $\mathcal{P}_2$ whose extensions of $\mathbb{Q}_2$ are isomorphic to F_1 and F_2. $\square$

Actually we search for the first two primes such that 2 has no inertial degree on the extension obtained adding to $\mathbb{Q}$ the roots of their Frobenius automorphisms.

The first step of the algorithm is to prove that the residual representations are indeed isomorphic so as to apply Faltings-Serre's method. In doing this we need to compute all extensions of a fixed degree (2 or 3 in our case) with prescribed ramification. Since we deal with abelian extensions, we can use class field theory.

Theorem 5.2. *If L/K is an abelian extension unramified outside the set of places $\{\mathfrak{p}_i\}_{i=1}^n$ then there exists a modulus $\mathfrak{m} = \prod_{i=1}^n \mathfrak{p}_i^{e(\mathfrak{p}_i)}$ such that $\mathrm{Gal}(L/K)$ corresponds to a subgroup of the ray class group $Cl(\mathcal{O}_K, \mathfrak{m})$.*

Since we are interested in the case K an imaginary quadratic field, all the ramified places of L/K are finite ones, hence $\mathfrak{m}$ is an ideal on $\mathcal{O}_K$. A bound for $e(\mathfrak{p})$ is given by the following result.

Proposition 5.3. *Let L/K be an abelian extension of prime degree p. If $\mathfrak{p}$ ramifies on L/K, then*

$$\begin{cases} e(\mathfrak{p}) = 1 & \text{if } \mathfrak{p} \nmid p \\ 2 \leq e(\mathfrak{p}) \leq \left\lfloor \frac{pe(\mathfrak{p}|p)}{p-1} \right\rfloor + 1 & \text{if } \mathfrak{p} \mid p. \end{cases}$$

Proof. See [Coh00] Proposition 3.3.21 and Proposition 3.3.22. □

To distinguish representations, given a character ψ of a ray class field we need to find a prime ideal $\mathfrak{p}$ with $\psi(\mathfrak{p}) \neq 1$. Let ψ be a character of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ of prime order p. Take any branch of the logarithm over $\mathbb{C}$ and identify $\log(\{\xi_p^i\})$ with $\mathbb{Z}/p\mathbb{Z}$ in any way (where ξ_p denotes a primitive p-th root of unity).

Proposition 5.4. *Let K be a number field, $\mathfrak{m}_K$ a modulus and $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ the ray class field for $\mathfrak{m}_K$. Let $\{\psi_i\}_{i=1}^n$ be a basis of order p characters of $Cl(\mathcal{O}_K, \mathfrak{m})$ and $\{\mathfrak{p}_j\}_{j=1}^{n'}$ be prime ideals of $\mathcal{O}_K$ such that*

$$\langle \log(\psi_1(\mathfrak{p}_j)), \ldots, \log(\psi_n(\mathfrak{p}_j))\rangle_{j=1}^{n'} = (\mathbb{Z}/p\mathbb{Z})^n.$$

Then for every non trivial character ψ of $Cl(\mathcal{O}_K, \mathfrak{m})$ of order p, $\psi(\mathfrak{p}_j) \neq 1$ for some $1 \leq j \leq n$.

Proof. Suppose that $\psi(\mathfrak{p}_j) = 1$ for $1 \leq j \leq m$. Since $\{\psi_i\}_{i=1}^n$ is a basis, there exists exponents ε_i such that

$$\psi = \prod_{i=1}^n \psi_i^{\varepsilon_i}$$

Taking logarithm and evaluating at $\mathfrak{p}_j$ we see that $(\varepsilon_1, \ldots \varepsilon_n)$ is a solution of the homogeneous system

$$\begin{pmatrix} \log(\psi_1(\mathfrak{p}_1)) & \ldots & \log(\psi_n(\mathfrak{p}_1)) \\ \vdots & & \vdots \\ \log(\psi_1(\mathfrak{p}_m)) & \ldots & \log(\psi_n(\mathfrak{p}_m)) \end{pmatrix}.$$

Since $\{(\log(\psi_1(\mathfrak{p}_j)), \ldots, \log(\psi_n(\mathfrak{p}_j)))\}_{j=1}^m$ span $(\mathbb{Z}/p\mathbb{Z})^n$, the matrix has maximal rank, hence $\varepsilon_i = 0$ and ψ is the trivial character. □

Remark 7. A set of prime ideals satisfying the conditions of the previous Proposition always exists by Tchebotarev's density theorem.

5.1. **Residual image isomorphic to S_3.**

Remark 8. If the residual representation is absolutely irreducible, we can apply a descent result (see Corollaire 5 in [Ser95], which can be applied because the Brauer group of a finite field is trivial) and conclude that since the traces are all in $\mathbb{F}_2$ the representation can be defined (up to isomorphism) as a representation with values on a two-dimensional $\mathbb{F}_2$-vector space. Thus, the image can be assumed to be contained in $\mathrm{GL}_2(\mathbb{F}_2)$ and because of the absolute irreducibility assumption we conclude that the image has to be isomorphic to S_3.

Furthermore, we have the following result,

Theorem 5.5. *If the image is absolutely ireducible, then the field E can be taken to be $\mathbb{Q}_2$.*

Proof. This follows from the same argument as the previous Remark. See also Corollary of [CSS97], page 256. □

Remark 9. Once we prove that the residual representation of $\rho_{\pi,2}$ has image greater than C_3 we automatically know that it can be defined on $\mathrm{GL}_2(\mathbb{Z}_2)$.

We have the 2-adic Galois representations $\rho_{\mathcal{E}}$ and ρ_f and we want to prove that they are isomorphic. We start by proving that the reduced representations are isomorphic. For doing this we compute all quadratic extensions of K using Class Field theory and Proposition 5.3. Let $K_{\mathcal{E}}$ denote the quadratic extension of K contained on $L_{\mathcal{E}}$. Following the ideas of step (5) of the previous case, we can prove that L_f (the fixed field of the kernel of ρ_f) contains no quadratic extension of K or contains $K_{\mathcal{E}}$ (note that an ideal with inertial degree 3 on $L_{\mathcal{E}}$ splits on $K_{\mathcal{E}}$). This is done on steps $(1)-(4)$.

Remark 10. Let $P(x)$ denote the degree 3 polynomial in $K[x]$ whose roots are the x-coordinates of the points of order 2 of $\mathcal{E}$. The fact that the splitting field of $P(x)$ is an S_3 extension allows us to compute how primes decompose on $K_{\mathcal{E}}$ knowing how they decompose on the cubic extension K_P of K obtained by adjoining any root of $P(x)$. The factorization as well as the values of $\psi(\mathfrak{p})$ are given by the next table:

$\mathfrak{p}\mathcal{O}_{K_P}$	$\mathfrak{p}\mathcal{O}_{K_{\mathcal{E}}}$	$\mathfrak{p}\mathcal{O}_{L_{\mathcal{E}}}$	$\psi(\mathfrak{p})$
$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{q}_1\mathfrak{q}_2$	$\mathfrak{t}_1\ldots\mathfrak{t}_6$	1
$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}$	$\mathfrak{t}_1\mathfrak{t}_2\mathfrak{t}_3$	-1
$\mathfrak{p}$	$\mathfrak{q}_1\mathfrak{q}_2$	$\mathfrak{t}_1\mathfrak{t}_2$	1

Proof. The last two cases are clear (since the inertial degree is multiplicative and it is at most 3). The not so trivial case is the first one. Since $L_{\mathcal{E}}/K$ is Galois, $\mathfrak{p}\mathcal{O}_{L_{\mathcal{E}}}$ has 3 or 6 prime factors. Assume

$$\mathfrak{p}\mathcal{O}_{L_{\mathcal{E}}} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3. \tag{1}$$

Then it must be the case that (after relabeling the ideals if needed) if σ denotes one order three element in $\mathrm{Gal}(L_{\mathcal{E}}/K)$, $\sigma(\mathfrak{q}_1) = \mathfrak{q}_2$ and $\sigma^2(\mathfrak{q}_1) = \mathfrak{q}_3$. Since the decomposition groups $D(\mathfrak{q}_i|\mathfrak{p})$ have order 2 and are conjugates of each other by powers of σ, they are disjoint and they are all the order 2 subgroups of S_3. Since K_P is a degree 2 subextension of $L_{\mathcal{E}}$, it is the fixed field of an order 2 subgroup. Without loss of generality, assume K_P is the fixed field of $D(\mathfrak{q}_1|\mathfrak{p})$. If we intersect equation (1) with $\mathcal{O}_{K_P}$ we get

$$\mathfrak{p}\mathcal{O}_{K_P} = (\mathfrak{q}_1 \cap \mathcal{O}_{K_P})(\mathfrak{q}_2 \cap \mathcal{O}_{K_P})(\mathfrak{q}_3 \cap \mathcal{O}_{K_P}).$$

We are assuming that $(\mathfrak{q}_i \cap \mathcal{O}_{K_P}) \neq (\mathfrak{q}_j \cap \mathcal{O}_{K_P})$ if $i \neq j$. Let τ be the non trivial element on $D(\mathfrak{q}_1|\mathfrak{p})$, so τ acts trivially on K_P. In particular, τ fixes $\mathfrak{q}_2 \cap \mathcal{O}_{K_P}$ and $\tau(\mathcal{O}_{L_{\mathcal{E}}}) = \mathcal{O}_{L_{\mathcal{E}}}$ then $\tau(\mathfrak{q}_2) = \tau((\mathfrak{q}_2 \cap \mathcal{O}_{K_P})\mathcal{O}_{L_{\mathcal{E}}}) = \mathfrak{q}_2$ which contradicts that $D(\mathfrak{q}_1|\mathfrak{p}) \cap D(\mathfrak{q}_2|\mathfrak{p}) = \{1\}$. $\square$

Next we need to discard the C_3 case. Let $\mathfrak{m}_K$ be as described on step (1) of the algorithm, and $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ be the ray class field. Suppose that $\tilde{\rho}_f$ has image isomorphic to C_3. Let χ be (one of) the cubic character of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ corresponding to L_f. Let $\{\chi_i\}_{i=1}^m$ be a basis of cubic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$. We look for prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ that are inert on $K_{\mathcal{E}}$ or split completely on $L_{\mathcal{E}}$ (that is, they have order 1 or 2 on S_3 and in particular have even trace for the residual representation $\tilde{\rho}_{\mathcal{E}}$) and such that $\langle(\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_m(\mathfrak{p}_j)))\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$. There exists such ideals by Tchebotarev's density Theorem. By Proposition 5.4, there exists an index i_0 such that $\chi(\mathfrak{p}_{i_0}) \neq 1$, hence $\mathrm{Tr}(\tilde{\rho}_f(\mathfrak{p}_{i_0})) \equiv 1 \pmod 2$ while $\mathrm{Tr}(\tilde{\rho}_{\mathcal{E}}(\mathfrak{p}_{i_0})) \equiv 0 \pmod 2$. Step (6) discards this case.

Once we know that $\tilde{\rho}_f$ has S_3 image with the same quadratic subfield as $\tilde{\rho}_{\mathcal{E}}$, we take $K_{\mathcal{E}}$ as the base field and proceed in the same way as the previous case. This is done on steps (7) and (8).

At this point we already decided whether the two residual representations are isomorphic or not. If they are, we can apply Faltings-Serre's method explained on the previous section. We look for quadratic extensions $\tilde{L}$ of L unramified outside $\mathfrak{m}_L$ such that its normal closure is isomorphic to S_4 or $S_3 \times C_2$.

Applying Faltings-Serre's method, we need to compute all fields $\tilde{L}$ with Galois group $\mathrm{Gal}(\tilde{L}/K) \simeq S_4 \times C_2$ in the S_3 case and $\mathrm{Gal}(\tilde{L}/K) \simeq A_4 \times C_2$ in the C_3 case. The group $S_4 \times C_2$ fits in the exact sequences

$$1 \to C_2 \times C_2 \to S_4 \times C_2 \to S_3 \times C_2 \to 1$$

and

$$1 \to C_2 \to S_4 \times C_2 \to S_4 \to 1.$$

The group $A_4 \times C_2$ fits in the exact sequence

$$1 \to C_2 \times C_2 \to A_4 \times C_2 \to C_3 \times C_2 \to 1.$$

Every element of order 4 or 6 on $S_4 \times C_2$ maps to an element of order 4 on S_4 or to an element of order 6 on $S_3 \times C_2$ under the previous surjections, while any element of order 6 on $A_4 \times C_2$ maps to an element of order 6 on $C_3 \times C_2$. We can restrict ourselves to compute normal extensions of L with Galois group S_4 or $S_3 \times C_2$ in the S_3 case and normal extensions of L with Galois group $C_3 \times C_2$ on the C_3 case. Note that in all cases the extensions are obtained by computing the normal closure of a quadratic extension.

Let $\mathfrak{m}_L$ be a modulus on L invariant under the action of $\mathrm{Gal}(L/K)$. Then $\mathrm{Gal}(L/K)$ has an action on $Cl(\mathcal{O}_L, \mathfrak{m}_L)$ and it induces an action on the set of characters of the group. Concretely, if ψ is a character on $Cl(\mathcal{O}_L, \mathfrak{m}_L)$ and $\sigma \in \mathrm{Gal}(L/K)$, $\sigma.\psi = \psi \circ \sigma$.

Lemma 5.6. *If ψ is a character on $Cl(\mathcal{O}_L, \mathfrak{m}_L)$ that corresponds to the quadratic extension $L[\sqrt{\alpha}]$ and $\sigma \in \mathrm{Gal}(L/K)$ then $\sigma^{-1}.\psi$ corresponds to $L[\sqrt{\sigma(\alpha)}]$.*

Proof. The character is characterized by its value on non-ramified primes. Let $\mathfrak{p}$ be a non-ramified prime on $L[\sqrt{\alpha}]/L$. It splits on $L[\sqrt{\alpha}]$ if and only if $\psi(\mathfrak{p}) = 1$. If $\mathfrak{p}$ does not divide the fractional ideal α, this is equivalent to α being a square modulo $\mathfrak{p}$. But for $\sigma \in \mathrm{Gal}(L/K)$, α is a square modulo $\mathfrak{p}$ if and only if $\sigma(\alpha)$ is a square modulo $\sigma(\mathfrak{p})$ hence the extension $L[\sqrt{\sigma(\alpha)}]$ corresponds to the character $\sigma^{-1}.\psi$. □

Proposition 5.7. *Let L/K be a Galois extension with $\mathrm{Gal}(L/K) \simeq S_3$ and ψ a quadratic character of $Cl(\mathcal{O}_L, \mathfrak{m}_L)$ with $\mathfrak{m}_L$ as above.*

1. *The quadratic extension of L corresponding to ψ is Galois if and only if $\sigma.\psi = \psi$ for all $\sigma \in \mathrm{Gal}(L/K)$.*
2. *The quadratic extension of L corresponding to ψ has normal closure isomorphic to S_4 if and only if the elements fixing ψ form an order 2 subgroup and $(\psi)(\sigma.\psi) = \sigma^2.\psi$, where σ is any order 3 element in $\mathrm{Gal}(L/K)$.*

Proof. Let $L[\sqrt{\alpha}]$ be a quadratic extension of L. The normal closure (with respect to K) is the field

$$\tilde{L} = \prod_{\sigma \in \mathrm{Gal}(L/K)} L[\sqrt{\sigma(\alpha)}]$$

(where by the product we mean the smallest field containing all of them inside $\bar{\mathbb{Q}}$). In particular $\mathrm{Gal}(\tilde{L}/L)$ is an abelian 2-group. By the previous proposition, if $L[\sqrt{\alpha}]$ corresponds to the quadratic character ψ then the other ones correspond to the characters $\sigma.\psi$ where $\sigma \in \mathrm{Gal}(L/K)$.

The first assertion is clear. To prove the second one, the condition $(\psi)(\sigma.\psi) = \sigma^2\psi$ and ψ being fixed by an order 2 subgroup implies that $[\tilde{L} : L] = 4$. Hence the group $\mathrm{Gal}(\tilde{L}/K)$ fits in the exact sequence

$$1 \to C_2 \times C_2 \to \mathrm{Gal}(\tilde{L}/K) \to S_3 \to 1.$$

In particular $\mathrm{Gal}(\tilde{L}/K)$ is isomorphic to the semidirect product $S_3 \ltimes (C_2 \times C_2)$, with the action given by a morphism $\Theta : S_3 \to GL_2(\mathbb{F}_2)$. Its kernel is a normal subgroup, hence it can be $GL_2(\mathbb{F}_2)$ (i.e. the trivial action), $\langle\sigma\rangle$ (the order 3 subgroup) or trivial. The condition on the stabilizer of ψ forces the image of Θ to contain an order 3 element, hence the kernel is trivial. Up to inner automorphisms, there is a unique isomorphism from $GL_2(\mathbb{F}_2)$ to itself (and morphisms that differ by an inner automorphism give isomorphic groups) hence $\mathrm{Gal}(\tilde{L}/K) \simeq S_4$ as claimed. ☐

Remark 11. On the S_4 case of the last proposition, the condition on the action of σ is necessary. Consider the extension $L = \mathbb{Q}[\xi_3, \sqrt[3]{2}]$ where ξ_3 is a primitive third root of unity. It is a Galois degree 6 extension of $\mathbb{Q}$ with Galois group S_3. Take as generators for the Galois group the elements σ, τ given by

$$\begin{array}{lcl} \sigma : \xi_3 \mapsto \xi_3 & \text{and} & \sigma : \sqrt[3]{2} \mapsto \xi_3\sqrt[3]{2} \\ \tau : \xi_3 \mapsto \xi_3^2 & \text{and} & \tau : \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{array}$$

The extension $L\left[\sqrt{1+\sqrt[3]{2}}\right]$ is clearly fixed by σ, but its normal closure has degree 8 over L since $\sqrt{1+\xi_3^2\sqrt[3]{2}}$ is not on the field $L\left[\sqrt{1+\sqrt[3]{2}}, \sqrt{1+\xi_3\sqrt[3]{2}}\right]$ as can be easily checked.

To compute all such extensions, we use Class Field Theory and Proposition 5.7. To compute the $S_3 \times C_2$ extensions we follow the method of the C_3 case. The only difference is that we check for invariance under an order 3 element plus invariance under an order 2 element. This is done on steps $(11) - (15)$.

At last, we need to compute the quadratic extensions whose normal closure has Galois group isomorphic to S_4. Using the second part of Proposition 5.7, we need to compute quadratic characters χ such that $\chi(\sigma.\chi)(\sigma^2.\chi) = 1$ (where σ denotes an order three element of $\mathrm{Gal}(L/K)$) and also whose fixed subgroup under the action of $\mathrm{Gal}(L/K)$ has order 2. Let S denote the set of all such characters. Since σ does not act trivially on elements of S, we find that χ, $\sigma.\chi$ and $\sigma^2.\chi$ are three different elements of S that give the same normal closure. Then we can write S as a disjoint union of three sets. Furthermore, since σ acts transitively (by multiplication on the right) on the set of order 2 elements of S_3, we see that

$$S = V_\tau \cup V_{\tau\sigma} \cup V_{\tau\sigma^2}$$

where V_τ denotes the quadratic characters of S invariant under the action of τ and the union is disjoint. Hence each one of these sets is in bijection with all extensions $\tilde{L}$ of L. We compute one subspace and use Proposition 5.4 on this subspace, noting that the elements of order 4 correspond to primes that are inert on any of the three extensions of L (corresponding to χ, $\sigma.\chi$ and $\sigma^2.\chi$) hence we consider not one prime above $\mathfrak{p} \subset \mathcal{O}_K$ but all of them. This is done on steps $(16) - (19)$.

5.2. **Trivial residual image or residual image isomorphic to C_2.** The first step is to decide if we can take E to be an extension of $\mathbb{Q}_2$ with residue field $\mathbb{F}_2$ so as to apply Livne's Theorem 4.1. Once this is checked, the algorithm is divided into two parts. Let $\rho_{\mathcal{E}}, \rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to \mathrm{GL}_2(\mathbb{Z}_2)$ be given, with the residual image of $\rho_{\mathcal{E}}$ being either trivial or isomorphic to C_2. Steps (2) to (6) serve to the purpose of seeing whether ρ_f has also trivial or C_2 residual image or not. Note that the output of step (6) does not say that the residual representations are actually the same, but they have isomorphic semisimplifications (in this case it is equivalent to say that the traces are even). For example, there can be isogenous curves, one of which has trivial residual image and the other has C_2 residual image.

Suppose we computed the ideals of steps $(2) - (5)$ and $\tilde{\rho}_f$ has even trace on the Frobenius of these elements. We claim that ρ_f has residual image either trivial or C_2. Suppose on the contrary that ρ_f has residual image isomorphic to C_3. Let L_2/K be the cyclic extension of K corresponding (by Galois theory) to the kernel of $\tilde{\rho}_f$. This corresponds to a cubic character χ of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$. An easy calculation shows that if $\mathfrak{p} \subset \mathcal{O}_K$ is a prime ideal not dividing $\mathfrak{m}$, then $\chi(\mathfrak{p}) = 1$ if and only if $\mathrm{Tr}(\tilde{\rho}_f(\mathrm{Frob}_{\mathfrak{p}})) = 0$. This implies that $\chi(\mathfrak{p}_j) = 1$ for each $j = 1, \ldots, m$. But χ is a non-trivial character, then by Proposition 4.6 we get a contradiction.

Similarly, suppose that the residual image of ρ_2 is S_3. Let L_2/K be the S_3 extension of K corresponding (by Galois theory) to the kernel of $\tilde{\rho}_f$, and M_2/K its unique quadratic subextension. The extension L_2/M_2 corresponds to a cubic character χ of $Cl(\mathcal{O}_{M_2}, \mathfrak{m}_{M_2})$ and the proof follows the previous case.

Steps $(7)-(10)$ check if the representations are indeed isomorphic once we know that the traces are even using Theorem 4.1. We need to find a finite set of primes T, which will only depend on K, and check that the representations agree at those primes. In the algorithm and in the theorem, we identify the group $\mathrm{Gal}(K_S/K)$ with the group of quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m})$. In step (7), we compute the image of $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K_S/K)$ via this isomorphism and compute enough prime ideals so as to get a non-cubic set of $\mathrm{Gal}(K_S/K)$. Then the representations are isomorphic if and only if the traces at those primes agree.

5.3. **Residual image isomorphic to C_3.** Let K be an imaginary quadratic field and let

$$\rho_{\mathcal{E}}, \rho_f : \mathrm{Gal}(\bar{\mathbb{Q}}/K) \to GL_2(\mathbb{Q}_2)$$

be the Galois representations attached to $\mathcal{E}$ and f respectively.

The first step is to decide if we can take E to be an extension of $\mathbb{Q}_2$ with residue field $\mathbb{F}_2$. Once this is checked, we need to prove that the residual representation $\tilde{\rho}_f$ has image isomorphic to C_3. For doing this we start proving that it has no order 2 elements on its image. If such an element exists, there exists a degree 2 extension of K unramified outside $2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)$. We use Proposition 5.3 and Class Field Theory to compute all such extensions. Once a basis of the quadratic characters is chosen, we apply Proposition 5.4 to find a set of ideals such that for any quadratic extension, (at least) one prime $\mathfrak{q}$ on the set is inert on it. Since the residual image is isomorphic to a subgroup of S_3, $\tilde{\rho}_f(\mathfrak{q})$ has order exactly 2. In particular its trace is even. If $\mathrm{Tr}(\tilde{\rho}_f(\mathfrak{p}))$ is odd at all primes, $\mathrm{Im}(\tilde{\rho}_f)$ contains no order 2 elements. Also since $\mathrm{Tr}(\mathrm{id}) \equiv 0 \pmod 2$ we see that $\tilde{\rho}_f$ cannot have trivial image hence its image is isomorphic to C_3. This is done on steps (2) to (5) of the algorithm.

To prove that $\tilde{\rho}_f$ factors through the same field as $\tilde{\rho}_{\mathcal{E}}$ we compute all cubic Galois extensions of K. This can be done using Class Field Theory again, and this explains the choice of the modulus on step (1), so as to be used for both quadratic and cubic extensions. Note that the characters χ and χ^2 give raise to the same field extension. If $\psi_{\mathcal{E}}$ denotes (one of) the cubic character corresponding to $L_{\mathcal{E}}$, we extend it to a basis $\{\psi_{\mathcal{E}}, \chi_i\}_{i=1}^m$ of the cubic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ and find a set of prime ideals $\{\mathfrak{p}_j\}_{j=1}^{m'}$ such that $\langle(\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j)))\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$ and $\psi_{\mathcal{E}}(\mathfrak{p}_j) = 1$ for all $1 \leq j \leq m'$.

If χ is a cubic character corresponding to L_f, $\chi = \psi_{\mathcal{E}}^{\varepsilon}\varkappa$, where $\varkappa = \prod_{i=1}^n \chi_i^{\varepsilon_i}$. If $\varkappa = 1$, then $\chi = \psi_{\mathcal{E}}$ or $\psi_{\mathcal{E}}^2$ and we are done. If not, by Proposition 5.4, there exists an index i_0 such that $\varkappa(\mathfrak{p}_{i_0}) \neq 1$. Furthermore, since $\psi_{\mathcal{E}}(\mathfrak{p}_{i_0}) = 1$, $\chi(\mathfrak{p}_{i_0}) \neq 1$. Hence $\mathrm{Tr}(\tilde{\rho}_f(\mathfrak{p}_{i_0})) \equiv 1 \pmod 2$ and $\mathrm{Tr}(\tilde{\rho}_{\mathcal{E}}(\mathfrak{p}_{i_0})) \equiv 0 \pmod 2$.

At this point we already decided whether the two residual representations are isomorphic or not. If they are, we can apply Livne's Theorem 4.1 to the field L_E which is the last step of the algorithm.

6. Examples

In this section we present three examples of elliptic curves over imaginary quadratic fields, one for each class of residual image and show how the method works. The first publications comparing elliptic curves with modular forms over imaginary quadratic fields are due to Cremona and Whitley (see [CW94]), where they consider imaginary quadratic fields with class number 1. The study was continued by other students of Cremona. We consider some examples of Lingham's Ph.D. thesis where examples are computed for quadratic fields with class number 3 to show that our computations work on general situations. For all examples, we take $K = \mathbb{Q}[\sqrt{-23}]$ and we denote $\omega = \frac{1+\sqrt{-23}}{2}$.

All computations were done using the PARI/GP system ([PAR08]). On the next section we present the commands used to check our examples so as to serve as a guide for further cases. The routines written by the authors can be downloaded from [CNT].

6.1. **Image isomorphic to S_3.** Let $\mathcal{E}$ be the elliptic curve with equation

$$\mathcal{E} : y^2 + \omega xy + y = x^3 + (1-\omega)x^2 - x$$

It has conductor $\mathfrak{n}_{\mathcal{E}} = \bar{\mathfrak{p}}_2\mathfrak{p}_{13}$ where $\bar{\mathfrak{p}}_2 = \langle 2, 1-\omega\rangle$ and $\mathfrak{p}_{13} = \langle 13, 8+\omega\rangle$. There is an automorphic form of level $\mathfrak{n}_f = \bar{\mathfrak{p}}_2\mathfrak{p}_{13}$ (denoted by f_2 on [Lin05] table 7.1) which is the candidate to correspond to $\mathcal{E}$. We know that f has a 2-adic Galois representation attached whose L-series local factors agree at all primes except (at most) $\{\mathfrak{p}_{23}, \bar{\mathfrak{p}}_2, \mathfrak{p}_2, \mathfrak{p}_{13}, \bar{\mathfrak{p}}_{13}\}$. Let $\rho_{\mathcal{E}}$ be the 2-adic Galois representation attached to $\mathcal{E}$. Its residual representation has image isomorphic to S_3 as can easily be checked by computing the extension $L_{\mathcal{E}}$ of K obtained adding the coordinates of the 2-torsion points. Using the routine `setofprimes` we find that the set of primes of $\mathbb{Q}[\sqrt{-23}]$ above $\{3, 5, 7, 29, 31, 41, 47\}$ is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. Note that the natural answer would be the set $\{3, 5, 7, 11, 19, 29, 31, 37\}$, but since some of these ideals have norm greater than 50, they are not on table 7.1 of [Lin05]. This justifies our first list.

To prove that the answer is correct, we apply the algorithm described on section 2.1:

(1) Since 2 is unramified on $K/\mathbb{Q}$, the modulus is $\mathfrak{m}_K = 2^3 13\sqrt{-23}$.
(2) The ray class group is isomorphic to $C_{396} \times C_{12} \times C_2 \times C_2 \times C_2 \times C_2$. Using Remark 10 we find that the character ψ on the computed basis corresponds to χ_3, where $\{\chi_i\}$ is the dual basis of quadratic characters.
(3) The extended basis is $\{\psi, \chi_1, \chi_2, \chi_4, \chi_5, \chi_6\}$. Computing some prime ideals, we find that the set $\{\bar{\mathfrak{p}}_3, \mathfrak{p}_5, \bar{\mathfrak{p}}_{29}, \mathfrak{p}_{31}, \mathfrak{p}_{47}\}$ has the desired properties (using Remark 10 we know that the primes with inertial degree 3 are the ones on the third case). On distinguishing one ideal from its conjugate we follow the notation of [Lin05] for consistency (although it may not be the order of GP's output).
(4) Table 7.1 of [Lin05] shows that $\mathrm{Tr}(\tilde{\rho}_f(\mathrm{Frob}_\mathfrak{p}))$ is odd on all such primes $\mathfrak{p}$.
(5) The group of cubic characters has as dual basis for $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ the characters $\{\chi_1, \chi_2\}$, i.e. $\chi_i(v_j) = \delta_{i,j}\xi_3$, where ξ_3 is a primitive cubic root of unity and $\delta_{i,j}$ is Dirac's delta function. The ideals $\mathfrak{p}_3$ and $\mathfrak{p}_7$ are inert on the quadratic subextension of $L_\mathcal{E}$ and

$$\langle(\log(\chi_1(\mathfrak{p}_3)), \log(\chi_2(\mathfrak{p}_3))), (\log(\chi_1(\mathfrak{p}_7)), \log(\chi_2(\mathfrak{p}_7)))\rangle = (\mathbb{Z}/3\mathbb{Z})^2$$

(6) From table 7.1 (of [Lin05]) we see that $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_3}))$ is even, hence $\tilde{\rho}_f$ has image S_3 with the same quadratic subfield as $\tilde{\rho}_\mathcal{E}$.
(7) The field $K_\mathcal{E}$ can be given by the equation $x^4 + 264 * x^3 + 26896 * x^2 + 1244416 * x + 21958656$. The prime number 2 is ramified on $K_\mathcal{E}$, and factors as $2\mathcal{O}_{K_\mathcal{E}} = \mathfrak{p}_{2,1}^2\mathfrak{p}_{2,2}$. The prime number 13 is also ramified and factors as $13\mathcal{O}_{K_\mathcal{E}} = \mathfrak{p}_{13,1}^2\mathfrak{p}_{13,2}\mathfrak{p}_{13,3}$. The prime number 23 is ramified, but has a unique ideal dividing it on $K_\mathcal{E}$. The modulus to consider is $\mathfrak{m}_{K_\mathcal{E}} = \mathfrak{p}_{2,1}^5\mathfrak{p}_{2,2}^3\mathfrak{p}_{13,1}\mathfrak{p}_{13,2}\mathfrak{p}_{13,3}\mathfrak{p}_{23}$.
(8) $Cl(\mathcal{O}_{K_\mathcal{E}}, \mathfrak{m}_{K_\mathcal{E}}) \simeq C_{792} \times C_{12} \times C_{12} \times C_{12} \times C_4 \times C_2 \times C_2 \times C_2$. We claim that $\psi_\mathcal{E} = \chi_1^2\chi_4$, where χ_i is the dual basis for cubic characters of $Cl(\mathcal{O}_{K_\mathcal{E}}, \mathfrak{m}_{K_\mathcal{E}})$. To prove this, we use Remark 1. We know that $\mathfrak{p}_3$ is inert on $K_\mathcal{E}$ and $\psi_\mathcal{E}(\mathfrak{p}_3) = 1$. The prime number 7 is inert on $K_\mathcal{E}$ hence $\psi_\mathcal{E}(\mathfrak{p}_7) = 1$; the prime 37 is inert in K, but splits as a product of two ideals on $K_\mathcal{E}$. Then $\psi_\mathcal{E}(\mathfrak{p}_{37}) = 1$ on both ideals. There is a unique (up to squares) character vanishing on them, and this is $\psi_\mathcal{E}$.

    The basis $\{\psi_\mathcal{E}, \chi_1, \chi_2, \chi_3\}$ extends $\{\psi_\mathcal{E}\}$ to a basis of cubic characters. The point here is that the characters χ_i need not give Galois extensions over K. A character gives a Galois extension if and only if its modulo is invariant under the action of $\mathrm{Gal}(K_\mathcal{E}/K)$. The characters χ_1, χ_3, χ_4 do satisfy this property, hence the subgroup of cubic characters of $Cl(\mathcal{O}_{K_\mathcal{E}}, \mathfrak{m}_{K_\mathcal{E}})$ with invariant conductor has rank 3. A basis is given by $\{\psi_\mathcal{E}, \chi_1, \chi_3\}$. If we evaluate χ_1 and χ_3 at the prime above $\mathfrak{p}_3$ and $\mathfrak{p}_7$ we see that they span the $\mathbb{Z}/3\mathbb{Z}$-module. We already compared the residual traces on these ideals, hence the two residual representations are indeed isomorphic.

(9) We compute an equation for $L_{\mathcal{E}}$ over $\mathbb{Q}$. From the ideal factorizations $2\mathcal{O}_{L_{\mathcal{E}}} = \mathfrak{q}_{2,1}^2\mathfrak{q}_{2,2}^2\mathfrak{q}_{2,3}^2\mathfrak{q}_{2,4}^3$, $13\mathcal{O}_{L_{\mathcal{E}}} = \mathfrak{q}_{13,1}^2\mathfrak{q}_{13,2}^2\mathfrak{q}_{13,3}^2\mathfrak{q}_{13,4}\mathfrak{q}_{13,5}$ and $23\mathcal{O}_{L_{\mathcal{E}}} = \mathfrak{q}_{23,1}^2\mathfrak{q}_{23,2}^2\mathfrak{q}_{23,3}^2$ we take

$$\mathfrak{m}_{L_{\mathcal{E}}} = \mathfrak{q}_{2,1}^5\mathfrak{q}_{2,2}^5\mathfrak{q}_{2,3}^5\mathfrak{q}_{2,4}^7\mathfrak{q}_{13,1}\mathfrak{q}_{13,2}\mathfrak{q}_{13,3}\mathfrak{q}_{13,4}\mathfrak{q}_{13,5}\mathfrak{q}_{23,1}\mathfrak{q}_{23,2}\mathfrak{q}_{23,3}$$

as the modulus and compute the ray class group $Cl(\mathcal{O}_{L_{\mathcal{E}}}, m_{L_{\mathcal{E}}})$. It has 18 generators (see the *GP Code* section).

(10) We compute the Galois group $\mathrm{Gal}(L_{\mathcal{E}}/K)$, and chose an order 3 and an order 2 elements from it.

(11) We compute the kernels of the system and find out that the kernel for the order 3 element has dimension 8.

(12) The kernel for the order 2 element has dimension 11.

(13) The intersection of the previous two subspaces has dimension 6. It is generated by the characters

$$\{\chi_1, \chi_2\chi_5, \chi_2\chi_3\chi_6\chi_7, \chi_3\chi_4\chi_9, \chi_{12}\chi_{13}\chi_{14}, \chi_8\chi_{10}\chi_{12}\chi_{15}\chi_{17}\}.$$

(14) The ideals above $\{3, 5, 11, 29, 31\}$ satisfy that their logarithms span the $\mathbb{Z}/2\mathbb{Z}$ vector space.

(15) If we look at table 7.1 of [Lin05], we found that the ideal above 11 is missing since it has norm 121, but we can replace it by the ideals above 47. So we checked that the two representations agree on order 6 elements.

(16) The space of elements satisfying the condition on the order 3 element has dimension 10.

(17) The intersection of the two subspaces has dimension 5. A basis is given by the characters

$$\{\chi_1\chi_2\chi_4, \chi_1\chi_2\chi_6, \chi_3\chi_{10}\chi_{11}\chi_{14}, \chi_3\chi_{16}, \chi_1\chi_{10}\chi_{11}\chi_{12}\chi_{13}\chi_{17}\}.$$

(18) The prime ideals above $\{3, 7, 19, 29, 31\}$ do satisfy the condition, but since the prime 19 is inert on K, its norm is bigger than 50. Nevertheless, we can replace it by the primes above 41 which are on Table 7.1 of [Lin05].

(19) Looking at table 7.1 of [Lin05] we find that the two representations are indeed isomorphic.

(20) From the same table we see that the factors at the primes $\bar{\mathfrak{p}}_2$, $\mathfrak{p}_2$, $\mathfrak{p}_{23}$, $\bar{\mathfrak{p}}_{13}$ and $\mathfrak{p}_{13}$ also agree hence the two L-series are the same.

If the stronger version of Theorem 3.1 saying that the level of the Galois representaion equals the level of the automorphic form is true, the set of primes to consider can be diminished removing the primes above 37 on the second set of primes.

6.2. **Trivial residual image or image isomorphic to C_2.** Let $\mathcal{E}$ be the elliptic curve over K with equation

$$\mathcal{E} : y^2 + \omega xy = x^3 - x^2 - (\omega + 6)x.$$

According to [Lin05], the conductor of $\mathcal{E}$ is $\mathfrak{p}_2\overline{\mathfrak{p}}_3$, where $\mathfrak{p}_2 = \langle 2, \omega\rangle$ and $\mathfrak{p}_3 = \langle 3, -1 + \omega\rangle$.

Using the routine `setofprimes`, we find that the set

$$\{5, 7, 11, 13, 17, 19, 29, 31, 41, 47, 59, 61, 67, 71, 83, 89, 97, 101, 127, 131, 139, 151, 163,$$
$$179, 197, 211, 233, 239, 277, 311, 349, 353, 397, 439, 443, 739, 1061, 1481\}$$

is enough for checking modularity. We will confirm that this is indeed the case.

(1) The primes above 29 and 41 prove that the residual representation of the automorphic form lies on $\mathrm{GL}_2(\mathbb{F}_2)$, because the values of $a_{\mathcal{P}_{29}}, a_{\overline{\mathcal{P}_{29}}}, a_{\mathcal{P}_{41}}$ and $a_{\overline{\mathcal{P}_{41}}}$ are $6, 6, -2, 2$ respectively. Then degree 4 extension of $\mathbb{Q}_2$ has equation $x^4 + 8x^3 + 144x^2 + 512x + 896$, and it is totally ramified.
(2) The modulus is $\mathfrak{m}_K = 2^3 3^2 \sqrt{-23}$, and the ray class group $Cl(\mathcal{O}_K, \mathfrak{m}_K) \simeq C_{198} \times C_6 \times C_2 \times C_2 \times C_2 \times C_2$.
(3) − (4) There are 64 quadratic (including the trivial) extensions of K with conductor dividing $\mathfrak{m}_K$. We calculate each one, with the corresponding ray class group described in the algorithm; we pick a basis of cubic characters of each group, and evaluate them at each prime in $\{5, 7, 11, 13, 17, 19, 29, 31\}$. We find that this set is indeed enough for proving whether $\tilde{\rho}_f$ has residual image trivial or isomorphic to C_2.
(5) Since $\mathrm{Tr}(\rho_f(\mathrm{Frob}_\mathfrak{p})) \equiv 0 \pmod 2$ for the primes on the previous set (see [Lin05] table 7.1) we get that the residual image is trivial or isomorphic to C_2.
(6) − (7) The set

$$\{5, 7, 13, 29, 31, 41, 47, 59, 61, 67, 71, 83, 89, 97, 101, 127, 131, 139, 151, 163,$$
$$179, 197, 211, 233, 239, 277, 311, 349, 353, 397, 439, 443, 739, 1061, 1481\}$$

is enough. In order to see this, we must check that the Frobenius at all the primes of K above these ones cover $\mathrm{Gal}(K_S/K) \setminus \{\mathrm{id}\}$. We calculate a basis $\{\psi_1, \psi_2, \psi_3, \psi_4, \psi_5\}$ for the quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$, and compute, for $\mathfrak{p}$ a prime of K above one of these primes, $(\log \psi_1(\mathfrak{p}), \ldots, \log \psi_5(\mathfrak{p}))$. We simply check that this set of coordinates has 63 elements, so the primes we listed are enough.
(8) The primes listed are not on Table 7.1 of [Lin05]. We asked Professor John Cremona to compute the missing values so as to prove modularity for this curve.

If the stronger version of Theorem 3.1 saying that the level of the Galois representaion equals the level of the automorphic form is true, the set of primes to consider can be diminished to the primes above $\{5, 7, 11, 13, 17, 23, 29, 31, 47, 59, 71, 101, 131\}$.

6.3. **Image isomorphic to C_3.** Let $\mathcal{E}$ be the elliptic curve with equation

$$\mathcal{E} : y^2 = x^3 - \omega x^2 + (4\omega - 1)x - 5.$$

This curve is taken from Table 7.3 of [Lin05]. It has conductor $\mathfrak{p}_2^2 \bar{\mathfrak{p}}_2^3$, where $\mathfrak{p}_2 = \langle 2, \omega \rangle$ and $\bar{\mathfrak{p}}_2 = \langle 2, 1 + \omega \rangle$. There is an automorphic form f (denoted f_4 on [Lin05]) which has level $\mathfrak{n} = \mathfrak{p}_2^2 \bar{\mathfrak{p}}_2^3$ and is the candidate to correspond to $\mathcal{E}$. From Section 2 we know that f has a Galois 2-adic representation ρ_f attached to it, whose L-series agree at all primes with the possible exceptions $\mathfrak{p}_2, \bar{\mathfrak{p}}_2$ and $\mathfrak{p}_{23}$, where $\mathfrak{p}_{23}$ is the unique ideal or norm 23 on K. Let $\rho_\mathcal{E}$ denote the 2-adic Galois representation attached to $\mathcal{E}$. Its residual representation has image isomorphic to C_3 as can be easily proved by computing the extension $L_\mathcal{E}$ of K obtained adjoining the 2-torsion points coordinates.

Using the GP routine `setofprimes` (which can be downloaded from [CNT]), we find that the set of primes of $\mathbb{Q}[\sqrt{-23}]$ above

$$\{3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 47, 53, 59, 73, 79, 83, 89, 101, 131, 167, 173, 191, 211,$$
$$223, 241, 271, 307, 317, 347, 421, 463, 593, 599, 607, 617, 691, 809, 821, 853, 877, 883,$$

$997, 1151, 1481, 1553, 1613, 1789, 1871, 2027, 2339, 2347, 2423, 2693, 3571, 4831\}$

is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well.

To prove that the result is correct, we apply the algorithm described on Section 2.3

(1) The primes above 59 and 173 are enough to prove that the residual representation of the automorphic form lies on $\mathrm{GL}_2(\mathbb{F}_2)$. The values of $a_{\mathcal{P}_{59}}, a_{\overline{\mathcal{P}_{59}}}$, $a_{\mathcal{P}_{173}}$ and $a_{\overline{\mathcal{P}_{173}}}$ are $-12, 4, -6, 10$ respectively. The Frobenius polinomials of the first primes split in $\mathbb{Q}_2$, hence the Galois representations lies on a quadratic extension of $\mathbb{Q}_2$. And 2 ramifies for the second primes, as claimed.
(2) Since 2 is unramified on $K/\mathbb{Q}$, the modulus is $\mathfrak{m}_K = 2^3.\sqrt{-23}$. We compute this ray class group and find that $Cl(\mathcal{O}_K, \mathfrak{m}_K) \simeq C_{66} \times C_2 \times C_2 \times C_2$.
(3) There is a unique (up to squares) order three character, hence a unique cubic extension of K unramified outside $\mathfrak{m}_K$ so it corresponds to $L_{\mathcal{E}}$.
(4) Let $\{\chi_1, \ldots, \chi_4\}$ be a set of generators of the order two characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ with respect to the previous isomorphism. By computing their values at prime ideals of $\mathcal{O}_K$ we found that the set $C = \{\mathfrak{p}_3, \bar{\mathfrak{p}}_3, \mathfrak{p}_{13}, \bar{\mathfrak{p}}_{13}\}$ satisfies the desired properties.
(5) The traces of the Frobenius at these primes are odd (see [Lin05] table 7.1).
(6) Since there are no other order three characters, we have that $\rho_{\mathcal{E}} \simeq \rho_f$.
(7) As in the previous example, Livne's method implies that the primes above the primes in the set
$\{3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 47, 53, 59, 73, 79, 83, 89, 101, 131, 167, 173, 191, 211, 223, 241, 271, 307, 317, 347, 421, 463, 593, 599, 607, 617, 691, 809, 821, 853, 877, 883, 997, 1151, 1481, 1553, 1613, 1789, 1871, 2027, 2339, 2347, 2423, 2693, 3571, 4831\}$
are enough to prove modularity.
(8) Most of the primes listed are not on Table 7.1 of [Lin05]. We asked Professor John Cremona to compute the missing values so as to prove modularity for this curve.

Remark 12. This case is rather special, since the extension L is Galois over $\mathbb{Q}$. In particular the residual representation $\tilde{\rho}_{\mathcal{E}}$ and $\tilde{\rho}_{\bar{\mathcal{E}}}$ (where bar denotes conjugation) are isomorphic. This allows working with extensions over $\mathbb{Q}$ and avoid working with relative Galois extensions.

7. GP Code

In this section we show how to compute the previous examples with our routines and the outputs.

7.1. Image S_3.

```
? read(routines);
? K=bnfinit(w^2-w+6);
? Setofprimes(K,[w,1-w,1,-1,0],[2,13])
Case = S_3
Class group of K:  [396, 12, 2, 2, 2, 2]
Primes for discarding other quadratic extensions: [3, 5, 11, 29, 31]
Primes discarding C_3 case:  [3, 7]
The ray class group for K_E is  [792, 12, 12, 12, 4, 2, 2, 2]
```

```
Cubic character on K_E basis:  [0; 0; 0; 1]
Primes proving C_3 extension of K_E:  [3, 7, 37]
Class group of L:  [2376, 12, 12, 12, 4, 4, 4, 4, 4, 2, 2, 2, 2, 2,
2, 2, 2, 2]
%3 = [3, 5, 7, 11, 19, 29, 31, 37]
```

7.2. Image isomorphic to C_2 or trivial.

```
? read(routines);
? K=bnfinit(w^2-w+6);
Case = C_2 or trivial
Primes for proving that the residual representation
lies on F_2:  [29, 41]
Class group of K:  [198, 6, 2, 2, 2, 2]
There are 64 subgroups of Cl_K of index <= 2
Primes proving C_2 or trivial case [5, 7, 11, 13, 17, 19, 29, 31]
Livne's method output:[5, 7, 11, 13, 17, 19, 29, 31, 37, 41, 47,
59, 71, 97, 101, 127, 131, 139, 151, 163, 179, 197, 211, 233, 239,
277, 311, 349, 353, 397, 439, 443, 739, 1061, 1481]
%3 = [5, 7, 11, 13, 17, 19, 29, 31, 37, 41, 47, 59, 71, 97, 101,
127, 131, 139, 151, 163, 179, 197, 211, 233, 239, 277, 311, 349,
353, 397, 439, 443, 739, 1061, 1481]
```

7.3. Trivial residual image or image isomorphic to C_3.

```
? read(routines);
? K=bnfinit(w^2-w+6);
? Setofprimes(K,[0,-w,0,4*w-1,-5],[2])
Case = C_3
Primes for proving that the residual representation
lies on F_2:  [59, 173]
Class group of K:  [66, 2, 2, 2]
Primes proving C_3 image:  [59, 173, 3, 13]
Cubic character on K basis:  [;]
Primes proving C_3 extension of K_E:  []
Livne's method output:[3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 47,
53, 59, 73, 79, 83, 89, 101, 131, 167, 173, 191, 211, 223, 241,
271, 307, 317, 347, 421, 463, 593, 599, 607, 617, 691, 809, 821,
853, 877, 883, 997, 1151, 1481, 1553, 1613, 1789, 1871, 2027,
2339, 2347, 2423, 2693, 3571, 4831]
%3 = [3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 47, 53, 59, 73, 79, 83,
89, 101, 131, 167, 173, 191, 211, 223, 241, 271, 307, 317, 347,
421, 463, 593, 599, 607, 617, 691, 809, 821, 853, 877, 883, 997,
1151, 1481, 1553, 1613, 1789, 1871, 2027, 2339, 2347, 2423, 2693,
3571, 4831]
```

References

[BH] Tobias Berger and Gergely Harcos. ℓ-adic representations associated to modular forms over imaginary quadratic fields. *Int. Math. Res. Not. to appear.* arXiv:0707.1338.

[CNT] Computational number theory. http://www.ma.utexas.edu/users/villegas/cnt/.

[Coh00] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem*. Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[CW94] J. E. Cremona and E. Whitley. Periods of cusp forms and elliptic curves over imaginary quadratic fields. *Math. Comp.*, 62(205):407–429, 1994.

[HST93] Michael Harris, David Soudry, and Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to $\mathrm{GSp}_4(\mathbf{Q})$. *Invent. Math.*, 112(2):377–411, 1993.

[Lin05] Mark Lingham. *Modular forms and elliptic curves over imaginary quadratic fields*. PhD thesis, University of Nottingham, October 2005.

[Liv87] Ron Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 247–261. Amer. Math. Soc., Providence, RI, 1987.

[PAR08] The PARI Group, Bordeaux. *PARI/GP, version* `2.4.3`, 2008. available from `http://pari.math.u-bordeaux.fr/`.

[Sch06] Matthias Schütt. On the modularity of three Calabi-Yau threefolds with bad reduction at 11. *Canad. Math. Bull.*, 49(2):296–312, 2006.

[Ser66] Jean-Pierre Serre. Groupes de Lie l-adiques attachés aux courbes elliptiques. In *Les Tendances Géom. en Algébre et Théorie des Nombres*, pages 239–256. Éditions du Centre National de la Recherche Scientifique, Paris, 1966.

[Ser68] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser85] Jean-Pierre Serre. Résumé des cours de 1984-1985. *Annuaire du Collège de France*, pages 85–90, 1985.

[Ser95] Jean-Pierre Serre. Representaions lineaires sur des anneaux locaux, d'apres carayol. *Publ. Inst. Math. Jussieu*, 49, 1995.

[Tay94] Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields. II. *Invent. Math.*, 116(1-3):619–643, 1994.

Departament d'Àlgebra i Geometria, Facultat de Matemàtiques, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585. 08007 Barcelona
E-mail address: `ldieulefait@ub.edu`

Departamento de Matemática, Universidad de Buenos Aires, Pabellón I, Ciudad Universitaria. C.P:1428, Buenos Aires, Argentina - Institut de Mathématiques de Jussieu, Université Paris 7, Denis Diderot, 2, place Jussieu, F-75251 PARIS CEDEX 05 France.
E-mail address: `lguerb@dm.uba.ar`

Departamento de Matemática, Universidad de Buenos Aires, Pabellón I, Ciudad Universitaria. C.P:1428, Buenos Aires, Argentina
E-mail address: `apacetti@dm.uba.ar`