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 [BH07]) we can associate to an automorphic representation a family of compatible ℓ-adic representations. Our algorithm is based on Faltings-Serre's method to prove that ℓ-adic Galois representations are isomorphic. Using the algorithm we provide the first examples of modular elliptic curves over imaginary quadratic fields with residual 2-adic image isomorphic to S_3 and C_3.

1. Introduction

Modularity for elliptic curves over the rationals was one of the biggest achievements of the last century. It has been proven by Wiles, Taylor-Wiles and Breuil-Conrad-Diamond-Taylor.

Some progress has been made on a Shimura-Taniyama-Weil type correspondence over totally real fields, but the question is still very open for general number fields. Furthermore, not totally real fields are more intractable to Taylor-Wiles machinery. The case of imaginary quadratic fields has been extensively investigated numerically by Cremona, starting with his Ph.D. thesis and the articles [Cre84], [Cre92] and [CW94]. More recently, some of his students extended the calculations to fields with higher class numbers. Their work focuses on the modular symbol method which relies on computing homology groups by tessellating the hyperbolic 3-space. This allows to compute the Hecke eigenvalues of eigenforms. Doing a computer search, they furthermore exhibit candidates for matching elliptic curves by showing that the Euler factors of the L-function of the elliptic curve and that of the modular form are identical for all prime ideals up to a certain norm. The numerical data supports the conjecture (see [Cre92]):

Conjecture 1. Let K be an imaginary quadratic field. In general there is a one-to-one correspondence between rational newforms of weight 2, level $\mathfrak{n}$ and isogeny classes of elliptic curves defined over K with conductor $\mathfrak{n}$. The exceptional cases are:

- If E has complex multiplication by an order in K, then E corresponds to an Eisenstein series which is not a cup form.

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 supported by PICT 2006-00312 and UBACyT X867.

- If for a cusp form f there exists a quadratic character ε of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ such that $f \otimes \varepsilon$ is the lift of a cusp form over $\mathbb{Q}$, then f corresponds 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 ℓ-adic Tate module of A is isomorphic to two copies of the Galois representation.

Furthermore, outside the exceptional cases the properties of the classical case hold, namely:

- For a prime ideal $\mathfrak{p}$ not dividing $\mathfrak{n}$, the trace of Frobenius of the curve at $\mathfrak{p}$ equals the eigenvalue of the Hecke Operator $T_{\mathfrak{p}}$ acting on the corresponding newform.
- If $\mathfrak{p}$ divides $\mathfrak{n}$, then if $\mathfrak{p}^2$ divides $\mathfrak{n}$, the trace of Frobenius of the curve at $\mathfrak{p}$ is zero. Otherwise, it equals minus the eigenvalue of $W_{\mathfrak{p}}$.

This conjecture implies that the local factors of the automorphic representation L-series and the local factors of the elliptic curve L-series coincide.

In the present paper we present an algorithm to determine this statement for imaginary quadratic fields. In particular, if for a given newform one can compute enough Hecke eigenvalues, our algorithm allows to prove modularity for all examples considered in the cited articles . The algorithm is based on the so called Faltings-Serre method. For ℓ-adic Galois representations the Faltings-Serre method enables one to prove isomorphicity of the semisimplifications (and therefore equality of the associated L-functions) by comparing only a finite number of Euler factors.

The Galois representations considered are on the elliptic curves side the one on the ℓ-adic Tate module and on the automorphic forms side the one given in [HST93] and [Tay94]. In these articles, the authors prove the existence of an ℓ-adic Galois representation associated to modular forms over imaginary quadratic fields with cyclotomic central character. Furthermore, the L-function Euler factors agree with that of the modular form outside a set of density 0 of prime ideals. The result was improved in [BH07] to agreement outside an explicit finite set of prime ideals. This now allows to prove modularity, by checking directly the finitely many "bad" places.

Taylor also applied the Faltings-Serre method (with $\ell = 2$) to prove the equality of the Euler-factors of the elliptic curve over $\mathbb{Q}[\sqrt{-3}]$ of conductor $\left(\frac{17+\sqrt{-3}}{2}\right)$ (corresponding to the second case of our algorithm) for a set of density one primes, therefore (almost!) proving the modularity of the elliptic curve.

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

We thank Professor John Cremona for computing the Hecke eigenvalues of the automorphic forms considered in the examples and verifying they match the L-function Euler factors of the elliptic curves. This proves modularity of such elliptic curves. We would also like to thank Professor Jean-Pierre Serre for useful talks and the example provided to us while dealing with the case of residual 2-adic image isomorphic to C_3, and Professor Matthias Schütt for reading a first version of this

paper and making us corrections and comments on it. At last we would like to thank the referee for making the exposition clearer.

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 ℓ-adic Galois representations are isomorphic or not for any prime ℓ. 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. We denote by G_K the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$.

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 by $e(\mathfrak{q}|\mathfrak{p})$ the ramification index.

Let K_λ be a finite extension of $\mathbb{Q}_l$, $\mathcal{O}_{K_\lambda}$ be its ring of integers and $\mathbb{F}_\lambda$ be the residue field. Given a representation $\rho : G_K \to \mathrm{GL}_2(\mathcal{O}_{K_\lambda})$, we denote by $\tilde{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F}_\lambda)$ its residual representation, that is the composition of ρ with the quotient map $\mathrm{GL}_2(\mathcal{O}_{K_\lambda}) \mapsto \mathrm{GL}_2(\mathbb{F}_\lambda)$.
In the special case where ρ is a representation coming from the action of G_K on the Tate module $T_\ell(\mathcal{E})$ of an elliptic curve $\mathcal{E}$, the residual representation corresponds to the action of G_K on the ℓ-torsion points $\mathcal{E}[\ell]$.

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 in $L_{\mathcal{E}}$ on the computed basis.

(3) Extend $\{\psi\}$ to a basis $\{\psi, \chi_i\}_{i=1}^{n}$ of the quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$. 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 in $L_{\mathcal{E}}$ 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 $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}}))$ is odd for all prime ideals $\mathfrak{p}$ found in the last step, $\tilde{\rho}_f$ 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 $\{\mathfrak{p}_j\}_{j=1}^{m'}$ such that $\psi(\mathfrak{p}_j) = -1$ or $\mathfrak{p}_j$ splits completely in $L_{\mathcal{E}}$ and

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

(6) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}}))$ is even for all prime ideals $\mathfrak{p}$ found in the last step, $\tilde{\rho}_f$ 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

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

(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 $1 \leq j \leq m'$, 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 $\mathfrak{m}_{L_{\mathcal{E}}} = \prod_{\mathfrak{q}|2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)} \mathfrak{q}^{e(\mathfrak{q})}$ 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 $\{\mathfrak{a}_i\}_{i=1}^n$ be a basis for the even order elements of $Cl(\mathcal{O}_{L_{\mathcal{E}}}, \mathfrak{m}_{L_{\mathcal{E}}})$ and 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 $1 \leq i \leq m$ 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

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

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 $1 \leq i \leq n$ output "$\rho_f \simeq \rho_{\mathcal{E}}$". If not output "the two representations are not isomorphic".

(20) If the local factors of $L(f,s)$ and the local factors of $L(\mathcal{E},s)$ coincide for prime ideals $\mathfrak{p}$ dividing $2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)$ then $L(f,s) = L(\mathcal{E},s)$.

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

(1) Choose prime ideals $\mathcal{P}_i$, $i = 1, 2$ such that if $\alpha_{\mathcal{P}_i}$ and $\beta_{\mathcal{P}_i}$ denote the roots of the characteristic polynomial of $\mathrm{Frob}_{\mathcal{P}_i}$, $\alpha_{\bar{\mathcal{P}}_i} + \beta_{\bar{\mathcal{P}}_i} \neq 0$ and in the extension $\mathbb{Q}[\alpha_{\mathcal{P}_i}]$ 2 has no inertial degree. 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) 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 $\mathfrak{m}_L = \prod_{\mathfrak{p}|2\Delta(K)\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}} \mathfrak{p}^{e(\mathfrak{p})}$, 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

$$\langle (\log(\chi_1(\mathfrak{q}_j)), \dots, \log(\chi_n(\mathfrak{q}_j))) \rangle_{j=1}^{n'} = (\mathbb{Z}/3\mathbb{Z})^n.$$

(5) Consider the collection $\{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$ of all prime ideals of $\mathcal{O}_K$ which are below the prime ideals found in step (4).

(6) If $\mathrm{Tr}(\tilde{\rho}_f(\mathrm{Frob}_{\mathfrak{p}_i})) \equiv 0 \pmod 2$ for all prime ideals $\mathfrak{p}$ found in the last step, 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

$$\{(\log(\chi_1(\mathfrak{p}_i)), \dots, \log(\chi_n(\mathfrak{p}_i))\}_{i=1}^{2^n-1} = (\mathbb{Z}/2\mathbb{Z})^n \backslash \{0\}$$

(9) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_i})) = \mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathfrak{p}_i}))$ for $i = 1, \dots, 2^n - 1$, $\rho_{\mathcal{E}}^{ss} \simeq \rho_f^{ss}$. If not, output "the two representations are not isomorphic".
(10) If the local factors of $L(f, s)$ and the local factors of $L(\mathcal{E}, s)$ coincide for prime ideals $\mathfrak{p}$ dividing $2\mathfrak{n}(\mathcal{E})\mathfrak{n}(f)\overline{\mathfrak{n}(f)}\Delta(K)$ 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. The following result is useful for identifying non-cubic subsets of $(\mathbb{Z}/2\mathbb{Z})$-vector spaces.

Proposition 2.1. *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]. □

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

(1) Choose prime ideals $\mathcal{P}_i$, $i = 1, 2$ such that if $\alpha_{\mathcal{P}_i}$ and $\beta_{\mathcal{P}_i}$ denote the roots of the characteristic polynomial of $\mathrm{Frob}_{\mathcal{P}_i}$, $\alpha_{\bar{\mathcal{P}}_i} + \beta_{\bar{\mathcal{P}}_i} \neq 0$ and on the extension $\mathbb{Q}[\alpha_{\mathcal{P}_i}]$ 2 has no inertial degree. 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

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

(where we take any root of the logarithm and identify $\log(\pm 1)$ with $\mathbb{Z}/2\mathbb{Z}$).
(5) If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}}))$ is odd for all prime ideals $\mathfrak{p}$ found in the last step, $\tilde{\rho}_f$ 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

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

(where we take any root of the logarithm and identify log of the cubic roots of unity with $\mathbb{Z}/3\mathbb{Z}$). If $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_j})) \equiv \mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathfrak{p}_j}))$ (mod 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, ℓ-adic representations of the group G_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 $T_\ell(\mathcal{E})$ which is a free rank two $\mathbb{Z}_\ell$-module with a G_K-action, thus giving rise to a ℓ-adic representation

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

In order to make sure that the Galois representation $\rho_{\mathcal{E},\ell}$ is absolutely irreducible we will assume that $\mathcal{E}$ does not have Complex Multiplication. The ramification locus of the representation $\rho_{\mathcal{E},\ell}$ consists of primes of K dividing ℓ together with the set S of primes of bad reduction of $\mathcal{E}$. The family of Galois representations $\{\rho_{\mathcal{E},\ell}\}$ 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 [BH07]) have proved that one can attach compatible families of two-dimensional Galois representations $\{\rho_\ell\}$ to any regular algebraic cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_K)$, assuming that it has unitary central character ω with $\omega = \omega^c$, where the superscript c denotes the action of the non-trivial automorphism of K. This is equivalent to saying that the central character is the restriction of a character of $G_{\mathbb{Q}}$. 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_ℓ and also that, at unramified places $\mathfrak{p}$, the characteristic polynomial of $\rho_\ell(\mathrm{Frob}_{\mathfrak{p}})$ 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_ℓ 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 [BH07]):

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

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

such that if $\mathfrak{p}$ is a prime of K not in S then $\rho_{\pi,\ell}$ is unramified at $\mathfrak{p}$ and the characteristic polynomial of $\rho_{\pi,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ 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 $\rho_{\pi,\ell}$ is unramified at $\mathfrak{p}$, the above theorem does not imply that the trace of $\rho_{\pi,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ 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 $\{\rho_{\pi,\ell}\}$, i.e., that the conductor should be independent of ℓ

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 ℓ that $\rho_{\mathcal{E},\ell} \cong \rho_{\pi,\ell}$ then the same holds for every prime ℓ.

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 ℓ-adic Tate module of A is isomorphic to two copies of the Galois representation. This phenomenon was studied by Cremona on [Cre92], and is the phenomenon mentioned in Conjecture 1. Even in this case, the algorithm works, since the input in any case is an elliptic curve over K and an automorphic form.

From now on, we assume that the field generated by the traces of Frobenius elements is the rational field $\mathbb{Q}$, since these are the newforms corresponding to elliptic curves. This is the case considered in Lingham's examples, where he computed rational newforms.

Remark 5. At first the image is defined over a finite extension of $\mathbb{Q}_\ell$. Actually, it can be defined over the ring of integer of an at most degree 4 extension $E_{\mathfrak{L}}$ of $\mathbb{Q}_\ell$. 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 $E_{\mathfrak{L}}$ as its completion at any prime above ℓ by Corollary 1 of [Tay94].

4. Faltings-Serre method

4.1. **First case: the residual image is absolutely irreducible.** In this section we review Faltings-Serre ([Ser85]) method by stating the main ideas of [Sch06] (Section 5) in our particular case. Take $\ell = 2$ and let

$$\rho_i : G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$$

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

- They have the same determinant.
- They are unramified outside a finite set S.
- The mod 2 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 $\mathfrak{p}$. Choose the maximal r such that $\mathrm{Tr}(\rho_1) \equiv \mathrm{Tr}(\rho_2) \pmod{2^r}$, and consider the non-trivial map $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathbb{F}_2$ given by

$$\phi(\sigma) \equiv \frac{\mathrm{Tr}(\rho_1(\sigma)) - \mathrm{Tr}(\rho_2(\sigma))}{2^r} \pmod 2.$$

Since the mod 2 residual representations $\tilde{\rho_1}$ and $\tilde{\rho_2}$ are absolutely irreducible and their images are isomorphic, we can assume that $\tilde{\rho_1} = \tilde{\rho_2}$.

Since $\operatorname{Tr}\rho_1 \equiv \operatorname{Tr}\rho_2 \pmod{2^r}$, given $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/K)$, there exists $\mu(\sigma) \in M_2(\mathbb{Z}_2)$ such that

$$\rho_1(\sigma) = (1 + 2^r\mu(\sigma))\rho_2(\sigma).$$

Then,

$$\phi(\sigma) = \frac{\operatorname{Tr}(\rho_1(\sigma)) - \operatorname{Tr}(\rho_2(\sigma))}{2^r} = \operatorname{Tr}(\mu(\sigma)\rho_2(\sigma)) \equiv \operatorname{Tr}(\mu(\sigma)\tilde{\rho}_1(\sigma)) \pmod 2. \tag{1}$$

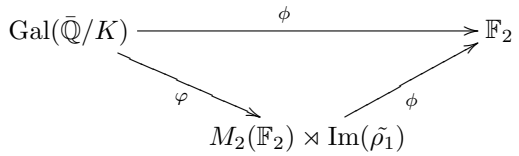
Consider the map $\varphi : \operatorname{Gal}(\bar{\mathbb{Q}}/K) \mapsto M_2(\mathbb{F}_2) \rtimes \operatorname{Im}(\tilde{\rho_1})$ given by

$$\varphi(\sigma) = (\mu(\sigma), \tilde{\rho}_1(\sigma)) \pmod 2.$$

An easy computation shows that

$$\mu(\sigma\tau) \equiv \mu(\sigma) + \tilde{\rho}_1(\sigma)^{-1}\mu(\tau)\tilde{\rho}_1(\sigma) \pmod 2,$$

which implies that φ is a group morphism. Furthermore, since $\ker(\phi)$ contains the group $\left\{\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/K) \,:\, \mu(\sigma) \equiv 0 \pmod 2\right\} \rtimes \{1\}$, ϕ factors through $M_2(\mathbb{F}_2) \rtimes \operatorname{Im}(\tilde{\rho_1})$. We have the diagram



By (1), ϕ is defined on $M_2(\mathbb{F}_2) \rtimes \operatorname{Im}(\tilde{\rho_1})$ by $\phi(A, C) = \operatorname{Tr}(AC)$. Let $\tilde{\mu}$ denote the composition of μ with reduction modulo 2. Since

$$\det(\rho_1(\sigma)) \equiv (1 + 2^r \operatorname{Tr}(\mu(\sigma)))\det(\rho_2(\sigma)) \pmod{2^{r+1}},$$

the condition $\det(\rho_1) = \det(\rho_2)$ implies that $\operatorname{Im}(\tilde{\mu}) \subset M_2^0(\mathbb{F}_2) := \{M \in M_2(\mathbb{F}_2) : \operatorname{Tr}(M) \equiv 0 \pmod 2\}$, hence it has order at most 2^3. In our case, $\operatorname{Im}(\tilde{\rho}_i) = S_3$.

Lemma 4.1. *$M_2^0(\mathbb{F}_2) \rtimes S_3 \simeq S_4 \times C_2$.*

This can be proved in different ways, we give an explicit isomorphism for latter considerations. Take the isomorphism between $\mathrm{GL}_2(\mathbb{F}_2)$ 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 $\left\{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$ 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 in $S_4 \times C_2$). If we denote by L the fixed field of $\ker(\tilde{\rho}_1)$, we need to compute all possible extensions $\tilde{L}$ of L Galois over K, unramified outside S and with Galois group over K isomorphic to a subgroup of $S_4 \times C_2$. For each $\tilde{L}$, take a prime ideal $\mathfrak{p}_{\tilde{L}} \subset K$ with inertial degree 4 or 6 on $\tilde{L}$. Then $\{\mathfrak{p}_{\tilde{L}}\}$ has the desired properties.

Remark 6. In the proof given above one starts with a $\mod \ell^r$ congruence between the traces of ρ_1 and ρ_2 and uses the fact that this implies that the two $\mod \ell^r$ representations are isomorphic. This result is proved in [Ser95] (Theorem 1) but only with the assumption that the residual $\mod \ell$ 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 in [Liv87], where the author proves the next Theorem:

Theorem 4.2. *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]. □

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 restrict 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 the 2-group case for the field K_ρ and Livne's Theorem 4.2 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, the image of $\tilde{\rho}_{\mathcal{E}}$ is a 2-group. If not, assume (via a change of variables) that the elliptic curve has equation

$$\mathcal{E} : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

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 in 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 absolutely irreducible, we need to prove that the image lies (after conjugation) in 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 choose 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 $\alpha_{\mathcal{P}_i} \neq \beta_{\mathcal{P}_i}$, the field $E = \mathbb{Q}[\alpha_{\mathcal{P}_i}]$ has inertial degree 1 at 2 and $\alpha_{\bar{\mathcal{P}}_i} + \beta_{\bar{\mathcal{P}}_i} \neq 0$. If $\mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathcal{P}_i})) = \mathrm{Tr}(\rho_{\pi,2}(\mathcal{P}_i))$ for such primes, 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 page IV-14 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 by adding the roots of the polynomials x^2+14 and x^2+6 to $\mathbb{Q}_2$ (whose roots in $\bar{\mathbb{Q}}_2$ are different) are two ramified extensions of $\mathbb{Q}_2$. Their composition is a degree 4 field extension (since the prime 2 is totally ramified in the composition of these extensions over $\mathbb{Q}$). Since the set of primes inert in K have density zero, we can choose prime ideals $\mathcal{P}_1$ and $\mathcal{P}_2$ such that $\mathbb{Q}_2[\alpha_{\mathcal{P}_1}]$ and $\mathbb{Q}_2[\alpha_{\mathcal{P}_2}]$ are isomorphic to F_1 and F_2 respectively. □

Actually we search for the first two primes such that if $\alpha_{\mathcal{P}_i}$ and $\beta_{\mathcal{P}_i}$ denote the roots of the characteristic polynomial of their Frobenius automorphisms, $\alpha_{\bar{\mathcal{P}}_i} + \beta_{\bar{\mathcal{P}}_i} \neq 0$ and in the extension $\mathbb{Q}[\alpha_{\mathcal{P}_i}]$, 2 has no inertial degree.

The first step of the algorithm is to prove that the residual representations are indeed isomorphic so as to apply Faltings-Serre 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 in $\mathcal{O}_K$. 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 in 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*

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

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 $1 \leq j \leq n'$. 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 $(\varepsilon_1, \dots \varepsilon_n)$ is a solution of the homogeneous system

$$\begin{pmatrix} \log(\psi_1(\mathfrak{p}_1)) & \dots & \log(\psi_n(\mathfrak{p}_1)) \\ \vdots & & \vdots \\ \log(\psi_1(\mathfrak{p}_{n'})) & \dots & \log(\psi_n(\mathfrak{p}_{n'})) \end{pmatrix}.$$

Since $\{(\log(\psi_1(\mathfrak{p}_j)), \dots, \log(\psi_n(\mathfrak{p}_j)))\}_{j=1}^{n'}$ 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. What we do in practice is to enlarge the matrix

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

with enough prime ideals of K until it has rank n.

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. *Assume that the traces of Frobenius elements of a 2-dimensional ℓ-adic Galois representation are all in $\mathbb{Q}_\ell$ and that the residual representation is absolutely irreducible, then the field E can be taken to be $\mathbb{Q}_\ell$.*

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

Remark 9. Since all our traces lie in $\mathbb{Q}_2$, once we prove that the residual representation of $\rho_{\pi,2}$ has image strictly 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. The first step is to prove that if L_f denotes the fixed field of the kernel of ρ_f, then it contains no quadratic extension of K or it contains $K_{\mathcal{E}}$, the quadratic extension of K contained in $L_{\mathcal{E}}$.

We compute all quadratic extensions of K using Class Field theory and Proposition 5.3. Let ψ be the quadratic character of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ associated to $K_{\mathcal{E}}$. We extend $\{\psi\}$ to a basis $\{\psi, \chi_i\}_{i=1}^{n}$ of the quadratic characters of $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ and find a set of unramified prime ideals $\{\mathfrak{p}_j\}_{j=1}^{n'}$ with inertial degree 3 on $L_{\mathcal{E}}$ and such that $\langle(\log(\chi_1(\mathfrak{p}_j)), \ldots, \log(\chi_n(\mathfrak{p}_j)))\rangle_{j=1}^{n'} = (\mathbb{Z}/2\mathbb{Z})^n$. Since an ideal with inertial degree 3 on $L_{\mathcal{E}}$ splits on $K_{\mathcal{E}}$, $\psi(\mathfrak{p}_i) = 1$ for all $1 \leq i \leq n'$.

If χ is a quadratic character corresponding to a subfield of L_f, $\chi = \psi^{\varepsilon}\varkappa$, where $\varkappa = \prod_{i=1}^{n} \chi_i^{\varepsilon_i}$. If $\varkappa = 1$, then $\chi = \psi$ or trivial and we are done. Otherwise, by Proposition 5.4, there exists an index i_0 such that $\varkappa(\mathfrak{p}_{i_0}) \neq 1$. Furthermore, since $\psi(\mathfrak{p}_{i_0}) = 1$, $\chi(\mathfrak{p}_{i_0}) \neq 1$. Hence $\mathrm{Tr}(\tilde{\rho}_f(\mathfrak{p}_{i_0})) \equiv 0 \pmod 2$ and $\mathrm{Tr}(\tilde{\rho}_E(\mathfrak{p}_{i_0})) \equiv 1 \pmod 2$ which implies that the residual representations are not isomorphic. This is done in 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 in $K_{\mathcal{E}}$ knowing how they decompose in 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 the easy ones: if $\mathfrak{p}$ is inert in $\mathcal{O}_{K_P}$, the inertial degree of $\mathfrak{p}$ in $[L_{\mathcal{E}} : K]$ is 3 since the Galois group is non-abelian. This corresponds to the last case of the table.

If $\mathfrak{p}\mathcal{O}_{K_P}$ factors as a product of two ideals $\mathfrak{p}_1\mathfrak{p}_2$, one of them has inertial degree 1 and the other has inertial degree 2. Since the inertial degree is multiplicative, the inertial degree of $\mathfrak{p}$ in $[L_{\mathcal{E}} : K]$ is 2 and we are in the second case.

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

$$\mathfrak{p}\mathcal{O}_{L_{\mathcal{E}}} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3. \tag{2}$$

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 to 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 (2) 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 in $D(\mathfrak{q}_1|\mathfrak{p})$, 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 $D(\mathfrak{q}_1|\mathfrak{p}) \cap D(\mathfrak{q}_2|\mathfrak{p}) = \{1\}$. □

Next we need to discard the C_3 case. Let $\mathfrak{m}_K$ be as described in 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 in $K_{\mathcal{E}}$ or split completely in $L_{\mathcal{E}}$ (that is, they have order 1 or 2 in S_3 and in particular have even trace for the residual representation $\tilde{\rho}_{\mathcal{E}}$) and such that $\langle(\log(\chi_1(\mathfrak{p}_j)), \dots, \log(\chi_m(\mathfrak{p}_j)))\rangle_{j=1}^{m'} = (\mathbb{Z}/3\mathbb{Z})^m$. 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 in 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 method explained in the previous section. It implies computing all fields $\tilde{L}$ with Galois group $\mathrm{Gal}(\tilde{L}/K) \simeq S_4 \times C_2$. We claim that it is enough to look for quadratic extensions $\tilde{L}$ of L unramified outside $\mathfrak{m}_L$ such that its normal closure is isomorphic to S_4 or $S_3 \times C_2$.

The claim comes from the fact that 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

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

Furthermore, every element of order 4 or 6 in $S_4 \times C_2$ maps to an element of order 4 in S_4 or to an element of order 6 on $S_3 \times C_2$ under the previous surjections. Then if we compute normal extensions of L with Galois group S_4 or $S_3 \times C_2$ and a prime element of order 4 or 6 in each one of them, this set of primes is enough to decide whether the representations are isomorphic or not. The advantage of considering these two extensions is that they are obtained as normal closure of quadratic extensions of L.

Let $\mathfrak{m}_L$ be a modulus in 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 in $Cl(\mathcal{O}_L, \mathfrak{m}_L)$ and $\sigma \in \mathrm{Gal}(L/K)$, $\sigma.\psi = \psi \circ \sigma$.

Lemma 5.6. *If ψ is a character in $Cl(\mathcal{O}_L, \mathfrak{m}_L)$ 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 in $L[\sqrt{\alpha}]$ 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 $\psi \cdot (\sigma.\psi) = \sigma^2.\psi$, 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 $\Theta : S_3 \to \mathrm{GL}_2(\mathbb{F}_2)$. Its kernel is a normal subgroup, hence it can be $\mathrm{GL}_2(\mathbb{F}_2)$ (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 $\mathrm{GL}_2(\mathbb{F}_2)$ 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

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

The extension $L\left[\sqrt{1+\sqrt[3]{2}}\right]$ is clearly fixed by τ, but its normal closure has degree 8 over L since $\sqrt{1+\xi_3^2\sqrt[3]{2}}$ is not in 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. The first case is compute the $S_3 \times C_2$ extensions. A quadratic character χ is invariant under σ if and only if the character $\chi \cdot (\sigma.\chi)$ is trivial. If $\{\chi_i\}_{i=1}^n$ is a basis for the quadratic characters, $\chi = \prod_{i=1}^n \chi_i^{\varepsilon_i}$ for some ε_i. We are looking for exponents ε_i modulo 2 such that

$$\sum_{i=1}^{n} \varepsilon_i \log(\chi_i(\mathfrak{a})\chi_i(\sigma.\mathfrak{a})) = 0$$

for all ideals $\mathfrak{a}$. Since the characters are multiplicative, it is enough to check this condition on a basis. This is the system we consider in step (11) for an order 3 element σ of $\mathrm{Gal}(L_{\mathcal{E}}/K)$. On step (12) we do the same for an order 2 element τ of $\mathrm{Gal}(L_{\mathcal{E}}/K)$ and in step (13) we compute the intersection of the two subspaces. These characters give all $S_3 \times C_2$ extensions of $L_{\mathcal{E}}$. On step (14), using Proposition 5.4 we compute prime ideals having order 6 on each such extension.

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 then use Proposition 5.4 on a basis of it to compute prime ideals of K having order 4 in each such extension. Note that the elements of order 4 correspond to prime ideals that are inert in 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 in 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 4.2. 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 at 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 5.4 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 4.2. 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 (8), 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 semisimplifications of 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

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

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 in 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 $\mathfrak{q}$ in the set is inert in 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 in 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 in step (1), so as to be used for both quadratic and cubic extensions. Note that the characters χ and χ^2 give rise 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 4.2 to the field L_E which is the last step of the algorithm.

$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$
3	$\langle 2, \omega \rangle$	-2	$\langle 2, \omega + 1 \rangle$	1
25	$\langle 5 \rangle$	-1		
49	$\langle 7 \rangle$	-4		
29	$\langle 29, \omega + 10 \rangle$	0	$\langle 29, \omega + 18 \rangle$	-3
31	$\langle 31, \omega + 7 \rangle$	5	$\langle 31, \omega + 23 \rangle$	-4
41	$\langle 41, \omega + 25 \rangle$	12	$\langle 41, \omega + 15 \rangle$	9
47	$\langle 47, \omega + 33 \rangle$	9	$\langle 47, \omega + 13 \rangle$	6

TABLE 6.1. Values of $a_{\mathfrak{p}}$ used to prove modularity in the S_3 example.

6. Examples

In this section we present three examples of elliptic curves over imaginary quadratic fields, one for each class of residual 2-adic 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. The examples we consider are taken from Lingham's Ph.D. thesis (see [Lin05]), who considered imaginary quadratic fields with class number 3.

All our 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], under the item "modularity".

6.1. **Image isomorphic to S_3.** Let $K = \mathbb{Q}[\sqrt{-23}]$ and $\omega = \frac{1+\sqrt{-23}}{2}$. 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 $\mathfrak{n}_f = \bar{\mathfrak{p}}_2\mathfrak{p}_{13}$ and trivial character (denoted by f_2 in [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 with $L(f,s)$ 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 $\mathbb{Q}[\sqrt{-23}]$ dividing the rational primes $\{3, 5, 7, 29, 31, 41, 47\}$ is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. Note that the normal answer of the routine 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 in table 7.1 of [Lin05]. This justifies using some flags in the routine (as documented) to get our first list and prove modularity in this particular case. The values of the $a_{\mathfrak{p}}$ for these primes are listed in Table 6.1.

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

(1) Since 2 is unramified in $K/\mathbb{Q}$, 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 in 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 in the third case).
(4) Table 6.1 shows that $\mathrm{Tr}(\tilde{\rho}_f(\mathrm{Frob}_{\mathfrak{p}}))$ is odd in 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 in 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 6.1 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 $x^4 + 264 \cdot x^3 + 26896 \cdot x^2 + 1244416 \cdot x + 21958656$. The prime number 2 is ramified in $K_{\mathcal{E}}$, 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 in $K_{\mathcal{E}}$. The modulus to consider is $\mathfrak{m}_{K_{\mathcal{E}}} = \mathfrak{p}_{2,1}\mathfrak{p}_{2,2}\mathfrak{p}_{13,1}\mathfrak{p}_{13,2}\mathfrak{p}_{13,3}\mathfrak{p}_{23}$.
(8) $Cl(\mathcal{O}_{K_{\mathcal{E}}}, \mathfrak{m}_{K_{\mathcal{E}}}) \simeq C_{792} \times C_{12} \times C_6 \times C_3$. We claim that $\psi_{\mathcal{E}} = \chi_4$, where χ_i is the dual basis for cubic characters of $Cl(\mathcal{O}_{K_{\mathcal{E}}}, \mathfrak{m}_{K_{\mathcal{E}}})$. We know that $\mathfrak{p}_3$ is inert in $K_{\mathcal{E}}$ hence $\psi_{\mathcal{E}}(\mathfrak{p}_3) = 1$. The prime number 7 is inert in $K_{\mathcal{E}}$ hence $\psi_{\mathcal{E}}(\mathfrak{p}_7) = 1$; the prime 37 is inert in K, but splits as a product of two ideals in $K_{\mathcal{E}}$. Then $\psi_{\mathcal{E}}(\mathfrak{p}_{37}) = 1$ in both ideals. There is a unique (up to squares) character vanishing in 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 in 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 choose 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) The ideal above 11 is missing in table 7.1 of [Lin05] since it has norm 121, but we can replace it by the ideals above 47 which appears in Table 6.1. So we checked that the two representations agree in order 6 elements.
(16) The space of elements satisfying the condition in 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 in K, its norm is bigger than 50. Nevertheless, we can replace it by the primes above 41 which are in Table 6.1.
(19) Looking at Table 6.1 we find that the two representations are indeed isomorphic.
(20) From the same table we see that the eigenvalues for the Atkin-Lehner involutions $\mathcal{W}_{\mathfrak{p}}$ for $\mathfrak{p} = \bar{\mathfrak{p}}_2$ and $\mathfrak{p}_{13}$ are -1 and 1 respectively which is minus the trace of Frobenius of $\mathcal{E}$ at this primes. The Hecke eigenvalues of the automorphic form at the primes $\mathfrak{p}_2, \bar{\mathfrak{p}}_{13}$ and $\mathfrak{p}_{23}$ are $0, 5$ and 6 respectively, which also coincide with the elliptic curve $a_{\mathfrak{p}}$ in such primes, hence the two L-series agree.

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

6.2. **Trivial residual image or image isomorphic to C_2.** Let $\mathcal{E}$ be the elliptic curve over $K = \mathbb{Q}[\sqrt{-31}]$ with equation
$$\mathcal{E} : y^2 + \omega xy = x^3 - x^2 - (\omega + 6)x,$$
where $\omega = \frac{1+\sqrt{-31}}{2}$. According to [Lin05, Table 5.1], the conductor of $\mathcal{E}$ is $\mathfrak{p}_2\mathfrak{p}_5$, where $\mathfrak{p}_2 = \langle 2, \omega\rangle$ and $\mathfrak{p}_5 = \langle 5, \omega + 1\rangle$. There is a newform of level this level and trivial character (denoted by f_1 in [Lin05, Table 7.4]) 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 with $L(f, s)$ at all primes except (at most) $\{\mathfrak{p}_{31}, \bar{\mathfrak{p}}_2, \mathfrak{p}_2, \mathfrak{p}_5, \bar{\mathfrak{p}}_5\}$. Let $\rho_{\mathcal{E}}$ be the 2-adic Galois representation attached to $\mathcal{E}$. Its residual representation has image isomorphic to C_2 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
$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 47, 59, 67, 71, 89, 97, 101, 103, 107, 109, 149, 157,$$
$$163, 191, 193, 211, 293, 311, 317, 359, 443, 577, 607, 617, 653, 691, 701\}$$
is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. The values of the $a_{\mathfrak{p}}$ for these primes are listed in Table 6.2 which was computed by Professor Cremona (using

$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$	$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$
3	$\langle 3\rangle$	-4			109	$\langle 109, 14+\omega\rangle$	12	$\langle 109, 94+\omega\rangle$	-10
7	$\langle 7, 2+\omega\rangle$	4	$\langle 7, 4+\omega\rangle$	2	149	$\langle 149, 38+\omega\rangle$	10	$\langle 149, 110+\omega\rangle$	10
11	$\langle 11\rangle$	10			157	$\langle 157, 17+\omega\rangle$	-14	$\langle 157, 139+\omega\rangle$	10
13	$\langle 13\rangle$	16			163	$\langle 163, 67+1\omega\rangle$	24	$\langle 163, 95+1\omega\rangle$	-20
17	$\langle 17\rangle$	-18			191	$\langle 191, 27+1\omega\rangle$	8	$\langle 191, 163+1\omega\rangle$	24
19	$\langle 19, 5+\omega\rangle$	-6	$\langle 19, 13+\omega\rangle$	0	193	$\langle 193, 55+1\omega\rangle$	-10	$\langle 193, 137+1\omega\rangle$	-2
23	$\langle 23\rangle$	-30			211	$\langle 211, 89+1\omega\rangle$	20	$\langle 211, 121+1\omega\rangle$	6
29	$\langle 29\rangle$	30			293	$\langle 293, 76+1\omega\rangle$	28	$\langle 293, 216+1\omega\rangle$	-14
41	$\langle 41, \omega+12\rangle$	-2	$\langle 41, \omega+28\rangle$	2	311	$\langle 311, 111+1\omega\rangle$	-32	$\langle 311, 199+1\omega\rangle$	0
47	$\langle 47, 21+\omega\rangle$	6	$\langle 47, 25+\omega\rangle$	-8	317	$\langle 317, 35+1\omega\rangle$	-6	$\langle 317, 281+1\omega\rangle$	-18
59	$\langle 59, 10+\omega\rangle$	-4	$\langle 59, 48+\omega\rangle$	0	359	$\langle 359, 158+1\omega\rangle$	22	$\langle 359, 200+1\omega\rangle$	-18
67	$\langle 67, 30+\omega\rangle$	12	$\langle 67, 36+\omega\rangle$	-2	443	$\langle 443, 66+1\omega\rangle$	-4	$\langle 443, 376+1\omega\rangle$	-20
71	$\langle 71, 26+\omega\rangle$	-8	$\langle 71, 44+\omega\rangle$	-8	577	$\langle 577, 217+1\omega\rangle$	32	$\langle 577, 359+1\omega\rangle$	-10
89	$\langle 89\rangle$	110			607	$\langle 607, 291+1\omega\rangle$	-8	$\langle 607, 315+1\omega\rangle$	48
97	$\langle 97, 19+\omega\rangle$	16	$\langle 97, 77+\omega\rangle$	-2	617	$\langle 617, 78+1\omega\rangle$	2	$\langle 617, 538+1\omega\rangle$	30
101	$\langle 101, 37+\omega\rangle$	10	$\langle 101, 63+\omega\rangle$	0	653	$\langle 653, 157+1\omega\rangle$	-18	$\langle 653, 495+1\omega\rangle$	-4
103	$\langle 103, 40+\omega\rangle$	0	$\langle 103, 62+\omega\rangle$	8	691	$\langle 691, 52+1\omega\rangle$	-20	$\langle 691, 638+1\omega\rangle$	28
107	$\langle 107, 20+\omega\rangle$	-4	$\langle 107, 86+\omega\rangle$	-6	701	$\langle 701, 221+1\omega\rangle$	-22	$\langle 701, 479+1\omega\rangle$	34

TABLE 6.2. Values of $a_{\mathfrak{p}}$ used to prove modularity in the C_2 example.

some Magma code written by himself and Lingham) and sent to us in a private communication. He also checked that these values match the elliptic curve ones, which proves modularity in this case. To prove that the answer is correct, we apply the algorithm described on section 2.2:

(1) The primes above 41 and 47 prove that the residual representation of the automorphic form lies in $\mathrm{GL}_2(\mathbb{F}_2)$, because the values of $a_{\mathfrak{p}_{41}}, a_{\bar{\mathfrak{p}}_{41}}, a_{\mathfrak{p}_{47}}$ and $a_{\bar{\mathfrak{p}}_{47}}$ are $-2, 2, 6, -8$ respectively (see Table 6.2). The degree 4 extension of $\mathbb{Q}_2$ has equation $x^4 - 16x^3 + 252x^2 - 1504x + 2756$, and the prime 2 is totally ramified in this extension.
(2) The modulus is $\mathfrak{m}_K = 2^3 5\sqrt{-31}$, and the ray class group $Cl(\mathcal{O}_K, \mathfrak{m}_K) \simeq C_{60} \times C_{12} \times C_2 \times C_2 \times C_2 \times C_2$.
(3) – (5) 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 $\{3, 7, 11, 13, 17, 19\}$. It turns out that this set is indeed enough for proving whether $\tilde{\rho}_f$ has residual image trivial or isomorphic to C_2.
(6) Since $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}})) \equiv 0 \pmod 2$ for the primes in the previous set (see [Lin05] table 7.1) we get that the residual image is trivial or isomorphic to C_2.
(7) – (8) The set

$$\{3, 7, 11, 13, 17, 19, 23, 29, 47, 59, 67, 71, 89, 97, 101, 103, 107, 109, 149, 157, 163,$$
$$191, 193, 211, 293, 311, 317, 359, 443, 577, 607, 617, 653, 691, 701\}$$

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.
(9) – (10) From [Lin05, Table 7.5] we see that the eigenvalues for the Atkin-Lehner involutions $\mathcal{W}_{\mathfrak{p}}$ for $\mathfrak{p} = \mathfrak{p}_2$ and $\mathfrak{p}_5$ are 1 and -1 respectively which is minus the trace of Frobenius of $\mathcal{E}$ at this primes. The Hecke eigenvalues of

$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$	$\mathcal{N}\mathfrak{p}$	Basis of $\mathfrak{p}$	$a_{\mathfrak{p}}$	Basis of $\bar{\mathfrak{p}}$	$a_{\bar{\mathfrak{p}}}$
3	$\langle 3\rangle$	-2			293	$\langle 293, 76+\omega\rangle$	-14	$\langle 293, 216+\omega\rangle$	-30
5	$\langle 5, 1+\omega\rangle$	-1	$\langle 5, 3+\omega\rangle$	3	349	$\langle 349, 83+\omega\rangle$	2	$\langle 349, 265+\omega\rangle$	18
7	$\langle 7, 2+\omega\rangle$	-5	$\langle 7, 4+\omega\rangle$	-3	379	$\langle 379, 61+\omega\rangle$	-28	$\langle 379, 317+\omega\rangle$	-12
11	$\langle 11\rangle$	10			431	$\langle 431, 205+\omega\rangle$	-36	$\langle 431, 225+\omega\rangle$	4
10	$\langle 13\rangle$	-10			521	$\langle 521, 64+\omega\rangle$	6	$\langle 521, 456+\omega\rangle$	6
17	$\langle 17\rangle$	-2			577	$\langle 577, 217+\omega\rangle$	-10	$\langle 577, 359+\omega\rangle$	-42
19	$\langle 19, 5+\omega\rangle$	-7	$\langle 19, 13+\omega\rangle$	3	607	$\langle 607, 291+\omega\rangle$	-8	$\langle 607, 315+\omega\rangle$	40
23	$\langle 23\rangle$	-10			653	$\langle 653, 157+\omega\rangle$	-30	$\langle 653, 495+\omega\rangle$	50
29	$\langle 29\rangle$	-10			839	$\langle 839, 252+\omega\rangle$	32	$\langle 839, 586+\omega\rangle$	48
37	$\langle 37\rangle$	-38			857	$\langle 857, 109+\omega\rangle$	-10	$\langle 857, 747+\omega\rangle$	22
41	$\langle 41, 12+\omega\rangle$	-9	$\langle 41, 28+\omega\rangle$	-1	1031	$\langle 1031, 101+\omega\rangle$	-24	$\langle 1031, 929+\omega\rangle$	-24
43	$\langle 43\rangle$	-18			1063	$\langle 1063, 172+\omega\rangle$	-36	$\langle 1063, 890+\omega\rangle$	20
47	$\langle 47, 21+\omega\rangle$	0	$\langle 47, 25+\omega\rangle$	0	1117	$\langle 1117, 465+\omega\rangle$	-50	$\langle 1117, 651+\omega\rangle$	-18
53	$\langle 53\rangle$	42			1303	$\langle 1303, 222+\omega\rangle$	40	$\langle 1303, 1080+\omega\rangle$	-56
59	$\langle 59, 10+\omega\rangle$	7	$\langle 59, 48+\omega\rangle$	-3	1451	$\langle 1451, 142+\omega\rangle$	-52	$\langle 1451, 1308+\omega\rangle$	-20
67	$\langle 67, 30+\omega\rangle$	-8	$\langle 67, 36+\omega\rangle$	0	1493	$\langle 1493, 382+\omega\rangle$	-14	$\langle 1493, 1110+\omega\rangle$	-30
71	$\langle 71, 26+\omega\rangle$	1	$\langle 71, 44+\omega\rangle$	-9	1619	$\langle 1619, 577+\omega\rangle$	28	$\langle 1619, 1041+\omega\rangle$	-52
73	$\langle 73\rangle$	2			1741	$\langle 1741, 727+\omega\rangle$	74	$\langle 1741, 1013+\omega\rangle$	26
79	$\langle 79\rangle$	70			2003	$\langle 2003, 141+\omega\rangle$	-36	$\langle 2003, 1861+\omega\rangle$	-20
89	$\langle 89\rangle$	-50			2153	$\langle 2153, 404+\omega\rangle$	30	$\langle 2153, 1748+\omega\rangle$	30
109	$\langle 109, 14+\omega\rangle$	-13	$\langle 109, 94+\omega\rangle$	7	2333	$\langle 2333, 571+\omega\rangle$	94	$\langle 2333, 1761+\omega\rangle$	-34
127	$\langle 127\rangle$	-254			2707	$\langle 2707, 1053+\omega\rangle$	68	$\langle 2707, 1653+\omega\rangle$	-60
131	$\langle 131, 60+\omega\rangle$	4	$\langle 131, 70+\omega\rangle$	4	2767	$\langle 2767, 769+\omega\rangle$	-40	$\langle 2767, 1997+\omega\rangle$	8
149	$\langle 149, 38+\omega\rangle$	18	$\langle 149, 110+\omega\rangle$	2	2963	$\langle 2963, 1055+\omega\rangle$	0	$\langle 2963, 1907+\omega\rangle$	24
173	$\langle 173, 41+\omega\rangle$	10	$\langle 173, 131+\omega\rangle$	-6	3119	$\langle 3119, 665+\omega\rangle$	72	$\langle 3119, 2453+\omega\rangle$	-8
193	$\langle 193, 55+\omega\rangle$	11	$\langle 193, 137+\omega\rangle$	-21	3373	$\langle 3373, 857+\omega\rangle$	10	$\langle 3373, 2515+\omega\rangle$	90
227	$\langle 227, 106+\omega\rangle$	-12	$\langle 227, 120+\omega\rangle$	20	3767	$\langle 3767, 513+\omega\rangle$	32	$\langle 3767, 3253+\omega\rangle$	-80
283	$\langle 283, 47+\omega\rangle$	-20	$\langle 283, 235+\omega\rangle$	-20					

TABLE 6.3. Values of $a_{\mathfrak{p}}$ used to prove modularity in the C_3 example.

the automorphic form at the primes $\bar{\mathfrak{p}}_2, \bar{\mathfrak{p}}_5$ and $\mathfrak{p}_{31}$ are $1, 0$ and 4 respectively, which also coincide with the elliptic curve $a_{\mathfrak{p}}$ in such primes, hence the two L-series agree.

Remark 12. We apply our routine to the curve over $\mathbb{Q}[\sqrt{-3}]$ of conductor $\left(\frac{17+\sqrt{-3}}{2}\right)$ considered by Taylor and got the same set of primes needed to prove modularity, as expected.

6.3. **Image isomorphic to C_3.** Let $K = \mathbb{Q}[\sqrt{-31}]$ and $\omega = \frac{1+\sqrt{-31}}{2}$. Let $\mathcal{E}$ be the elliptic curve with equation

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

It has conductor $\mathfrak{n}_{\mathcal{E}} = \mathfrak{p}_2^3\bar{\mathfrak{p}}_2^2$ where $\mathfrak{p}_2 = \langle 2, \omega\rangle$. There is an automorphic form of the same level and trivial character (denoted by f_5 in [Lin05] table 7.4) 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 with $L(f,s)$ at all primes except (at most) $\{\mathfrak{p}_{31}, \bar{\mathfrak{p}}_2, \mathfrak{p}_2\}$. Let $\rho_{\mathcal{E}}$ be the 2-adic Galois representation attached to $\mathcal{E}$. Its residual representation has image isomorphic to C_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 GP routine `Setofprimes`, we find that the set of primes of $\mathbb{Q}[\sqrt{-31}]$ above

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 89, 109, 127, 131, 149,$$
$$173, 193, 227, 283, 293, 349, 379, 431, 521, 577, 607, 653, 839, 857, 1031, 1063, 1117,$$
$$1303, 1451, 1493, 1619, 1741, 2003, 2153, 2333, 2707, 2767, 2963, 3119, 3373, 3767\}$$

is enough for proving that the residual representations are isomorphic and that the 2-adic representations are isomorphic as well. The values of the $a_{\mathfrak{p}}$ for these primes are listed in Table 6.3 which was computed by Professor Cremona (using

some Magma code written by himself and Lingham) and sent to us on a private communication. He also checked that these values match the elliptic curve ones, which proves modularity in this case. To prove that the answer is correct, we apply the algorithm described in section 2.3:

(1) The primes above 131 and 149 prove that the residual representation of the automorphic form lies in $\mathrm{GL}_2(\mathbb{F}_2)$, because the values of $a_{\mathfrak{p}_{131}}, a_{\bar{\mathfrak{p}}_{131}}, a_{\mathfrak{p}_{149}}$ and $a_{\bar{\mathfrak{p}}_{149}}$ are $4, 4, 18, 2$ respectively. They satisfy the hypothesis of Theorem 5.1 and the degree 4 extension of $\mathbb{Q}$ obtained has equation $x^4 - 28x^3 + 684x^2 - 6832x + 24992$, where the prime 2 factors as the product of two ramified primes.
(2) Since 2 is unramified in $K/\mathbb{Q}$, the modulus is $\mathfrak{m}_K = 2^3.\sqrt{-31}$. We compute this ray class group and find that $Cl(\mathcal{O}_K, \mathfrak{m}_K) \simeq C_{30} \times C_6 \times C_2 \times C_2$.
(3) The group of cubic characters has as dual basis for $Cl(\mathcal{O}_K, \mathfrak{m}_K)$ the characters $\{\chi_1, \chi_2\}$. On the routine basis, the cubic character (up to squares) that correspond to $L_{\mathcal{E}}$ is χ_1.
(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 $C = \{\mathfrak{p}_5, \bar{\mathfrak{p}}_5, \mathfrak{p}_7, \bar{\mathfrak{p}}_7\}$ satisfies the desired properties.
(5) The traces of the Frobenius at these primes are odd (see Table 6.3). Hence the residual image is isomorphic to C_3.
(6) Since there is only one other cubic character (χ_2), it turns out that $\chi_1(\mathfrak{p}_3) = 1$, but $\chi_2(\mathfrak{p}_3) \neq 0$. Since $\mathrm{Tr}(\rho_f(\mathrm{Frob}_{\mathfrak{p}_3})) \equiv \mathrm{Tr}(\rho_{\mathcal{E}}(\mathrm{Frob}_{\mathfrak{p}_3}))\pmod 2$, the two residual representations are isomorphic.
(7) As in the previous example, Livne's method implies that the primes above the primes in the set

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 89, 109, 127, 131, 149,$$
$$173, 193, 227, 283, 293, 349, 379, 431, 521, 577, 607, 653, 839, 857, 1031, 1063, 1117,$$
$$1303, 1451, 1493, 1619, 1741, 2003, 2153, 2333, 2707, 2767, 2963, 3119, 3373, 3767\}$$

are enough to prove modularity.
(8) From [Lin05, Table 7.5] we see that the eigenvalues for the Atkin-Lehner involutions $\mathcal{W}_{\mathfrak{p}}$ for $\mathfrak{p} = \mathfrak{p}_2$ and $\bar{\mathfrak{p}}_2$ are 0 which is the trace of Frobenius of $\mathcal{E}$ at these primes. The Hecke eigenvalues of the automorphic form at the prime $\mathfrak{p}_{31}$ is 0 which also coincide with the elliptic curve $a_{\mathfrak{p}}$, hence the two L-series agree.

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, 6, 3]
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+8);
? Setofprimes(K,[w,-1,0,-w-6,0],[2,5])
Case = C_2 or trivial
Primes for proving that the residual representation lies on F_2:
 [41, 47]
Class group of K:  [60, 12, 2, 2, 2, 2]
There are 64 subgroups of Cl_K of index <= 2
Primes proving C_2 or trivial case [3, 7, 11, 13, 17, 19]
Livne's method output:[3, 7, 11, 13, 17, 19, 23, 29, 47, 59, 67, 71,
89, 97, 101, 103, 107, 109, 149, 157, 163, 191, 193, 211, 293, 311,
317, 359, 443, 577, 607, 617, 653, 691, 701]
%3 = [3, 7, 11, 13, 17, 19, 23, 29, 41, 47, 59, 67, 71, 89, 97, 101,
103, 107, 109, 149, 157, 163, 191, 193, 211, 293, 311, 317, 359,
443, 577, 607, 617, 653, 691, 701]
```

7.3. **Trivial residual image or image isomorphic to C_3.**

```
? read(routines);
? K=bnfinit(w^2-w+8);
? Setofprimes(K,[0,-1,0,3-w,-3],[2])
Case = C_3
Primes for proving that the residual representation lies on F_2:
 [131, 149]
Class group of K:  [30, 6, 2, 2]
Primes proving C_3 image:  [131, 149, 5, 7]
Cubic character on K basis:  [1; 0]
Primes proving C_3 extension of K_E:  [3]
Livne's method output:[3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43,
47, 53, 59, 67, 71, 73, 79, 89, 109, 127, 131, 149, 173, 193, 227,
283, 293, 349, 379, 431, 521, 577, 607, 653, 839, 857, 1031, 1063,
1117, 1303, 1451, 1493, 1619, 1741, 2003, 2153, 2333, 2707, 2767,
2963, 3119, 3373, 3767]
%3 = [3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41, 43, 47, 53, 59, 67,
71, 73, 79, 89, 109, 127, 131, 149, 173, 193, 227, 283, 293, 349,
379, 431, 521, 577, 607, 653, 839, 857, 1031, 1063, 1117, 1303,
1451, 1493, 1619, 1741, 2003, 2153, 2333, 2707, 2767, 2963, 3119,
3373, 3767]
```

References

[BH07] Tobias Berger and Gergely Harcos. l-adic representations associated to modular forms over imaginary quadratic fields. *Int. Math. Res. Not. IMRN*, (23):Art. ID rnm113, 16, 2007.

[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.

[Cre84] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.*, 51(3):275–324, 1984.

[Cre92] J. E. Cremona. Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields. *J. London Math. Soc. (2)*, 45(3):404–416, 1992.

[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. Available from `http://www.warwick.ac.uk/staff/J.E.Cremona/theses/index.html`.

[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`