Алгебра и анализ
Том 24 (2012), № 4

St. Petersburg Math. J.
Vol. 24 (2013), No. 4, Pages 575–589
S 1061-0022(2013)01254-4
Article electronically published on May 24, 2013

ON AN ELLIPTIC CURVE DEFINED OVER $\mathbb{Q}(\sqrt{-23})$

L. V. DIEULEFAIT, M. MINK, AND B. Z. MOROZ

Abstract. Recently, the first three examples were found of elliptic curves without complex multiplication and defined over an imaginary quadratic field that have been proved to satisfy the Hasse–Weil conjecture. In the paper, the same algorithm is employed to prove the modularity and thereby the Hasse–Weil conjecture for the fourth elliptic curve without CM defined over the imaginary quadratic field $\mathbb{Q}(\sqrt{-23})$.

§1. Introduction

1. An elliptic curve over $\mathbb{Q}$, being a modular curve [3], satisfies the Hasse–Weil conjecture. The situation for elliptic curves over other number fields is by far less clear, cf. [23, p. 144], although some progress has been recently made for curves over totally real fields (see, for instance, [11]). The techniques and ideas introduced by A. Wiles [24], and further developed in [3, 11] and the works cited there, could not so far be applied to treat elliptic curves over not totally real fields. In spite of previous efforts of several authors (see [8, 16], [22, Theorem 3], [5, 12], and the references therein), only in the recent paper [7] one finds the first examples of elliptic curves without complex multiplication and defined over an imaginary quadratic field that have been proved to satisfy the Hasse–Weil conjecture. The algorithm, described in [7], allows in principle to check the modularity of any of the elliptic curves considered by J. Cremona and his students, see [5, 12] and the works cited there. In this note, another curve from Lingham's list [12, Chapter 7] is proved to be modular. Our exposition depends heavily on the calculations carried out by the second author in her M. Sc. Thesis [13], to which we refer for some further details.

Let K be an imaginary quadratic field of discriminant d_K with the ring of integers $\mathfrak{o}$, and let $\mathcal{P}(K) := \operatorname{Spec}\mathfrak{o} \setminus \{(0)\}$. Let E be an elliptic curve defined over K, and let $\mathfrak{f}(E)$ denote the conductor of E. For $\mathfrak{p} \in \mathcal{P}(K)$, let $E_\mathfrak{p}$ denote the reduction of E modulo $\mathfrak{p}$, and let $L(E,s)$ be the Hasse–Weil L-function of E defined by the Euler product

$$L(E,s) := \prod_{\mathfrak{p}\in\mathcal{P}(K)} l_\mathfrak{p}(E, N\mathfrak{p}^{-s})^{-1} \tag{1}$$

absolutely convergent for $\operatorname{Re} s > 3/2$, where

$$l_\mathfrak{p}(E,t) := 1 - a(\mathfrak{p})t + (N\mathfrak{p})t^2$$

with

$$a(\mathfrak{p}) := N\mathfrak{p} + 1 - |E_\mathfrak{p}|, \quad |a(\mathfrak{p})| \le 2N\mathfrak{p}^{1/2} \tag{2}$$

if $\mathfrak{p} \nmid \mathfrak{f}(E)$, that is if E has good reduction at $\mathfrak{p}$, and

$$l_\mathfrak{p}(E,t) := 1 + a(\mathfrak{p})t$$

with $a(\mathfrak{p}) = 0, 1$, or -1 if E has additive, nonsplit multiplicative, or split multiplicative reduction at $\mathfrak{p}$, respectively.

2010 *Mathematics Subject Classification.* Primary 11G05, 11G40, 14G10.
Key words and phrases. Hasse–Weil conjecture, elliptic curve.

Proposition 1. *Two elliptic curves E and E' over K are isogenous if and only if $l_{\mathfrak{p}}(E,t) = l_{\mathfrak{p}}(E',t)$ for almost all $\mathfrak{p}$ in $\mathcal{P}(K)$.*

Proof. This is a theorem of Faltings [9]. □

The following assertion [19] is a refined form of the classical Hasse–Weil conjecture.

Conjecture 1. *There is an integral function $s \mapsto \Lambda(E,s)$ satisfying the functional equation*

$$\Lambda(E, 2-s) = \varepsilon \Lambda(E,s) \quad \text{for} \quad s \in \mathbb{C} \tag{3}$$

and such that

$$\Lambda(E,s) = A(E)^s \Gamma(s)^2 L(E,s) \quad \text{for} \quad \operatorname{Re} s > 3/2$$

with $A(E) := (2\pi)^{-2}(N\mathfrak{f}(E))^{1/2}|d_K|$ and $\varepsilon \in \{\pm 1\}$.

The following "parity conjecture" is part of the Birch and Swinnerton–Dyer conjecture.

Conjecture 2. *The sign of ε in the functional equation* (3) *is determined by the rank r of the elliptic curve E:*

$$\varepsilon = (-1)^r.$$

2. Let f be an automorphic cusp form on $\mathrm{GL}_2(\mathbb{A}_K)$ of the type $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$ in the sense of Weil [23, p. 143], which is an eigenform for the Hecke operators $T_{\mathfrak{p}}$, say

$$T_{\mathfrak{p}} f = c(\mathfrak{p}) f,$$

with $\mathfrak{p}$ ranging over all primes in $\mathcal{P}(K)$ that do not divide $\mathfrak{n}(f)$. One can attach to f a Dirichlet series defined by the Euler product

$$L(f,s) := \prod_{\mathfrak{p} \in \mathcal{P}(K)} l_{\mathfrak{p}}(f, N\mathfrak{p}^{-s})^{-1}, \tag{4}$$

where

$$l_{\mathfrak{p}}(f,t) := 1 - c(\mathfrak{p})t + (N\mathfrak{p})t^2$$

if $\mathfrak{p} \nmid \mathfrak{n}(f)$ and

$$l_{\mathfrak{p}}(f,t) := 1 + c(\mathfrak{p})t$$

with $c(\mathfrak{p}) \in \{0, \pm 1\}$ if $\mathfrak{p} \mid \mathfrak{n}(f)$.

Conjecture 3. *The eigenvalues $c(\mathfrak{p})$ satisfy the following inequality:*

$$|c(\mathfrak{p})| \le 2N\mathfrak{p}^{1/2}.$$

Conjecture 3 may be regarded as a generalized Ramanujan–Petersson conjecture; it has not been proved, although the Euler product (4) is known [10] to converge absolutely for $\operatorname{Re} s > 3/2$. The Ramanujan–Petersson conjecture for classical modular forms was proved by P. Deligne many years ago [6].

Proposition 2. *With f as above, there is an integral function $s \mapsto \Lambda(f,s)$, satisfying the functional equation*

$$\Lambda(f, 2-s) = \varepsilon \Lambda(f,s) \quad \text{for} \quad s \in \mathbb{C} \tag{5}$$

and such that

$$\Lambda(f,s) = A(f)^s \Gamma(s)^2 L(f,s) \quad \text{for} \quad \operatorname{Re} s > 3/2$$

with $A(f) := (2\pi)^{-2}(N\mathfrak{n}(f))^{1/2}|d_K|$ and $\varepsilon \in \{\pm 1\}$. Moreover, $\varepsilon = -\varepsilon_0$, where ε_0 is the eigenvalue of the Fricke involution.

Proof. Let $f, \widetilde{f}$ be an automorphic pair in the sense of [23]. Since f is an automorphic form of the type $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$, it follows that $\widetilde{f}$ is an eigenform for the Hecke operators with the same eigenvalues as f [23, p. 45]. Therefore, $\widetilde{f} = \lambda f$ with $\lambda \in \mathbb{C}^*$ by the strong multiplicity one theorem [15] (cf. also [10]). Since $\widetilde{f} = Jf$, where J is the Fricke involution, the assertion follows from [23, Theorem 6]. □

Definition 1. An automorphic cusp eigenform f on $\mathrm{GL}_2(\mathbb{A}_K)$ of the type $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$ is said to be attached to an elliptic curve E over K if

$$l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t) \quad \text{for} \quad \mathfrak{p} \in \mathcal{P}(K);$$

this binary relation will be denoted by $[E, f]$. An elliptic curve E is a modular curve if the relation $[E, f]$ is satisfied for an automorphic form f.

Definition 2. An automorphic cusp eigenform f on $\mathrm{GL}_2(\mathbb{A}_K)$ is rational if $l_\mathfrak{p}(f,t) \in \mathbb{Q}[t]$ for $\mathfrak{p} \in \mathcal{P}(K)$.

Corollary 1. *Let E be a modular curve, and let f be an automorphic form attached to E. Then f is a rational form, $\mathfrak{n}(f) = \mathfrak{f}(E)$, the elliptic curve E satisfies Conjecture* 1*, and the automorphic form f satisfies Conjecture* 3*.*

Proof. The assertion follows from Proposition 2 and the Hasse estimate (2). □

Corollary 2. *Two modular elliptic curves E and E' are isogenous if and only if there is an automorphic form f such that both relations $[E, f]$ and $[E', f]$ hold true.*

Proof. This follows from Proposition 1, in view of the strong multiplicity one theorem [15, 10]. □

3. Let $G_K := \mathrm{Gal}(\bar{K}|K)$ be the (absolute) Galois group of K, and let $\varphi(\mathfrak{p})$ stand for the Frobenius class in G_K of a prime $\mathfrak{p}$ in $\mathcal{P}(K)$. Let $T(E)$ be the dyadic Tate module, let $V(E) := T(E) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$, and let

$$\rho_E \,:\, G_K \to \mathrm{Aut}\, V(E)$$

be the two-dimensional dyadic Galois representation, describing the action of the group G_K on the $\mathbb{Q}_2$-vector space $V(E)$. Let $\mathfrak{p} \in \mathcal{P}(K)$; if $\mathfrak{p} \nmid 2\mathfrak{f}(E)$, then the representation ρ_E is unramified at $\mathfrak{p}$ and the characteristic polynomial of $\rho_E(\varphi(\mathfrak{p}))$ is equal to $l_\mathfrak{p}(E,t)$, that is

$$\mathrm{Tr}\, \rho_E(\varphi(\mathfrak{p})) = a(\mathfrak{p}) \quad \text{and} \quad \det \rho_E(\varphi(\mathfrak{p})) = N\mathfrak{p}.$$

Moreover, $\rho_E(G_K) \subseteq \mathrm{Aut}\, T(E)$ with $\mathrm{Aut}\, T(E) \cong \mathrm{GL}_2(\mathbb{Z}_2)$; in what follows we shall assume, without loss of generality, that

$$\rho_E(G_K) \subseteq \mathrm{GL}_2(\mathbb{Z}_2).$$

If a curve E has no complex multiplication, then the representation ρ_E is irreducible. The proof of those by now well-known results can be found, for instance, in [18].

Remark. Let E and E' be two elliptic curves without complex multiplication defined over K, and suppose that

$$L(E,s) = L(E',s); \tag{6}$$

then from Proposition 1 it follows that the curve E' is isogenous either to E or to $\bar{E}$, where $\bar{E}$ stands for the elliptic curve obtained from E by complex conjugation. Let ρ_1, ρ_2, ρ_3, and ρ_4 be the irreducible two-dimensional dyadic Galois representation, describing the action of the group G_K on $V(E)$, $V(\bar{E})$, $V(E')$, and $V(\bar{E}')$, respectively. In view of the Chebotarev density theorem and [2, §12, no. 1, Proposition 3], equation (6) implies that

$$\rho_1 \oplus \rho_2 \cong \rho_3 \oplus \rho_4;$$

therefore, either $\rho_3 \cong \rho_1$ or $\rho_3 \cong \rho_2$. By Proposition 1, this implies that the curve E' is isogenous either to E (in the first case) or to $\bar{E}$ (in the second case).

Let $\rho_f : G_K \to \mathrm{GL}_2(\bar{\mathbb{Q}}_2)$ be the irreducible two-dimensional dyadic Galois representation associated with a rational automorphic cusp eigenform f on $\mathrm{GL}_2(\mathbb{A}_K)$ of the type $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$. Without loss of generality it may be assumed that

$$\rho_f(G_K) \subseteq \mathrm{GL}_2(O_R),$$

where O_R is the ring of integers of a field R with

$$\mathbb{Q}_2 \subseteq R \subseteq \bar{\mathbb{Q}}_2, \quad [R : \mathbb{Q}_2] \leq 4.$$

Let $\mathfrak{n}_1(f) := (2d_K) \cdot \mathfrak{n}(f)$. If $\mathfrak{p} \nmid \mathfrak{n}_1(f)$, then the representation ρ_f is unramified at $\mathfrak{p}$ and the characteristic polynomial of $\rho_f(\varphi(\mathfrak{p}))$ is equal to $l_\mathfrak{p}(f,t)$, that is

$$\mathrm{Tr}\, \rho_f(\varphi(\mathfrak{p})) = c(\mathfrak{p}) \quad \text{and} \quad \det \rho_f(\varphi(\mathfrak{p})) = N\mathfrak{p}.$$

Moreover, given two primes $\mathfrak{p}$, $\mathfrak{q}$ in $\mathcal{P}(K)$ such that $\mathfrak{p} \nmid \mathfrak{n}_1(f)$, $\mathfrak{q} \nmid \mathfrak{n}_1(f)$, and

$$l_\mathfrak{p}(f,t) = (1 - \alpha(\mathfrak{p})t)(1 - \beta(\mathfrak{p})t), \quad l_\mathfrak{q}(f,t) = (1 - \alpha(\mathfrak{q})t)(1 - \beta(\mathfrak{q})t)$$

with $c(\mathfrak{q}) \neq 0$ and $\alpha(\mathfrak{p}) \neq \beta(\mathfrak{p})$, one can actually take

$$R = \mathbb{Q}_2(\alpha(\mathfrak{p}), \alpha(\mathfrak{q})). \tag{7}$$

The cited results were proved in the recent papers [22, 1].

Definition 3. Let E be an elliptic curve over K, and let f be a rational automorphic cusp eigenform on $\mathrm{GL}_2(\mathbb{A}_K)$ of the type $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$. The pair (E, f) is a suitable pair if

$$\mathfrak{f}(E) = \mathfrak{n}(f) \quad \text{and} \quad l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t) \quad \text{for} \quad \mathfrak{p} \mid \mathfrak{n}_1(f), \quad \mathfrak{p} \in \mathcal{P}(K).$$

Lemma 1. *An automorphic form f is attached to an elliptic curve E if and only if (E, f) is a suitable pair and $\rho_E \cong \rho_f$.*

Proof. Suppose that (E, f) is a suitable pair, then $\mathfrak{f}(E) = \mathfrak{n}(f)$ and $l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t)$ for $\mathfrak{p} | \mathfrak{n}_1(f)$. If, moreover, $\rho_E \cong \rho_f$, then

$$a(\mathfrak{p}) = \mathrm{Tr}\, \rho_E(\varphi(\mathfrak{p})) = \mathrm{Tr}\, \rho_f(\varphi(\mathfrak{p})) = c(\mathfrak{p})$$

for $\mathfrak{p} \nmid \mathfrak{n}_1(f)$ because $2\mathfrak{f}(E) \mid \mathfrak{n}_1(f)$. Thus,

$$l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t) \quad \text{for} \quad \mathfrak{p} \in \mathcal{P}(K),$$

and therefore $[E, f]$ holds true. Conversely, suppose the relation $[E, f]$ is satisfied. Then

$$l_\mathfrak{p}(E,t) = l_\mathfrak{p}(f,t) \quad \text{for} \quad \mathfrak{p} \in \mathcal{P}(K);$$

therefore, (E, f) is a suitable pair and, moreover,

$$\mathrm{Tr}\, \rho_E(\varphi(\mathfrak{p})) = a(\mathfrak{p}) = c(\mathfrak{p}) = \mathrm{Tr}\, \rho_f(\varphi(\mathfrak{p})) \quad \text{for} \quad \mathfrak{p} \nmid \mathfrak{n}_1(f), \quad \mathfrak{p} \in \mathcal{P}(K). \tag{8}$$

By the Chebotarev density theorem, from (8) it follows that the set

$$\{\sigma \mid \sigma \in G_K, \ \mathrm{Tr}\, \rho_E(\sigma) = \mathrm{Tr}\, \rho_f(\sigma)\}$$

is a dense subset of G_K, whence $\mathrm{Tr}\, \rho_E = \mathrm{Tr}\, \rho_f$ and, consequently, $\rho_E \cong \rho_f$ because the representations ρ_E and ρ_f, being irreducible, are semisimple, cf. [2, §12, no. 1, Proposition 3]. This proves the lemma. □

Notation 1. Let $|S|$ stand for the cardinality of a set S; let $\mathrm{ord}(g)$ denote the order of a group element g; let $\widehat{G}$ stand for the group of characters of an Abelian group G. Let $\mathcal{C}_n$ denote the cyclic group of order n; let $\mathfrak{S}_n$ and $\mathfrak{A}_n$ denote the symmetric and the alternating groups of permutations of n symbols, respectively. Let $\mathcal{A}^*$ denote the multiplicative group of a ring $\mathcal{A}$. As usual, let $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$, and $\mathbb{F}_q$ stand for the field of rational numbers, the ring of rational integers, the monoid of positive rational integers, and the finite field of q elements, respectively; the set of the rational primes is denoted by P. The algebraic closure of a field k is denoted by $\bar{k}$; let $[L:k]$ stand for the degree of a finite extension of fields $L|k$, let $G(L|k)$ denote the Galois group of a normal extension $L|k$, and let $G_k := G(\bar{k}|k)$. A number field is a finite extension of $\mathbb{Q}$; given a number field k, let $\mathfrak{o}_k$ denote its ring of integers, let d_k be the discriminant of k, let $\mathcal{P}(k) := \mathrm{Spec}\,\mathfrak{o}_k \setminus \{(0)\}$, and let $\varphi(\mathfrak{p})$ stand for the Frobenius class in G_k of a prime $\mathfrak{p}$ in $\mathcal{P}(k)$ as above.

§2. Preliminaries and formulation of the main results

Now, let $K = \mathbb{Q}(\sqrt{-23})$, then $\mathfrak{o}_K = \mathbb{Z} \oplus \omega\mathbb{Z}$ with

$$\omega := \frac{1+\sqrt{-23}}{2}$$

and $d_K = -23$; the class number of K is equal to 3.

Notation 2. For $p \in P$, let $\mathfrak{p}_p$ stand for a prime in $\mathcal{P}(K)$ dividing p; if p splits in K, we denote by $\bar{\mathfrak{p}}_p$ the other prime in $\mathcal{P}(K)$ dividing p. Thus, for instance, $23\mathfrak{o}_K = \mathfrak{p}_{23}^2$, $3\mathfrak{o}_K = \mathfrak{p}_3\bar{\mathfrak{p}}_3$, and $5\mathfrak{o}_K = \mathfrak{p}_5$.

M. Lingham [12] compiled a list of 46 suitable pairs and checked that

$$l_{\mathfrak{p}}(E,t) = l_{\mathfrak{p}}(f,t) \text{ for } N\mathfrak{p} < 50, \quad \mathfrak{p} \in \mathcal{P}(K),$$

for each pair (E,f) in his list. From now on, let E stand for the elliptic curve defined by the equation

$$E : y^2 + (\omega+1)xy + y = x^3 + (\omega+1)x^2 - 7x + (5-3\omega), \tag{9}$$

and let f be the modular form f_{44} in Lingham's list [12, Chapter 7], with $a(\mathfrak{p})$ and $c(\mathfrak{p})$ defined as in §1.

Lemma 2. *The following assertions hold true*:

1. *E is an elliptic curve of rank* 1 *without complex multiplication.*
2. *f is a rational automorphic cusp eigenform on* $\mathrm{GL}_2(\mathbb{A}_K)$ *of type* $(1, \mathfrak{n}(f), \mathcal{H}_\infty)$.
3. *The eigenvalue ε_0 of the Fricke involution is equal to* 1, *so that $\varepsilon = -1$ in the functional equation* (5).
4. *The pair (E,f) is a suitable pair with*

$$\mathfrak{f}(E) = \mathfrak{n}(f) = \mathfrak{p}_2\mathfrak{p}_3^3\bar{\mathfrak{p}}_3, \quad \mathfrak{n}_1(f) := (46)\cdot\mathfrak{n}(f), \text{ and } a(\mathfrak{p}) = c(\mathfrak{p}) \text{ for}$$

   $N\mathfrak{p} < 50, \quad \mathfrak{p} \in \mathcal{P}(K)$.

5. *Moreover,*

$$\begin{aligned} &c(\mathfrak{p}_2) = c(\mathfrak{p}_5) = 1, \ \ c(\bar{\mathfrak{p}}_2) = c(\mathfrak{p}_{13}) = -2, \ \ c(\mathfrak{p}_3) = 0,\\ &c(\bar{\mathfrak{p}}_3) = c(\bar{\mathfrak{p}}_{13}) = c(\mathfrak{p}_{23}) = -1, \ \ c(\mathfrak{p}_7) = 6, \ \ c(\mathfrak{p}_{29}) = -6,\\ &c(\bar{\mathfrak{p}}_{29}) = -9, \ \ c(\mathfrak{p}_{31}) = c(\bar{\mathfrak{p}}_{47}) = 3, \ \ c(\bar{\mathfrak{p}}_{31}) = -10,\\ &c(\mathfrak{p}_{41}) = -8, \ \ c(\bar{\mathfrak{p}}_{41}) = c(\mathfrak{p}_{47}) = 5. \end{aligned}$$

Proof. See [12, Chapter 7]. □

Theorem 1. *The automorphic form f is attached to the elliptic curve E.*

Theorem 1 is the main result of this work. In view of Lemmas 1 and 2, it can be deduced from the following theorem, which is proved in the last section.

Theorem 2. *The representations ρ_E and ρ_f are equivalent.*

Corollary 3. *The elliptic curve E satisfies Conjectures* 1 *and* 2 *and the automorphic form f satisfies Conjecture* 3.

Proof. This follows from Theorem 1, Corollary 1, and Lemma 2.

By (7) and Lemma 2, it may be assumed that

$$R = \mathbb{Q}_2(\alpha(\mathfrak{p}_{41}), \alpha(\bar{\mathfrak{p}}_{31})) = \mathbb{Q}_2(\sqrt{-1}, \sqrt{-6})$$

with $O_R/\mathfrak{m}_R \cong \mathbb{F}_2$, where $\mathfrak{m}_R$ denotes the maximal ideal of O_R. Since

$$\rho_E(G_K) \subseteq \mathrm{GL}_2(\mathbb{Z}_2) \text{ and } \rho_f(G_K) \subseteq \mathrm{GL}_2(O_R),$$

one can reduce those representations modulo 2 and modulo $\mathfrak{m}_R$, respectively; let

$$\bar{\rho}_E : G_K \to \mathrm{GL}_2(\mathbb{F}_2) \text{ and } \bar{\rho}_f : G_K \to \mathrm{GL}_2(\mathbb{F}_2)$$

be the residual representations. □

Proposition 3. *The representations $\bar{\rho}_E$ and $\bar{\rho}_f$ are equivalent.*

Proposition 3 will be proved in the next section. In §4 we shall explain the so-called Faltings–Serre method, to be used in the proof of Theorem 2 in the last section.

§3. Equivalence of the residual representations

1. We start with a few simple observations. First of all,

$$\mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) \text{ and } \mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3.$$

Lemma 3. *Any two representations*

$$\rho_1, \rho_2 : \mathfrak{S}_3 \to \mathrm{GL}_2(\mathbb{F}_2)$$

with

$$\operatorname{Ker}\rho_1 = \operatorname{Ker}\rho_2 = \mathcal{C}_1$$

are equivalent.

Proof. It can easily be checked.

Clearly, $\operatorname{Ker}\bar{\rho}_E = G_L$ and $\operatorname{Ker}\bar{\rho}_f = G_{L'}$ for two finite normal extensions $L \mid K$ and $L' \mid K$ with

$$\bar{\rho}_E(G_K) \cong G(L|K) \quad \text{and} \quad \bar{\rho}_f(G_K) \cong G(L'|K).$$ □

Lemma 4. *Let $f(t) := t^4 - t^3 + 8t^2 - t + 1$, then $L = K_1 \cdot K_2$ with*

$$[K_1 : K] = 3, \ \ [K_2 : K] = 2, \ \ K_2 \cong \mathbb{Q}[t]/(f(t)), \ \ G(L|K) \cong \mathfrak{S}_3,$$

and $d_L = 2^{13} \cdot 3^7 \cdot 23^6$. In particular, $\bar{\rho}_E(G_K) = \mathrm{GL}_2(\mathbb{F}_2)$.

Proof. On rewriting equation (9) in the Weierstrass form

$$E : y^2 = F(x), \quad F(t) := t^3 + \frac{7\omega - 1}{4}t^2 + \frac{\omega - 13}{2}t + \frac{21}{4} - 3\omega = \prod_{i=1}^{3}(t - \alpha_i),$$

one concludes that $L = K(\alpha_1, \alpha_2, \alpha_3)$ and sets $K_1 := K(\alpha_1)$. Then, a straightforward calculation [14] establishes the claim. □

Notation 3. Let $\mathfrak{N} := \{\mathfrak{p}_{23}, \mathfrak{p}_2, \bar{\mathfrak{p}}_2, \mathfrak{p}_3, \bar{\mathfrak{p}}_3\}$, $\mathfrak{N} \subseteq \mathcal{P}(K)$.

Corollary 4. *The field extensions $L|K$ and $L'|K$ are unramified at primes in $\mathcal{P}(K) \setminus \mathfrak{N}$.*

Proof. The extension $L|K$ is unramified by Lemma 4, and the extension $L'|K$ is unramified because $\mathfrak{n}_1(f) = (46)\mathfrak{p}_2\mathfrak{p}_3^3\bar{\mathfrak{p}}_3$ by Lemma 2. □

Lemma 5. *Let $g \in \mathrm{GL}_2(\mathbb{F}_2)$, then $\mathrm{Tr}\, g = 0$ if and only if $g^2 = 1$.*

Proof. It is clear. □

Corollary 5. *We have*

$$|\bar{\rho}_f(G_K)| \notin \{1, 2\}.$$

Proof. Since $\mathrm{Tr}\, \bar{\rho}_f(\varphi(\mathfrak{p}_5)) = 1$ by Lemma 2, the assertion follows from Lemma 5. □

Notation 4. Let k be a number field. We denote by $I(k)$ and $I_0(k)$ the group of fractional ideals of k and the monoid of nonzero ideals of $\mathfrak{o}_k$, respectively. For $\mathfrak{a} \in I_0(k)$, let

$$J(\mathfrak{a}) := \big\{\mathfrak{A} \mid \mathfrak{A} = \mathfrak{B}\mathfrak{C}^{-1}, \quad \mathfrak{B} \in I_0(k), \quad \mathfrak{C} \in I_0(k), \quad (\mathfrak{B}\mathfrak{C}, \mathfrak{a}) = (1)\big\},$$
$$Pr(\mathfrak{a}) := \big\{(\alpha) \mid \alpha \in k^*, \quad \alpha = 1 \bmod \mathfrak{a}\big\}, \quad H(\mathfrak{a}) := J(\mathfrak{a})/Pr(\mathfrak{a}),$$

and let $k(\mathfrak{a})$ denote the ray class field corresponding to the ray class group $H(\mathfrak{a})$. Let $\mathfrak{f}(L|k)$ denote the conductor of a finite Abelian extension $L|k$. By a slight abuse of language, we shall often identify $\widehat{H}(\mathfrak{a})$ with $\widehat{G}(k(\mathfrak{a})|k)$. Given a finite extension $L|k$ of the field k and primes $\mathfrak{P}$ in $\mathcal{P}(L)$, $\mathfrak{p}$ in $\mathcal{P}(k)$ with $\mathfrak{P}|\mathfrak{p}$, let $e(\mathfrak{P}, \mathfrak{p})$ and $f(\mathfrak{P}, \mathfrak{p})$ stand for the ramification index and the inertia degree of the prime $\mathfrak{P}$ in the extension $L|k$, respectively; if $L|k$ is a normal extension, let $f_L(\mathfrak{p})$, $\mathfrak{p} \in \mathcal{P}(k)$, stand for the common value of the numbers $f(\mathfrak{P}, \mathfrak{p})$, $\mathfrak{P} \in \mathcal{P}(L)$, $\mathfrak{P}|\mathfrak{p}$.

Lemma 6. *Let $T|k$ be a cyclic extension of number fields of degree $l := [T : k]$, $l \in P$. Then*

$$\mathfrak{f}(T|k) = \prod_{\mathfrak{p} \in \mathcal{P}(k)} \mathfrak{p}^{\alpha(\mathfrak{p})}, \quad \alpha(\mathfrak{p}) \in \mathbb{Z},$$

with

$$\alpha(\mathfrak{p}) \in \{0, 1\} \quad \text{if} \quad \mathfrak{p} \nmid l, \quad 2 \le \alpha(\mathfrak{p}) \le \frac{le(\mathfrak{p}, l)}{l - 1} + 1 \quad \text{if} \quad \mathfrak{p} \mid l.$$

Proof. See [4, pp. 149–150, 487]. □

2. Let

$$\mathfrak{m} := (\mathfrak{p}_2\bar{\mathfrak{p}}_2)^3(\mathfrak{p}_3\bar{\mathfrak{p}}_3)^2\mathfrak{p}_{23}, \quad \mathfrak{m} \in I_0(K).$$

Lemma 7. *The group $\bar{\rho}_f(G_K)$ is not isomorphic to $\mathcal{C}_3$.*

Proof. Let $\mathcal{P}_0 := \{\mathfrak{p}_7, \mathfrak{p}_{13}\}$, then $\mathcal{P}_0 \subseteq \mathcal{P}(K) \setminus \mathfrak{N}$; moreover, Lemma 2 implies that

$$\mathrm{Tr}\, \bar{\rho}_f(\varphi(\mathfrak{q})) = 0 \ \text{ for } \ \mathfrak{q} \in \mathcal{P}_0. \tag{10}$$

Suppose that $|\bar{\rho}_f(G_K)| = 3$. Then $L'|K$ is a cyclic cubic extension; therefore, from Lemma 6 and Corollary 4 it follows that

$$K \subseteq L' \subseteq K(\mathfrak{m}).$$

Let $\chi \in \widehat{H}(\mathfrak{m})$ with $\mathrm{Ker}\, \chi = G(K(\mathfrak{m})|L')$, then $\mathrm{ord}(\chi) = 3$. On the other hand, [14] shows that $\chi(\mathfrak{p}) \ne 1$ for some $\mathfrak{p}$ in $\mathcal{P}_0$; therefore $\mathrm{ord}(\bar{\rho}_f(\varphi(\mathfrak{p})|L')) = 3$, so that $\mathrm{Tr}\, \bar{\rho}_f(\varphi(\mathfrak{p})) = 1$ by Lemma 5, in contradiction with (10). Thus, $|\bar{\rho}_f(G_K)| \ne 3$. This proves the lemma. □

Corollary 6. *We have*

$$\bar{\rho}_f(G_K) = \mathrm{GL}_2(\mathbb{F}_2).$$

Proof. This follows from Corollary 5 and Lemma 7. □

Lemma 8. *There is a representation $\widehat{\rho}_f : G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ that is equivalent to ρ_f.*

Proof. By Corollary 6, the residual representation $\bar{\rho}_f$ is absolutely irreducible. Moreover, the Chebotarev density theorem and Lemma 2 show that $\operatorname{Tr}\rho_f(G_K) \subseteq \mathbb{Q}_2$. On the other hand, $\rho_f(G_K) \subseteq \mathrm{GL}_2(O_R)$ and $O_R \cap \mathbb{Q}_2 = \mathbb{Z}_2$, whence $\operatorname{Tr}\rho_f(G_K) \subseteq \mathbb{Z}_2$. The assertion of the lemma can now be deduced from [21, Corollaire 5] (cf. [7, Theorem 5.5]). □

By Lemma 4 and Corollary 6, $G(L|K) \cong \mathfrak{S}_3$ and $G(L'|K) \cong \mathfrak{S}_3$; therefore, there are unique quadratic extensions $K_2|K$ and $K_2'|K$ such that $K \subseteq K_2 \subseteq L$ and $K \subseteq K_2' \subseteq L'$.

Lemma 9. *The fields K_2 and K_2' coincide.*

Proof. As above, from Lemma 6 and Corollary 4 it follows that

$$K \subseteq K_2 \cdot K_2' \subseteq K(\mathfrak{m}).$$

Let $\{\psi, \psi'\} \subseteq \widehat{H}(\mathfrak{m})$, $\operatorname{Ker}\psi = G(K(\mathfrak{m})|K_2)$, and $\operatorname{Ker}\psi' = G(K(\mathfrak{m})|K_2')$. A prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus \mathfrak{N}$ splits in K_2 (respectively, in K_2') if and only if $\psi(\mathfrak{p}) = 1$ (respectively, $\psi'(\mathfrak{p}) = 1$). Let

$$\mathcal{P}_1 := \{\mathfrak{p}_5, \bar{\mathfrak{p}}_{13}, \bar{\mathfrak{p}}_{29}, \mathfrak{p}_{31}, \bar{\mathfrak{p}}_{41}\};$$

clearly, $\mathcal{P}_1 \subseteq (\mathcal{P}(K) \setminus \mathfrak{N})$. It turns out [14] that

$$H(\mathfrak{m})/H(\mathfrak{m})^2 \cong \mathcal{C}_2^6,$$

the set $\mathcal{P}_1$ generates a subgroup of $H(\mathfrak{m})/H(\mathfrak{m})^2$ isomorphic to $\mathcal{C}_2^5$, and $\psi(\mathfrak{p}) = 1$ for $\mathfrak{p} \in \mathcal{P}_1$. Therefore, if $\psi \neq \psi'$, then $\psi'(\mathfrak{p}_0) = -1$ for some prime $\mathfrak{p}_0$ in $\mathcal{P}_1$. Since $G(L'|K) \cong \mathfrak{S}_3$, the prime $\mathfrak{p}_0$ splits in L', so that

$$\operatorname{ord}(\bar{\rho}_f(\varphi(\mathfrak{p}_0))) = \operatorname{ord}(\bar{\rho}_f(\varphi(\mathfrak{p}_0)|L')) = \operatorname{ord}(\varphi(\mathfrak{p}_0)|L') = 2. \tag{11}$$

By Lemma 5, relation (11) implies that $\operatorname{Tr}\bar{\rho}_f(\varphi(\mathfrak{p}_0)) = 0$ and, consequently,

$$\operatorname{Tr}\rho_f(\varphi(\mathfrak{p})) = c(\mathfrak{p}) = 0 \pmod 2.$$

On the other hand, Lemma 2 implies that $c(\mathfrak{p}) = 1 \pmod 2$ for $\mathfrak{p} \in \mathcal{P}_1$. Thus, $\psi = \psi'$ and $K_2 = K_2'$, as claimed. □

3. The following result is the key lemma in the proof of Proposition 3.

Lemma 10. *The fields L and L' coincide.*

Proof. Let $\mathfrak{N}_1 := \{\mathfrak{q}_2, \bar{\mathfrak{q}_2}, \mathfrak{q}_3, \bar{\mathfrak{q}_3}, \mathfrak{q}_{23}, \overline{\mathfrak{q}_{23}}\}$, $\mathfrak{N}_1 \subseteq \mathcal{P}(K_2)$, where

$$(2) = \mathfrak{q}_2\bar{\mathfrak{q}_2}^2, \quad (3) = \mathfrak{q}_3^2\bar{\mathfrak{q}_3}, \quad (23) = (\mathfrak{q}_{23}\overline{\mathfrak{q}_{23}})^2 \ \text{ in } \ I_0(K_2),$$

and let $\mathfrak{m}_1 := \mathfrak{q}_2\bar{\mathfrak{q}_2}\mathfrak{q}_3^4\bar{\mathfrak{q}_3}^2\mathfrak{q}_{23}\overline{\mathfrak{q}_{23}}$, $\mathfrak{m}_1 \in I_0(K_2)$. By Lemma 6 and Corollary 4,

$$K_2 \subseteq L \cap L' \subseteq L \cdot L' \subseteq K_2(\mathfrak{m}_1).$$

Let $\{\psi, \psi'\} \subseteq \widehat{H}(\mathfrak{m}_1)$, $\operatorname{Ker}\psi = G(K_2(\mathfrak{m}_1)|L)$, and $\operatorname{Ker}\psi' = G(K_2(\mathfrak{m}_1)|L')$. A prime $\mathfrak{q}$ in $\mathcal{P}(K_2) \setminus \mathfrak{N}_1$ splits in L (respectively, in L') if and only if $\psi(\mathfrak{q}) = 1$ (respectively, $\psi'(\mathfrak{q}) = 1$). Let $\mathcal{P}_2 := \{\mathfrak{q}_{13}, \mathfrak{q}_{29}, \bar{\mathfrak{q}}_{29}\}$, where

$$(13) = \mathfrak{p}_{13}\bar{\mathfrak{p}}_{13}, \quad (29) = \mathfrak{p}_{29}\bar{\mathfrak{p}}_{29} \ \text{ in } \ I_0(K)$$

and

$$\mathfrak{q}_{13} = \mathfrak{p}_{13}\mathfrak{o}_{K_2}, \quad \mathfrak{p}_{29} = \mathfrak{q}_{29}\bar{\mathfrak{q}}_{29} \ \text{ in } \ I_0(K_2);$$

then $\mathcal{P}_2 \subseteq \mathcal{P}(K_2) \setminus \mathfrak{N}_1$. It turns out [14] that

$$H(\mathfrak{m}_1)/H(\mathfrak{m}_1)^3 \cong \mathcal{C}_3^4,$$

the set $\mathcal{P}_2$ generates a subgroup of $H(\mathfrak{m}_1)/H(\mathfrak{m}_1)^3$ isomorphic to $\mathcal{C}_3^3$, and $\psi(\mathfrak{q}) = 1$ for $\mathfrak{q} \in \mathcal{P}_2$. Suppose that $\psi \neq \psi'$, then there is a prime $\mathfrak{q}_0$ in $\{\mathfrak{q}_{29}, \bar{\mathfrak{q}}_{29}\}$ such that

$\psi'(\mathfrak{q}_0) \neq 1$ and, therefore, $\mathfrak{q}_0$ does not split in L'. Thus, from the supposition $\psi \neq \psi'$ it follows that

$$\operatorname{ord}(\bar\rho_f(\varphi(\mathfrak{p}_{29})) = \operatorname{ord}(\bar\rho_f(\varphi(\mathfrak{p}_{29})|L'))) = \operatorname{ord}(\varphi(\mathfrak{p}_{29})|L') = 3. \tag{12}$$

By Lemma 6, relation (12) implies that $\operatorname{Tr}\bar\rho_f(\varphi(\mathfrak{p}_{29})) = 1$ and, consequently,

$$\operatorname{Tr}\rho_f(\varphi(\mathfrak{p}_{29})) = c(\mathfrak{p}_{29}) = 1 \pmod 2.$$

On the other hand, $c(\mathfrak{p}_{29}) = -6$ by Lemma 2. This contradiction shows that $\psi = \psi'$, whence $L = L'$, as claimed. □

Proof of Proposition 3. By Lemma 10, we have

$$\operatorname{Ker}\bar\rho_E = \operatorname{Ker}\bar\rho_f = G_L.$$

Since

$$\bar\rho_f(G_K) = \bar\rho_E(G_K) = \mathrm{GL}_2(\mathbb{F}_2)$$

by Lemma 4 and Corollary 6, from Lemma 3 it follows that the representations $\bar\rho_E$ and $\bar\rho_f$ are equivalent. This completes the proof of the proposition. □

§4. The Faltings–Serre method

1. In this section we describe the Faltings–Serre method along the lines of [7] (see also [20, 17]). We start with a few simple group theoretic observations. Write $\mathfrak{S}_4 = \langle\omega_1, \omega_2\rangle$ and $\mathfrak{S}_3 = \langle\zeta, \eta\rangle$, with $\omega_1 := (1324)$, $\omega_2 := (1234), \zeta := (12), \eta := (13)$, and define two surjective homomorphisms

$$\tau_1 : \mathfrak{S}_4 \times \mathcal{C}_2 \to \mathfrak{S}_3 \times \mathcal{C}_2, \quad \tau_1 : (\omega_1, 1) \mapsto (\zeta, 1), \quad (\omega_2, 1) \mapsto (\eta, 1), \quad (1, \zeta) \mapsto (1, \zeta),$$

and

$$\tau_2 : \mathfrak{S}_4 \times \mathcal{C}_2 \to \mathfrak{S}_4, \quad \tau_2 : (\alpha, \beta) \mapsto (\alpha, 1) \quad \text{for} \quad \alpha \in \mathfrak{S}_4, \quad \beta \in \mathcal{C}_2.$$

Lemma 11. *The maps τ_1 and τ_2 satisfy the following conditions.*

1. $\operatorname{Ker}\tau_1 \cong \mathcal{C}_2^2$ *and* $\operatorname{Ker}\tau_2 \cong \mathcal{C}_2$.
2. *Let $g \in \mathfrak{S}_4 \times \mathcal{C}_2$, then* $\operatorname{ord}(g) = 6$ *if and only if* $\operatorname{ord}(\tau_1(g)) = 6$, *and* $\operatorname{ord}(g) = 4$ *if and only if* $\operatorname{ord}(\tau_2(g)) = 4$.

Proof. This is straightforward. □

Notation 5. Let $M_2(\mathcal{A})$ be the algebra of (2×2)-matrices with entries in a ring $\mathcal{A}$, and let $M_2^{(0)}(\mathcal{A}) := \{a \mid a \in M_2(\mathcal{A}),\ \operatorname{Tr} a = 0\}$.

Consider the group

$$\mathfrak{G} := \{(m, n) \mid m \in M_2(\mathbb{F}_2),\ n \in \mathrm{GL}_2(\mathbb{F}_2)\},$$

multiplication being defined by

$$(m_1, n_1) \cdot (m_2, n_2) := (m_1 + n_1 m_2 n_1^{-1}, n_1 n_2)$$

for $\{(m_1, n_1), (m_2, n_2)\} \subseteq \mathfrak{G}\}$, and its subgroup

$$\mathfrak{G}^{(0)} := \{(m, n) \mid m \in M_2^{(0)}(\mathbb{F}_2),\ n \in \mathrm{GL}_2(\mathbb{F}_2)\}.$$

We define a map

$$g : \mathfrak{G} \to \mathbb{F}_2, \quad g : (m, n) \mapsto \operatorname{Tr}(m \cdot n) \quad \text{for} \quad (m, n) \in \mathfrak{G};$$

let $g_0 := g \mid \mathfrak{G}^{(0)}$.

Lemma 12. *The group $\mathfrak{G}^{(0)}$ is isomorphic to the direct product $\mathfrak{S}_4 \times \mathcal{C}_2$.*

Proof. Let

$$v_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ v_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ v_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \ v_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The $\mathbb{F}_2$-vector space $M_2^{(0)}(\mathbb{F}_2)$ has a basis $\{v_0, v_1, v_2\}$ and $v_3 = v_1 + v_2$. On identifying $\mathrm{GL}_2(\mathbb{F}_2)$ with $\mathfrak{S}_3$ via the isomorphism

$$\iota : \mathfrak{S}_3 \to \mathrm{GL}_2(\mathbb{F}_2), \quad \iota : (12) \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \iota : (13) \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

we have $\mathfrak{G}^{(0)} = H_1 \times H_2$, where

$$H_1 := \{(0, \nu), (v_i, \nu) \mid 1 \le i \le 3, \ \nu \in \mathfrak{S}_3\}, \quad H_2 := \{(0, (1)), (v_0, (1))\},$$

the multiplication law being defined as follows:

$$(v_k, \sigma) \cdot (v_i, \tau) = (v_k + v_{\sigma(i)}, \sigma\tau), \quad \{\sigma, \tau\} \subseteq \mathfrak{S}_3, \ \ 0 \le i, \ \ k \le 3, \tag{13}$$

with $\sigma(0) = 0$ for $\sigma \in \mathfrak{S}_3$. It is clear that $H_2 \cong \mathcal{C}_2$. Let

$$\mathfrak{B}_2 := \{(1), (12)(34), (13)(24), (14)(23)\}$$

and consider the injective homomorphism

$$\vartheta^{(0)} : \mathfrak{B}_2 \to M_2^{(0)}(\mathbb{F}_2), \quad \vartheta^{(0)} : (13)(24) \mapsto v_2, \quad (14)(23) \mapsto v_1.$$

Since

$$\mathfrak{S}_4 = \bigcup_{\sigma \in \mathfrak{S}_3} \mathfrak{B}_2 \sigma,$$

the map

$$\vartheta : \mathfrak{S}_4 \to H_1, \quad \vartheta : \alpha\sigma \mapsto (\vartheta^{(0)}(\alpha), \sigma), \quad \alpha \in \mathfrak{B}_2, \ \ \sigma \in \mathfrak{S}_3,$$

defines an isomorphism $\mathfrak{S}_4 \cong H_1$. Thus, $\mathfrak{G}^{(0)} \cong \mathfrak{S}_4 \times \mathcal{C}_2$, as claimed. □

Lemma 13. *We have* $g_0^{-1}(\{1\}) = \{\sigma \mid \sigma \in \mathfrak{G}^{(0)}, \ \mathrm{ord}(\sigma) \in \{4, 6\}\}$.

Proof. This follows easily from the multiplication law (13) and the definition of the map g_0. □

Notation 6. Let $j : \mathfrak{G}^{(0)} \to \mathfrak{S}_4 \times \mathcal{C}_2$ stand for the isomorphism defined in Lemma 12.

2. In what follows until the end of this section, we let K be an arbitrary imaginary quadratic field. Let

$$\rho_1, \rho_2 : G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$$

be two continuous 2-adic representations unramified outside of a finite set S of primes of K, and let $\bar{\rho}_i : G_K \to \mathrm{GL}_2(\mathbb{F}_2)$ denote the reduction of ρ_i,$i = 1, 2$, modulo 2. Suppose that $\bar{\rho}_1 = \bar{\rho}_2$, $\bar{\rho}_1(G_K) = \mathrm{GL}_2(\mathbb{F}_2)$, and $\det \rho_1 = \det \rho_2$. Let $\mathrm{Ker}\, \bar{\rho}_1 = G_L$, so that $L|K$ is a finite normal extension with $G(L|K) \cong \mathfrak{S}_3$.

Notation 7. Let $\chi_i := \mathrm{Tr}\, \rho_i$, $i = 1, 2$, and let $\mathfrak{M}$ stand for the set of the number fields M such that $L \subseteq M$ and $M|K$ is a finite normal extension unramified outside S.

Lemma 14. *Suppose that* $\chi_1 \ne \chi_2$. *Then there is a number field* M *in* $\mathfrak{M}$ *with the following properties*: *its Galois group* $G(M|K)$ *is isomorphic to a subgroup of the group* $\mathfrak{S}_4 \times \mathcal{C}_2$; $f_M(\mathfrak{p}) \in \{4, 6\}$ *for at least one prime* $\mathfrak{p}$ *in* $\mathcal{P}(K) \setminus S$; *and* $\chi_1(\varphi(\mathfrak{p})) \ne \chi_2(\varphi(\mathfrak{p}))$ *for any prime* $\mathfrak{p}$ *in* $\mathcal{P}(K) \setminus S$ *with* $f_M(\mathfrak{p}) \in \{4, 6\}$.

Proof. Suppose that $\chi_1 \neq \chi_2$ and let

$$r := \max\{s \mid s \in \mathbb{N},\ \chi_1 = \chi_2 \pmod{2^s}\}. \tag{14}$$

Relation (14) implies [21, Théorème 1] (cf. [7, Remark 6]) that

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

for a certain function $\mu : G_K \to M_2(\mathbb{Z}_2)$; let $\bar{\mu} : G_K \to M_2(\mathbb{F}_2)$ stand for the reduction of μ modulo 2. Then the map

$$h : G_K \to ; \mathfrak{G}, \quad h : \sigma \mapsto (\bar{\mu}(\sigma), \bar{\rho}_1(\sigma)) \quad \text{for} \quad \sigma \in G_K,$$

is a homomorphism. Moreover, since

$$\det \rho_1 = \det \rho_2 \quad \text{and} \quad \det(1 + 2^r\mu) = 1 + 2^r \operatorname{Tr} \mu \pmod{2^{r+1}},$$

it follows that $\operatorname{Tr} \bar{\mu} = 0$. Thus, $h(G_K) \subseteq \mathfrak{G}^{(0)}$. Let

$$M := \{x \mid x \in \bar{K}, \sigma x = x \ \text{ for } \ \sigma \in \operatorname{Ker} h\},$$

so that $\operatorname{Ker} h = G_M$, $G(M|K) \cong h(G_K)$, and

$$f_M(\mathfrak{p}) = \operatorname{ord}(h(\varphi(\mathfrak{p}))) \quad \text{for} \quad \mathfrak{p} \in \mathcal{P}(K) \setminus S.$$

Furthermore, $M \in \mathfrak{M}$ and, by Lemma 12, the Galois group $G(M|K)$ is isomorphic to a subgroup of the group $\mathfrak{S}_4 \times \mathcal{C}_2$. Let

$$h_0 := g \circ h, \quad h_0 : G_K \to \mathbb{F}_2, \quad h_0 : \sigma \mapsto \operatorname{Tr}(\bar{\mu}(\sigma)\bar{\rho}_1(\sigma)) \quad \text{for} \quad \sigma \in G_K.$$

By Lemma 13, $h_0(\sigma) = 1$ if and only if $\operatorname{ord}(h(\sigma)) \in \{4, 6\}$ for $\sigma \in G_K$. If $f_M(\mathfrak{p}) \notin \{4, 6\}$ for every prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus S$, then $\operatorname{ord}(h(\varphi(\mathfrak{p}))) \notin \{4, 6\}$ and, therefore,

$$0 = h_0(\varphi(\mathfrak{p})) = \operatorname{Tr}(\bar{\mu}(\varphi(\mathfrak{p}))\bar{\rho}_1(\varphi(\mathfrak{p}))) = (\chi_1(\varphi(\mathfrak{p})) - \chi_2(\varphi(\mathfrak{p})))2^{-r} \pmod{2},$$

that is

$$|\chi_1(\varphi(\mathfrak{p})) - \chi_2(\varphi(\mathfrak{p}))|_2 \leq \frac{1}{2^{r+1}} \tag{15}$$

for every prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus S$. In view of the Chebotarev density theorem, inequality (15) implies that

$$\chi_1 = \chi_2 \pmod{2^{r+1}},$$

contrary to the choice of r. Therefore, we conclude that $f_M(\mathfrak{p}) \in \{4, 6\}$ for at least one prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus S$. Finally, if $f_M(\mathfrak{p}) \in \{4, 6\}$, $\mathfrak{p} \in \mathcal{P}(K) \setminus S$, then

$$1 = h_0(\varphi(\mathfrak{p})) = \operatorname{Tr}(\bar{\mu}(\varphi(\mathfrak{p}))\bar{\rho}_1(\varphi(\mathfrak{p}))) = (\chi_1(\varphi(\mathfrak{p})) - \chi_2(\varphi(\mathfrak{p})))2^{-r} \pmod{2},$$

whence $\chi_1(\varphi(\mathfrak{p})) \neq \chi_2(\varphi(\mathfrak{p}))$. This completes the proof of the lemma. □

Lemma 15. *Suppose that for every extension $M|K$ with $M \in \mathfrak{M}$ and $G(M|K) \cong \mathfrak{S}_3 \times \mathcal{C}_2$ there exists a prime $\mathfrak{p}_1$ in $\mathcal{P}(K) \setminus S$ with $f_M(\mathfrak{p}_1) = 6$ and*

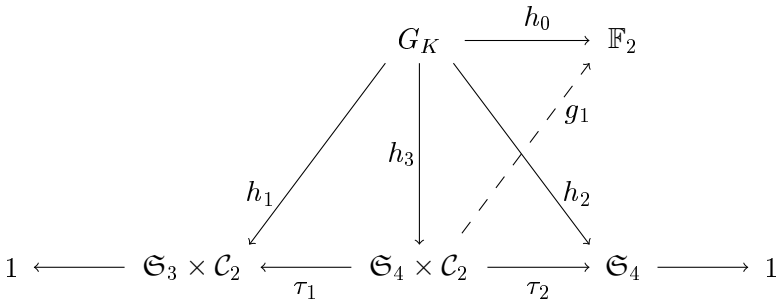
$$\chi_1(\varphi(\mathfrak{p}_1)) = \chi_2(\varphi(\mathfrak{p}_1)),$$

and that for every extension $M|K$ with $M \in \mathfrak{M}$ and $G(M|K) \cong \mathfrak{S}_4$ there exists a prime $\mathfrak{p}_2$ in $\mathcal{P}(K) \setminus S$ with $f_M(\mathfrak{p}_2) = 4$ and

$$\chi_1(\varphi(\mathfrak{p}_2)) = \chi_2(\varphi(\mathfrak{p}_2)).$$

Then $\rho_1 \cong \rho_2$.

Proof. Suppose that the representation ρ_1 is not equivalent to the representation ρ_2. Since those representations are irreducible, it follows [2, §12, no. 1, Proposition 3] that $\chi_1 \neq \chi_2$. Therefore, by Lemma 14, there are a number field M in $\mathfrak{M}$, a homomorphism $h_3 : G_K \to \mathfrak{S}_4 \times \mathcal{C}_2$ with $h_3(G_K) \cong G(M|K)$, and a prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus S$ with $f_M(\mathfrak{p}) \in \{4, 6\}$. Combining the maps defined above, we obtain the following commutative diagram:



with $h_3 := j \circ h$, $h_1 := \tau_1 \circ h_3$, $h_2 := \tau_2 \circ h_3$, $g_1 := g_0 \circ j^{-1}$, and $G_M = \operatorname{Ker} h_3$. Let

$$M_i := \{x \mid x \in \bar{K},\ \sigma x = x \quad \text{for} \quad \sigma \in \operatorname{Ker} h_i\},$$

so that

$$\operatorname{Ker} h_i = G_{M_i}, \quad G(M_i|K) \cong h_i(G_K), \quad \text{and} \quad M_i \subseteq M \quad \text{for} \quad i = 1, 2.$$

Since $M \in \mathfrak{M}$ and $G(L|K) \cong \mathfrak{S}_3$, there is a surjective homomorphism $j_0 : h_3(G_K) \to \mathfrak{S}_3$; let $h_0 := j_0 \circ h_3$, then $\operatorname{Ker} h_0 = G_L$. It can easily be checked that $\operatorname{Ker} h_i \subseteq \operatorname{Ker} h_0$ and therefore $L \subseteq M_i$ for $i = 1, 2$, so that $\{M_1, M_2\} \subseteq \mathfrak{M}$. Let $\sigma \in \varphi(\mathfrak{p})$, then $\operatorname{ord}(h_3(\sigma)) \in \{4, 6\}$ and, by Lemma 11, either $\operatorname{ord}(h_1(\sigma)) = 6$ or $\operatorname{ord}(h_2(\sigma)) = 4$. It follows that either $h_1(G_K) = \mathfrak{S}_3 \times \mathcal{C}_2$ or $h_2(G_K) = \mathfrak{S}_4$. Then the assumption of the lemma implies that there is a prime $\mathfrak{p}_0$ in $\mathcal{P}(K) \setminus S$ such that

$$\chi_1(\varphi(\mathfrak{p}_0)) = \chi_2(\varphi(\mathfrak{p}_0)) \tag{16}$$

and either $f_{M_1}(\mathfrak{p}_0) = 6$ or $f_{M_2}(\mathfrak{p}_0) = 4$. But, in view of Lemma 14, the latter condition implies that

$$\chi_1(\varphi(\mathfrak{p}_0)) \neq \chi_2(\varphi(\mathfrak{p}_0)),$$

in contradiction to (16). This proves the lemma. □

§5. Proof of Theorem 2

We return to the notation of §2 and §3; Lemma 8 allows us to assume that $\rho_f(G_K) \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$. Let

$$\mathfrak{m}_2 := \mathfrak{t}_{23}\bar{\mathfrak{t}}_{23}\mathfrak{t}_{2,1}^7\Big(\prod_{i=2}^{4}\mathfrak{t}_{2,i}\Big)^5\prod_{i=1}^{4}\mathfrak{t}_{3,i}, \quad \{\mathfrak{t}_{2,i}, \mathfrak{t}_{3,i}, \mathfrak{t}_{23}, \bar{\mathfrak{t}}_{23} \mid 1 \le i \le 4\} \subseteq \mathcal{P}(L),$$

with

$$(2) = \mathfrak{t}_{2,1}^3\Big(\prod_{i=2}^{4}\mathfrak{t}_{2,i}\Big)^2, \quad (3) = \mathfrak{t}_{3,1}^6\prod_{i=2}^{4}\mathfrak{t}_{3,i}, \quad (23) = (\mathfrak{t}_{23}\bar{\mathfrak{t}}_{23})^2 \ \text{ in } \ I_0(L).$$

Let

$$X := \{\chi \mid \chi \in \widehat{H}(\mathfrak{m}_2),\ \chi^2 = 1\}$$

be the group of the real characters of $H(\mathfrak{m}_2)$; it turns out [14] that $X \cong \mathcal{C}_2^{16}$. Since the ideal $\mathfrak{m}_2$ is $G(L|K)$-invariant, the group $G(L|K)$ acts on the characters of $H(\mathfrak{m}_2)$:

$$(\sigma\chi)(g) := \chi(\sigma g) \ \text{ for } \ \chi \in \widehat{H}(\mathfrak{m}_2),\ \ \sigma \in G(L|K),\ \ g \in H(\mathfrak{m}_2).$$

Lemma 16. *For every normal field extension $M|K$ unramified outside $\mathfrak{N}$ and such that $G(M|K) \cong \mathfrak{S}_3 \times \mathcal{C}_2$ and $L \subseteq M$, there exists a prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus \mathfrak{N}$ with $f_M(\mathfrak{p}) = 6$ and $\operatorname{Tr}(\rho_E(\varphi(\mathfrak{p}))) = \operatorname{Tr}(\rho_f(\varphi(\mathfrak{p})))$.*

Proof. Let

$$\mathcal{P}_1 := \{\mathfrak{p}_5, \bar{\mathfrak{p}}_{13}, \bar{\mathfrak{p}}_{29}, \mathfrak{p}_{31}, \bar{\mathfrak{p}}_{41}\}$$

be the set of primes in $\mathcal{P}(K) \setminus \mathfrak{N}$ introduced in the proof of Lemma 9, and let

$$\mathcal{P}_3 := \left\{\mathfrak{t} \mid \mathfrak{t} \in \mathcal{P}(L),\ \mathfrak{t} \mid \prod_{\mathfrak{q}\in\mathcal{P}_1} \mathfrak{q}\right\}.$$

It can be checked that $f_L(\mathfrak{p}) = 3$ for $\mathfrak{p} \in \mathcal{P}_1$. Since $[M : L] = 2$ and the extension $M|K$ is unramified outside $\mathfrak{N}$, from Lemma 6 it follows that $M \subseteq L(\mathfrak{m}_2)$. Let ψ be the real character in $\widehat{H}(\mathfrak{m}_2)$ corresponding to the extension $M|L$. The condition $G(M|K) \cong \mathfrak{S}_3 \times \mathcal{C}_2$ shows that the character ψ is $G(L|K)$-invariant [7, Proposition 5.7]. On the other hand, the subgroup

$$X_1 := \{\chi \mid \chi \in X,\ \sigma\chi = \chi \quad \text{for} \quad \sigma \in G(L|K)\}$$

of the $G(L|K)$-invariant real characters is isomorphic to $\mathcal{C}_2^5$, and if $\chi \in X_1 \setminus \{1\}$, then $\chi(\mathfrak{t}) = -1$ for some $\mathfrak{t}$ in $\mathcal{P}_3$ [14]. In particular, $\psi(\mathfrak{t}_0) = -1$ for some $\mathfrak{t}_0$ in $\mathcal{P}_3$, whence $f(\mathfrak{P}, \mathfrak{t}_0) = 2$ for $\mathfrak{P} \in \mathcal{P}(M)$ with $\mathfrak{P}|\mathfrak{t}_0$. Let $\mathfrak{t}_0|\mathfrak{p}_0$, $\mathfrak{p}_0 \in \mathcal{P}_1$, then

$$f(\mathfrak{P}, \mathfrak{p}_0) = f(\mathfrak{P}, \mathfrak{t}_0) f(\mathfrak{t}_0, \mathfrak{p}_0) = 6.$$

Moreover, since $N\mathfrak{p} < 50$ for $\mathfrak{p} \in \mathcal{P}_1$, it follows [12] that

$$\mathrm{Tr}(\rho_E(\varphi(\mathfrak{p}_0))) = a(\mathfrak{p}_0) = c(\mathfrak{p}_0) = \mathrm{Tr}(\rho_f(\varphi(\mathfrak{p}_0))).$$

This proves the lemma. □

Lemma 17. *For every normal field extension $M|K$ unramified outside $\mathfrak{N}$ and such that $G(M|K) \cong \mathfrak{S}_4$ and $L \subseteq M$, there exists a prime $\mathfrak{p}$ in $\mathcal{P}(K) \setminus \mathfrak{N}$ with $f_M(\mathfrak{p}) = 4$ and $\mathrm{Tr}(\rho_E(\varphi(\mathfrak{p}))) = \mathrm{Tr}(\rho_f(\varphi(\mathfrak{p})))$.*

Proof. Let

$$\mathcal{P}_4 := \{\mathfrak{p}_7, \mathfrak{p}_{13}, \bar{\mathfrak{p}}_{31}, \mathfrak{p}_{41}\},\ \mathcal{P}_4 \subseteq \mathcal{P}(K) \setminus \mathfrak{N},$$

and let

$$\mathcal{P}_5 := \left\{\mathfrak{t} \mid \mathfrak{t} \in \mathcal{P}(L),\ \mathfrak{t} \mid \prod_{\mathfrak{q}\in\mathcal{P}_1} \mathfrak{q}\right\}.$$

It can be checked that $f_M(\mathfrak{p}) = 2$ for $\mathfrak{p} \in \mathcal{P}_4$. Since $[M : L] = 4$, $G(M|K) \cong \mathfrak{S}_4$, and $G(L|K) \cong \mathfrak{S}_3$, it follows that $G(M|L) \cong \mathcal{C}_2^2$ and, therefore, there are exactly three number fields L_i with

$$L \subseteq L_i \subseteq M,\ [L_i : L] = 2,\ 1 \le i \le 3.$$

Moreover, since $M|K$ is unramified outside $\mathfrak{N}$, Lemma 6 applied to each of the fields L_i shows that $M \subseteq L(\mathfrak{m}_2)$. Let ψ_i be the real character in $\widehat{H}(\mathfrak{m}_2)$ corresponding to the extension $L_i|L$, $1 \le i \le 3$. It follows [7, Lemma 5.6 and Proposition 5.7] that there are two elements τ, σ in $G(L|K)$ with $\mathrm{ord}(\tau) = 2$, $\mathrm{ord}(\sigma) = 3$ and such that

$$\{\psi_i \mid 1 \le i \le 3\} = \{\sigma^j\psi_1 \mid 0 \le j \le 2\} \quad \text{and} \quad \tau\psi_1 = \psi_1.$$

We conclude that the extensions $M|K$ satisfying the assumptions of the lemma are in one-to-one correspondence with the set of characters $X_2 \setminus \{1\}$, where

$$X_2 := \{\chi \mid \chi \in X,\ \tau\chi = \chi,\ \chi(\sigma\chi)(\sigma^2\chi) = 1\},$$

with

$$\{\tau, \sigma\} \subseteq G(L|K), \quad \mathrm{ord}(\tau) = 2, \quad \mathrm{ord}(\sigma) = 3.$$

It turns out [14] that $X_2 \cong \mathcal{C}_2^4$, and if $\chi \in X_2 \setminus \{1\}$, then $\chi(\mathfrak{t}) = -1$ and, therefore, $f(\mathfrak{P}, \mathfrak{t}) = 2$ for $\mathfrak{P} \in \mathcal{P}(L_\chi)$ with $\mathfrak{P}|\mathfrak{t}$ for some $\mathfrak{t}$ in $\mathcal{P}_5$, where $L_\chi|L$ is the quadratic extension corresponding to the character χ, so that $L_\chi \subseteq L(\mathfrak{m}_2)$ and

$$f(\mathfrak{P}, \mathfrak{p}_0) = f(\mathfrak{P}, \mathfrak{t}) f(\mathfrak{t}, \mathfrak{p}_0) = 4$$

for $\mathfrak{p}_0 \in \mathcal{P}_4$ with $\mathfrak{t}|\mathfrak{p}_0$. Let $K \subseteq L_\chi \subseteq M$ and suppose that $G(M|K) \cong \mathfrak{S}_4$, then $f(\mathfrak{Q}, \mathfrak{p}_0) = 4$ for $\mathfrak{Q} \in \mathcal{P}(M)$ with $\mathfrak{Q}|\mathfrak{p}_0$. Moreover, since $N\mathfrak{p} < 50$ for $\mathfrak{p} \in \mathcal{P}_4$, it follows as above [12] that

$$\mathrm{Tr}(\rho_E(\varphi(\mathfrak{p}_0))) = a(\mathfrak{p}_0) = c(\mathfrak{p}_0) = \mathrm{Tr}(\rho_f(\varphi(\mathfrak{p}_0))).$$

This proves the lemma. □

Proof of Theorem 2. In view of Proposition 3, Corollary 6, Lemma 16, and Lemma 17, the representations ρ_E and ρ_f satisfy the assumptions of Lemma 15 with $S = \mathfrak{N}$. Therefore, $\rho_E \cong \rho_f$, as claimed. □

Acknowledgement. We are grateful to Professor G. Harder for his remarks and comments relating to this work. The third author is much obliged to Professor W.-Ch. W. Li for an important consultation.

References

[1] T. Berger and G. Harcos, *l-adic representations associated to modular forms over imaginary quadratic fields*, Int. Math. Res. Not. IMRN **2007**, no. 23, 16 pp. MR2380006 (2008m:11109)

[2] N. Bourbaki, *Éléments de mathématique*. 23. Première partie: *Les structures fondamentales de l'analyse*. Livre II: *Algèbre*. Chapitre 8: *Modules et anneaux semi-simples*, Actualités Sci. Ind., no. 1261, Hermann, Paris, 1958. MR0098114 (20:4576)

[3] C. Breuil, C. Brian, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$: *wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939. MR1839918 (2002d:11058)

[4] H. Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math., vol. 193, Springer-Verlag, New York, 2000. MR1728313 (2000k:11144)

[5] J. E. Cremona, *Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields*, Compositio Math. **51** (1984), 275–324. MR743014 (85j:11063)

[6] P. Deligne, *La conjecture de Weil*. I, Inst. Hautes Études Sci. Publ. Math. No. 43 (1974), 273–307. MR0340258 (49:5013)

[7] L. Dieulefait, L. Guerberoff, and A. Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), 1145–1170. MR2600560 (2011g:11122)

[8] J. Elstrodt, F. Grunewald, and J. Mennicke, *On the group* $\mathrm{PSL}_2(\mathbb{Z}[i])$, Number Theory Days, 1980 (Exeter, 1980), London Math. Soc. Lecture Note Ser., vol. 56, Cambridge Univ. Press, Cambridge–New York, 1982, pp. 255–283. MR697270 (84j:10024)

[9] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366. MR718935 (85g:11026a)

[10] H. Jacquet, and J. A. Shalika, *On Euler products and the classification of automorphic representations*. I, Amer. J. Math. **103** (1981), 499–558. MR618323 (82m:10050a)

[11] F. Jarvis and J. Manoharmayum, *On the modularity of supersingular elliptic curves over certain totally real number fields*, J. Number Theory **128** (2008), 589–618. MR2389858 (2009a:11125)

[12] M. Lingham, *Modular forms and elliptic curves over imaginary quadratic fields*, Ph. D. Thesis, Univ. Nottingham, 2005.

[13] M. Mink, *Beweis der Hasse–Weilschen Vermutung für eine elliptische Kurve über einem imaginärquadratischen Körper*, Diplomarbeit, Rheinische Friedrich-Wilhems-Univ., Bonn, 2010.

[14] The PARI Group (Bordeaux), PARI/GP, version 2.4.3 (see `pari.math.u-bordeaux.fr`).

[15] I. I. Piatetski-Shapiro, *Multiplicity one theorems*, Proc. Sympos. Pure Math., vol. 33, pt. 1, Amer. Math. Soc., Providence, RI, 1979, pp. 209–212. MR546599 (81m:22027)

[16] A. Scheutzow, *Computing rational cohomology and Hecke eigenvalues for Bianchi groups*, J. Number Theory **40** (1992), 317–328. MR1154042 (93b:11068)

[17] M. Schütt, *On the modularity of three Calabi–Yau threefolds with bad reduction at* 11, Canad. Math. Bull. **49** (2006), 296–312. MR2226253 (2007d:11041)

[18] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York–Amsterdam, 1968. MR0263823 (41:8422)

[19] ———, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou. Théoire des nombres **11** (1969/70), no. 2, exp. no. 19, 1–15.
[20] ———, *Résume des cours de* 1984–1985, Annuaire du Collége de France **1985**, 85–90.
[21] ———, *Représentations linéaires sur des anneaux locaux, d'apres Carayol*, Prépubl. no. 49 (1995), Inst. Math. Jussieu, Univ. Paris VI et Paris VII/CNRS, 1995.
[22] R. Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields*. II, Invent. Math. **116** (1994), 619–643. MR1253207 (95h:11050a)
[23] A. Weil, *Dirichlet series and automorphic forms*, Lecture Notes in Math., vol. 189, Springer-Verlag, Berlin etc., 1971.
[24] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551. MR1333035 (96d:11071)

Departament D'Álgebra Geometria, Facultat de Matemátiques, Universitat de Barcelona, Gran Via de les Corts Catalanes, 585, 08007 Barcelona, Spain
E-mail address: ldieulefait@ub.edu

Seminar für Mathematik und ihre Didaktik, Universität zu Köln, Gronewaldstr 2, D-50931 Köln, Germany
E-mail address: mmink@uni-koeln.de

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany
E-mail address: moroz@mpim-bonn.mpg.de

Received 10/JUN/2011
Originally published in English