Mathematische Zeitschrift

CrossMark

Some cases of Serre's uniformity problem

Pedro Lemos[1]

Abstract

We show that if $E/\mathbb{Q}$ is an elliptic curve without complex multiplication and for which there is a prime q such that the image of $\bar{\rho}_{E,q}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$, then $\bar{\rho}_{E,p}$ surjects onto $\mathrm{GL}_2(\mathbb{F}_p)$ for every prime $p > 37$. This result complements a previous result by the author. We also prove analogue results for certain families of $\mathbb{Q}$-curves, building on results of Ellenberg (Am J Math 126(4):763–787, 2004) and Le Fourn (Math Ann 365(1–2):173–214, 2016).

1 Introduction

Let K be a number field and E an elliptic curve defined over K. Given a prime number p, we will denote the mod p Galois representation obtained from the Galois action on the p-torsion points of $E(\bar{K})$ (where $\bar{K}$ is an algebraic closure of K) by $\bar{\rho}_{E,p}$. The image of this representation is contained in $\mathrm{GL}(E[p])$, which is (non-canonically) isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$. We will often implicitly make a choice of an $\mathbb{F}_p$-basis for $E[p]$ and regard $\bar{\rho}_{E,p}$ as having image contained in $\mathrm{GL}_2(\mathbb{F}_p)$. Throughout this paper, we will say that $\bar{\rho}_{E,p}$ is *surjective* if its image is the whole of $\mathrm{GL}_2(\mathbb{F}_p)$. The question of determining under what conditions these representations are surjective is very important in modern number theory. One of the earliest and most striking results in this area is due to Serre.

Theorem 1.1 ([16, Théorème 2]) *Let K be a number field and let E be an elliptic curve defined over K and without complex multiplication. There exists a constant $C_{E,K}$ such that $\bar{\rho}_{E,p}$ is surjective for every prime $p > C_{E,K}$.*

Serre's uniformity problem (see Sect. 4.3 of [16]) asks to what extent the constant $C_{E,K}$ of the theorem above is dependent on E. More precisely, it asks whether there exists a constant C_K depending only on K such that, given an elliptic curve E defined over K and without complex multiplication, the residual mod p Galois representation $\bar{\rho}_{E,p}$ is surjective for every prime $p > C_K$. An affirmative answer to this question would be likely to yield important applications in the study of certain Diophantine equations, as the work of Darmon and Merel [6] shows.

✉ Pedro Lemos
  lemos.pj@gmail.com

[1] Max Planck Institute for Mathematics, Vivatsgasse 7, 53111 Bonn, Germany

The most studied and most well understood case is, naturally, the one where $K = \mathbb{Q}$. The strongest result we have to this date is the following.

Theorem 1.2 ([2,3,11,12,16]) *Let E be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication. Let p be a prime number strictly larger than 37. If $\bar{\rho}_{E,p}$ is not surjective, then its image is contained in the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.*

In [10], the author showed that the normaliser of a non-split Cartan case cannot occur for primes $p > 37$ if an elliptic curve as in the theorem above admits a non-trivial cyclic isogeny defined over $\mathbb{Q}$.

Theorem 1.3 ([10, Theorem 1.1]) *Let E be an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication. Suppose that E admits a non-trivial cyclic isogeny defined over $\mathbb{Q}$. Then $\bar{\rho}_{E,p}$ is surjective for every prime $p > 37$.*

Another way of saying that an elliptic curve defined over a number field K admits a non-trivial cyclic isogeny defined over K is by saying that there exists a prime q for which the image of $\bar{\rho}_{E,q} : G_K \rightarrow \mathrm{GL}_2(\mathbb{F}_q)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. It is then natural to ask whether we can obtain results of the same kind if we replace "Borel subgroup" by another maximal subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. In the first part of this paper, we show that the same result holds if this maximal subgroup is chosen to be the normaliser of a split Cartan. More precisely, we show the following theorem.

Theorem 1.4 *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Suppose that there exists a prime q for which the image of $\bar{\rho}_{E,q}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. Then $\bar{\rho}_{E,p}$ is surjective for every $p > 37$.*

Note that it follows from the work of Bilu, Parent and Rebolledo [3] that there are only finitely many primes q for which there exists a non-CM elliptic curve defined over $\mathbb{Q}$ such that the image of $\bar{\rho}_{E,q}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. More precisely, they show that $q \in \{2, 3, 5, 7, 13\}$. Moreover, by the recent work of Balakrishnan, Dogra, Müller, Tuitman and Vonk [1], the prime 13 is not on this list, and the list is reduced to $\{2, 3, 5, 7\}$.

In order to prove this theorem, we follow the same strategy employed to prove Theorem 1.3, namely, we start by showing that if E is an elliptic curve satisfying the conditions of Theorem 1.4 and such that the image of $\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup for some prime $p \geq 11$, then its j-invariant is integral.

Proposition 1.5 *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Suppose that there exists a prime $p \geq 11$ for which the image of the residual Galois representation $\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Suppose, moreover, that there exists a prime q different from p such that the image of $\bar{\rho}_{E,q}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$. Then the j-invariant of E is integral.*

This result is proven an adaptation of Mazur's formal immersion argument (see [11,12]).

By Theorem 1.2, the only elliptic curves which could consitute a contradiction to Theorem 1.4 are those for which there exists a prime $p > 37$ such that the image of $\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan, and so they must all have integral j-invariants. Using explicit parametrisations of the j-invariant maps for $X_0(q)$, where q is an element of the set $\{2, 3, 5, 7\}$, we find out that there are only finitely many $\mathbb{Q}$-points of $X_0(q)$ with integral j-invariant. Moreover, we are able to compute all the possible j-invariants. As

any two elliptic curves with the same j-invariant are related to each other by a quadratic twist as long as their j-invariant is not 0 nor 1728, surjectivity only depends on the j-invariant, and so our problem is reduced to computing the largest non-surjective prime for a finite set of elliptic curves.

The second part of this paper is devoted to $\mathbb{Q}$-curves. Let us just recall a few definitions before proceeding. Let E be an elliptic curve defined over a Galois number field K. Given an element $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, we will denote by $^\sigma E$ the Galois conjugate of E by σ. Recall that E is said to be a $\mathbb{Q}$-curve if, for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, there exists an isogeny $\mu_\sigma : {}^\sigma E \to E$. If E/K is a $\mathbb{Q}$-curve, we shall say that it is *completely defined over K* if all of the isogenies μ_σ can be chosen in such a way that they are all defined over K. The main results of this paper make reference to some representations attached to $\mathbb{Q}$-curves that, following the notation introduced by Ellenberg [7,8], we will denote by $\mathbb{P}\bar{\rho}_{E,p}$. Despite the notation, these are *not*, in general, simply the projectivisations of $\bar{\rho}_{E,p}$ (the projectivisation of $\bar{\rho}_{E,p}$ is, by definition, the composition of $\bar{\rho}_{E,p}$ with the canonical projection $\mathrm{GL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p)$); in fact, $\mathbb{P}\bar{\rho}_{E,p}$ is defined on the whole of $G_\mathbb{Q}$, and not only on G_K, where K is the number field over which E is defined. However, there is a close relation between $\mathbb{P}\bar{\rho}_{E,p}$ and $\bar{\rho}_{E,p}$: if $P\bar{\rho}_{E,p}$ stands for the projectivisation of $\bar{\rho}_{E,p}$, then $P\bar{\rho}_{E,p}$ is isomorphic to $\mathbb{P}\bar{\rho}_{E,p}|_{G_K}$. For a brief review of the definition of $\mathbb{P}\bar{\rho}_{E,p}$, we refer the reader to Sect. 2. When K is a quadratic field, we say that a $\mathbb{Q}$-curve completely defined over K is of *degree d* if there exists an isogeny $\mu_\sigma : {}^\sigma E \to E$ defined over K and of degree d and there exists no other isogeny between $^\sigma E$ and E of smaller degree, where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the non-trivial element.

The main objective of the second part of the paper is to prove the following results (which are analogues of Theorems 1.3 and 1.4).

Theorem 1.6 *Let K be a quadratic field and let d be a square-free integer. There exists a constant $C_{K,d}$ satisfying the following property. If E is a $\mathbb{Q}$-curve completely defined over K, of degree d, without complex multiplication and for which there exists a prime $q \nmid d$ such that the image of $\mathbb{P}\bar{\rho}_{E,q}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$, then $\mathbb{P}\bar{\rho}_{E,p}$ surjects onto $\mathrm{PGL}_2(\mathbb{F}_p)$ for every $p > C_{K,d}$.*

Theorem 1.7 *Let K be a quadratic field and let $d \notin \{2, 3, 5, 7, 13\}$ be a square-free integer. There exists a constant $C_{K,d}$ satisfying the following property. If E is a $\mathbb{Q}$-curve completely defined over K, of degree d, without complex multiplication and for which there exists a prime $q \nmid d$ such that the image of $\mathbb{P}\bar{\rho}_{E,q}$ is contained in the normaliser of a split Cartan subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$, then $\mathbb{P}\bar{\rho}_{E,p}$ surjects onto $\mathrm{PGL}_2(\mathbb{F}_p)$ for every $p > C_{K,d}$.*

Most of the proof of these two theorems will use arguments of the same type of those used to prove Theorem 1.4 and described above. In particular, borrowing some ideas of Ellenberg [8], we will show the following.

Proposition 1.8 *Let K be a quadratic number field and let d be a square-free positive integer. Let E be a $\mathbb{Q}$-curve completely defined over K, of degree d and without complex multiplication. Suppose that p and q are distinct primes not dividing d such that the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ and that the image of $\mathbb{P}\bar{\rho}_{E,q}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. Suppose, moreover, that $p \geq 11$. Then the j-invariant of E is in $\mathcal{O}_K$, where $\mathcal{O}_K$ stands for the ring of integers of K.*

We remark that if $q \geq 11$ and $q \neq 13, 17, 41$, a much stronger result has been proven by Le Fourn [9, Proposition 3.3]. For the proof of Theorem 1.7, we will actually use the following result from [9].

Proposition 1.9 ([9, Proposition 3.6]) *Let K be a quadratic field and let $p = 11$ or $p > 13$ be a prime. Suppose that E is a $\mathbb{Q}$-curve of square-free degree d coprime to p such that the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in the normaliser of a split Cartan subgroup. Then $j(E) \in \mathcal{O}_K$.*

Finally, we would like to mention a theorem that will be used as an auxiliary result in the proof of Theorem 1.6, but which is interesting in its own right.

Theorem 1.10 *Let K be a quadratic number field and d a positive square-free integer. There exists a constant $C_{K,d}$ satisfying the following property. Let E/K be a $\mathbb{Q}$-curve completely defined over K, of degree d and without complex multiplication. If $p \nmid d$ is a prime for which the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$, then $p \leq C_{K,d}$. Moreover, if we restrict ourselves to the case where $p \equiv 1 \pmod 4$, then the constant $C_{K,d}$ can be chosen to be*

$$2^{6fc+1}(2^{6fc} + 1),$$

where c is the narrow class number of K and f is the residual degree of a prime of K lying above 2 (which is independent of the prime above 2 chosen). In particular, when $p \equiv 1 \pmod 4$, the constant $C_{K,d}$ is actually independent from d.

The reader is referred to the paper of Le Fourn [9], where results of a similar nature are proven. Specifically, in [9, Corollary 5.1], Le Fourn gives a bound for such primes that depends not only on the quadratic number field K, but also on the elliptic curve itself. However, by restricting himself to the cases where K is imaginary quadratic, he is able to give the absolute bound of $2 \cdot 10^{13}$ for the size of such primes (this is [9, Theorem 5.4]). In comparison, Theorem 1.10 shows the existence of a bound depending only on the quadratic number field K and on d, regardless of whether K is real or imaginary.

As a final remark, we would like, once again, to draw the reader's attention to the papers of Ellenberg [8] and Le Fourn [9]. In [8], Ellenberg shows that if K is an imaginary quadratic field and $d \geq 2$ is a square-free integer, then there exists a constant $C_{K,d}$ such that, given a $\mathbb{Q}$-curve E completely defined over K, of degree d and without complex multiplication, either $\mathbb{P}\bar{\rho}_{E,p}$ surjects onto $\mathrm{PGL}_2(\mathbb{F}_p)$ for every prime $p > C_{K,d}$, or E has potentially godd reduction at every prime of K of characteristic not dividing 6. The arguments appearing in the $\mathbb{Q}$-curve section of this paper will be based on some of his ideas. In [9], Le Fourn improves on the results of Ellenberg and gives an upper bound depending only on the discriminant of K (still assumed to be imaginary quadratic) and on the degree of the $\mathbb{Q}$-curve for the largest non-surjective prime associated to E. One peculiarity of their results is that they need the degree of the $\mathbb{Q}$-curve to be ≥ 2, i.e., they do not prove anything for elliptic curves defined over $\mathbb{Q}$. In this paper, we will start by proving Theorem 1.4, which is the analogue of Theorem 1.7 for elliptic curves defined over $\mathbb{Q}$, i.e., $\mathbb{Q}$-curves of degree 1.

2 Galois representations of $\mathbb{Q}$-curves

We follow the approach of Ellenberg [7]. For a more conceptual and complete treatment of the material in this section, the reader is referred to [15]. However, the description given here will suffice for the most part of the present article. Results from [15] will only be used in the proof of Theorem 1.10.

Let K be a Galois number field. Let E be a $\mathbb{Q}$-curve defined (but not necessarily completely defined) over K. Assume, moreover, that E does not have complex multiplication. For each $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, choose an isogeny $\mu_\sigma : {}^\sigma E \to E$. Note that if the restriction of σ to K is the trivial automorphism, then ${}^\sigma E = E$, and, in this case, we can choose μ_σ to be

the identity. We will always assume that we make this choice and that, moreover, if two elements $\sigma, \tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ restrict to the same automorphism of K, then $\mu_\sigma = \mu_\tau$. Since E does not have complex multiplication, we have $\mathrm{End}_{\bar{\mathbb{Q}}}(E) \otimes \mathbb{Q} = \mathbb{Q}$. Therefore, given $\sigma, \tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the element

$$c_E(\sigma, \tau) := \frac{1}{\deg \mu_{\sigma\tau}} \mu_\sigma \circ {}^\sigma \mu_\tau \circ \hat{\mu}_{\sigma\tau} \in \mathrm{End}_{\bar{\mathbb{Q}}}(E) \otimes \mathbb{Q},$$

where $\hat{\mu}_{\sigma\tau}$ stands for the dual isogeny of $\mu_{\sigma\tau}$, can be regarded as an element of $\mathbb{Q}^\times$.

Given, a prime number p, let $T_p(E)$ be the p-adic Tate module of E. Define the function (which, in general, is *not* a homomorphism) $\varpi_{E,p} : G_\mathbb{Q} \to \mathrm{GL}(T_p(E)) \cong \mathrm{GL}_2(\mathbb{Q}_p)$ in the following manner: given $P \in T_p(E)$ and $\sigma \in G_\mathbb{Q}$, we impose that $\varpi_{E,p}(\sigma)(P) = \mu_\sigma({}^\sigma P)$.

Remark Note that ${}^\sigma P \in {}^\sigma E(\bar{K})$. So, if σ does not restrict to the trivial automorphism of K, we may have ${}^\sigma P \notin E(\bar{K})$.

It is straightforward to check that the action of

$$\varpi_{E,p}(\sigma)\varpi_{E,p}(\tau)\varpi_{E,p}(\sigma\tau)^{-1}$$

on $T_p(E)$ is given by $c_E(\sigma, \tau) \in \mathbb{Q}^\times$. Thus, $\varpi_{E,p}$ gives rise to a well-defined homomorphism $\mathbb{P}\rho_{E,p} : G_\mathbb{Q} \to \mathrm{PGL}_2(\mathbb{Q}_p)$. If p does not divide the degree of any μ_σ, the construction of $\mathbb{P}\bar{\rho}_{E,p}$ is identical to this.

3 The case of elliptic curves over $\mathbb{Q}$

The aim of this section is to prove Proposition 1.5 and Theorem 1.4.

But before starting to prove the aforementioned results, let us introduce some notation and terminology that will be used throughout the paper. Table 2 contains a summary of facts and notation that we will need.

Recall that a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is called a *congruence subgroup* if there exists a positive integer N such that it contains

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \text{ and } b \equiv c \equiv 0 \pmod{N} \right\}.$$

In Table 1 we list some of the congruence subgroups that will appear more frequently during the course of this paper. In this table, N stands for a positive integer, p for an odd prime number, and r_p for the natural reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_p)$. Moreover, given an odd

Table 1 Some congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$

$\Gamma_0(N)$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N}$
$\Gamma_{\mathrm{sp}}(N)$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \pmod{N}$
$\Gamma_{\mathrm{sp}}^+(N)$	$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : b \equiv c \equiv 0 \text{ or } a \equiv d \equiv 0 \pmod{N}$
$\Gamma_{\mathrm{ns}}(p)$	$r_p^{-1}(C_{\mathrm{ns}}(p) \cap \mathrm{SL}_2(\mathbb{F}_p))$
$\Gamma_{\mathrm{ns}}^+(p)$	$r_p^{-1}(C_{\mathrm{ns}}^+(p) \cap \mathrm{SL}_2(\mathbb{F}_p))$

prime number p, we fix a non-split Cartan subgroup $C_{ns}(p)$ of $GL_2(\mathbb{F}_p)$ and write $C_{ns}^+(p)$ for its normaliser.

We will work with modular curves obtained as quotients of the extended upper half plane $\mathcal{H}^*$ by one of the congruence subgroups above or by some intersections of them. In fact, for any congruence subgroup Γ that we will work with, it can be shown that the Riemann surface $\Gamma \backslash \mathcal{H}^*$ descends to an algebraic curve defined over $\mathbb{Q}$. The point on this curve corresponding to $i\infty$ will be known as the *cusp at infinity* and will be denoted by ∞. In the following table we set up some terminology and summarise some of the facts concerning to these modular curves that will reveal to be useful later.

With the notation set up, we are now ready to prove the results we will need. We start by noting that if E is an elliptic curve defined over $\mathbb{Q}$ and without complex multiplication, then the values of q for which the image of $\bar{\rho}_{E,q}$ is contained in the normaliser of a split Cartan subgroup of $GL_2(\mathbb{F}_q)$ are very restricted. In fact, we have the following result.

Theorem 3.1 (Bilu–Parent–Rebolledo [3]) *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then, if q is a prime such that $q = 11$ or $q \geq 17$, the image of $\bar{\rho}_{E,q}$ cannot be contained in the normaliser of a split Cartan subgroup of $GL_2(\mathbb{F}_q)$.*

Recently, Balakrishnan, Dogra, Müller, Tuitman and Vonk [1] showed that the only $\mathbb{Q}$-rational points of $X_{sp}^+(13)$ are its cusps, thus proving the following theorem.

Theorem 3.2 ([1, Theorem 1.1]) *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then the image of $\bar{\rho}_{E,13}$ is not contained in the normaliser of a split Cartan subgroup of $GL_2(\mathbb{F}_{13})$.*

Therefore, we are reduced to considering the cases where $q \in \{2, 3, 5, 7\}$, i.e., the cases where the genus of $X_{sp}^+(q)$ is 0. However, further ahead, we will need some of the results in this section to hold in the case $q = 13$ as well. In fact, Theorem 3.2 will only be used in the proof of Theorem 1.4 in order to obtain the explicit bound of 37 (see Theorem 1.4 below); up until then, we will always assume that $q \in \{2, 3, 5, 7, 13\}$. We remark that these are precisely the primes q for which $X_0(q)$ has genus 0, a fact that plays an important role in the proof of Proposition 3.6.

The following is a more general version of [10, Proposition 2.2]. We will need this general form later.

Proposition 3.3 (cf. [10, Proposition 2.2]) *Let K be a number field of degree n and let E be an elliptic curve defined over K. Let p be a prime such that the image of $\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup of $GL_2(\mathbb{F}_p)$. If E has potentially multiplicative reduction at a prime λ not dividing p, then $N_{K/\mathbb{Q}}(\lambda)^2 \equiv 1 \pmod{p}$. Moreover, if $p > 2n+1$, then E has potentially good reduction at every prime of K dividing p.*

Proof Given a prime λ of K, write K_λ for the completion of K at λ. Let $\bar{K}$ and $\bar{K}_\lambda$ be algebraic closures of K and K_λ, respectively. Fix an embedding $\bar{K} \hookrightarrow \bar{K}_\lambda$. This induces an embedding of absolute Galois groups $G_{K_\lambda} \hookrightarrow G_K$, which amounts to a choice of a decomposition subgroup of G_K over λ.

Now, suppose that E has potentially multiplicative reduction at λ. Then we know that $E_{/K_\lambda}$ is a twist of a Tate curve E_q, $q \in K_\lambda^\times$.

Let ψ be the character associated to this twist. It is well-known that ψ is either trivial or quadratic. Therefore, we have

$$\bar{\rho}_{E,p}|_{G_{K_\lambda}} \sim \begin{pmatrix} \psi \chi_p & * \\ 0 & \psi \end{pmatrix},$$

where $\chi_p : G_{K_\lambda} \to \mathbb{F}_p^\times$ stands for the mod p cyclotomic character. As a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ is an index 2 subgroup of its normaliser, $\bar{\rho}_{E,p}(\sigma)^2$ is an element of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ for every $\sigma \in G_{K_\mathfrak{p}}$. Moreover, since ψ is at most quadratic, the eigenvalues of $\bar{\rho}_{E,p}(\sigma)^2$ are $\chi_p(\sigma)^2$ and 1. However, the eigenvalues of an element of a non-split Cartan subgroup are $\mathbb{F}_p$-conjugate. This means that $\chi_p(\sigma)^2 = 1$ for every $\sigma \in G_{K_\lambda}$.

If λ does not divide p, then this means that $N_{K/\mathbb{Q}}(\lambda)^2 \equiv 1 \pmod{p}$, as the statement of the proposition predicts.

Suppose now that $p > 2n + 1$ and that λ divides p. Then, as $\chi_p(\sigma)^2 = 1$ for every $\sigma \in G_{K_\lambda}$, we must have $[K_\lambda(\zeta_p) : K_\lambda] \leq 2$. On the other hand, $\mathbb{Q}_p(\zeta_p) \subseteq K_\lambda(\zeta_p)$ and $[\mathbb{Q}_p(\zeta_p) : \mathbb{Q}_p] = p - 1$. Hence, $[K_\lambda(\zeta_p) : \mathbb{Q}_p] \geq p - 1$, yielding $n \geq [K_\lambda : \mathbb{Q}_p] \geq (p-1)/2$, which contradicts the condition $p > 2n + 1$. $\qquad\square$

In order to simplify notation, we will write $X_{\mathrm{sp,ns}}^{-,+}(q, p)$ for the curve $X_{\mathrm{sp}}(q) \times_{X(1)} X_{\mathrm{ns}}^+(p)$, $X_{\mathrm{sp,ns}}^{+,+}(q, p)$ for the curve $X_{\mathrm{sp}}^+(q) \times_{X(1)} X_{\mathrm{ns}}^+(p)$, and $X_{0,\mathrm{ns}}^+(N, p)$ for the curve $X_0(N) \times_{X(1)} X_{\mathrm{ns}}^+(p)$, where N is a positive integer. These three curves correspond to certain quotients of the extended upper half plane: there is an analytic isomorphism between $X_{\mathrm{sp,ns}}^{-,+}(q, p)(\mathbb{C})$ and the quotient of $\mathcal{H}^*$ by $\Gamma_{\mathrm{sp}}(q) \cap \Gamma_{\mathrm{ns}}^+(p)$, another one between $X_{\mathrm{sp,ns}}^{+,+}(q, p)(\mathbb{C})$ and the quotient of $\mathcal{H}^*$ by $\Gamma_{\mathrm{sp}}^+(q) \cap \Gamma_{\mathrm{ns}}^+(p)$, and another between $X_{0,\mathrm{ns}}^+(N, p)(\mathbb{C})$ and the quotient of $\mathcal{H}^*$ by $\Gamma_0(N) \cap \Gamma_{\mathrm{ns}}^+(p)$.

In what follows, we will write w_{q^2} for the involution of $X_{0,\mathrm{ns}}^+(q^2, p)$ arising from the Atkin–Lehner involution of $X_0(q^2)$ (recall that the moduli intepretation of the Atkin–Lehner involution of $X_0(q^2)$ is as follows: a point of $X_0(q^2)$ represented by (E, φ)—where E is an elliptic curve and $\varphi : E \to E'$ is an isogeny of degree q^2—is mapped to $(E', \hat{\varphi})$, where $\hat{\varphi}$ stands for the dual isogeny of φ).

Lemma 3.4 *There is a $\mathbb{Q}$-isomorphism $\theta : X_{\mathrm{sp,ns}}^{-,+}(q, p) \to X_{0,\mathrm{ns}}^+(q^2, p)$. Moreover, the involution w_{q^2} of $X_{0,\mathrm{ns}}^+(q^2, p)$ coming from the Atkin–Lehner involution of $X_0(q^2)$ corresponds, under this isomorphism, to the involution ω_q of $X_{\mathrm{sp,ns}}^{-,+}(q, p)$ coming from the obvious involution of $X_{\mathrm{sp}}(q)$. In other words, we have $\theta \circ \omega_q = w_{q^2} \circ \theta$.*

Remark Even though there exists an isomorphism between $X_0(q^2)$ and $X_{\mathrm{sp}}(q)$, this is not enough to conclude Lemma 3.4, because this isomorphism does not preserve j-invariants.

Proof Even though the existence of an isomorphism between $X_{\mathrm{sp,ns}}^{-,+}(q, p)$ and $X_{0,\mathrm{ns}}^+(q^2, p)$ cannot be directly proven by appealing to the isomorphism between $X_0(q^2)$ and $X_{\mathrm{sp}}(q)$, the proofs of the existence of these two isomorphisms are essentially the same. Indeed, start by identifying $X_{0,\mathrm{ns}}^+(q^2, p)(\mathbb{C})$ with the Riemann surface $\Gamma_0(q^2) \cap \Gamma_{\mathrm{ns},1}^+(p) \backslash \mathcal{H}^*$, where $\Gamma_{\mathrm{ns},1}^+(p)$ is $r_p^{-1}(C_1 \cap \mathrm{SL}_2(\mathbb{F}_p))$ for some normaliser C_1 of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ (recall that $r_p : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{F}_p)$ stands for the reduction modulo p). Similarly, we identify $X_{\mathrm{sp,ns}}^{-,+}(q, p)(\mathbb{C})$ with the Riemann surface $\Gamma_{\mathrm{sp}}(q) \cap \Gamma_{\mathrm{ns}}^+(p) \backslash \mathcal{H}^*$. Set $\Gamma := \Gamma_0(q^2) \cap \Gamma_{\mathrm{ns},1}^+(p)$ and define

$$Q := \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}.$$

The map $\Gamma \backslash \mathcal{H}^* \to Q\Gamma Q^{-1} \backslash \mathcal{H}^*$ given by $z \mapsto qz$ is an isomorphism. Note that $Q\Gamma Q^{-1} = \Gamma_{\mathrm{sp}}(q) \cap \Gamma_{\mathrm{ns},2}^+(p)$, where $\Gamma_{\mathrm{ns},2}^+(p) = r_p^{-1}(C_2 \cap \mathrm{SL}_2(\mathbb{F}_p))$, where C_2 is a subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ conjugate to C_1. The Riemann surface $Q\Gamma Q^{-1} \backslash \mathcal{H}^*$ corresponds to the $\mathbb{C}$-points of an algebraic curve X_2. The isomorphism between $X_{0,\mathrm{ns}}^+(q, p)(\mathbb{C})$ and $X_2(\mathbb{C})$ just defined can be seen

to descend to an isomorphism defined over $\mathbb{Q}$. Therefore, we have a $\mathbb{Q}$-isomorphism between $X_{0,\mathrm{ns}}^+(q, p)$ and X_2. Now, we can define an isomorphism between X_2 and $X_{\mathrm{sp,ns}}^{-,+}(q, p)$ by a simple $\mathbb{F}_p$-base change. In a more formal way, we note that if $g \in \mathrm{GL}_2(\mathbb{F}_p)$ is such that $gC_2g^{-1} = C_1$, and if $X(p)$ denotes the modular curve parametrising elliptic curves with full p-torsion, then the automorphism of $X(p)$ defined by multiplication by g induces a $\mathbb{Q}$-isomorphism $C_2\backslash X(p) \to C_1\backslash X(p)$. Moreover, this isomorphism preserves j-invariants. Since we have

$$X_{\mathrm{sp,ns}}^{-,+}(q, p) = X_{\mathrm{sp}}(q) \times_{X(1)} C_1\backslash X(p) \quad \text{and} \quad X_2 = X_{\mathrm{sp}}(q) \times_{X(1)} C_2\backslash X(p),$$

there is a $\mathbb{Q}$-isomorphism from X_2 to $X_{\mathrm{sp,ns}}^{-,+}(q, p)$. The isomorphism θ is obtained by composing this isomorphism with the isomorphism from $X_{0,\mathrm{ns}}^+(q, p)$ to X_2 defined above.

The statement relating the involutions of $X_{\mathrm{sp,ns}}^{-,+}(q, p)$ and $X_{0,\mathrm{ns}}^+(q, p)$ with the isomorphism θ can be achieved by looking at the moduli interpretation of θ. $\square$

Remark The moduli intepretation of the isomorphism θ is given as follows. A $\mathbb{C}$-point in $X_{\mathrm{sp,ns}}^{+,+}(q, p)$ is represented by a tuple $(E, \varphi_1, \varphi_2, \mathfrak{n})$, where $\varphi_1 : E \to E_1$ and $\varphi_2 : E \to E_2$ are two independent isogenies of degree q and $\mathfrak{n}$ is a necklace (for the definition of a necklace, see [14]). The image of this point under θ is represented by the tuple $(E_1, \varphi_2 \circ \hat{\varphi}_1, \varphi_1(\mathfrak{n}))$, where $\hat{\varphi}_1$ stands for the dual isogeny of φ_1, and $\varphi_1(\mathfrak{n})$ is the necklace in E_1 obtained as the image of the necklace $\mathfrak{n}$ via φ_1.

The curve $X_{0,\mathrm{ns}}^+(q^2, p)$ comes equipped with two "degeneracy maps"

$$d_1, d_2 : X_{0,\mathrm{ns}}^+(q^2, p) \to X_{0,\mathrm{ns}}^+(q, p)$$

coming from the degeneracy maps from $X_0(q^2)$ to $X_0(q)$. Let us briefly recall that the moduli interpretations of these degeneracy maps from $X_0(q^2)$ to $X_0(q)$ are as follows: a point in $X_0(q^2)$ represented by (E, C)—where E is an elliptic curve and C is a cyclic subgroup of $E(\mathbb{C})$ of order q^2—is mapped by one of the degeneracy maps to $(E, C[q])$, and by the other to $(E/C[q], C/C[q])$. The maps d_1 and d_2 satisfy the relations

$$w_q \circ d_1 = d_2 \circ w_{q^2} \quad \text{and} \quad w_q \circ d_2 = d_1 \circ w_{q^2}, \tag{3.1}$$

where w_q is the involution $X_{0,\mathrm{ns}}(q, p)$ coming from the Atkin–Lehner involution of $X_0(q)$.

Let $J_{0,\mathrm{ns}}^+(q, p)$ stand for the Jacobian of $X_{0,\mathrm{ns}}^+(q, p)$. Adapting to our case a morphism from $X_0^+(q^2)$ to $J_0(q)$ that appears in Sect. 3 of [12] and in [13], we define

$$g : X_{0,\mathrm{ns}}^+(q^2, p) \to J_{0,\mathrm{ns}}^+(q, p)$$

by mapping a point P to the class of $d_1(P) - d_2(P)$. By abuse of notation, we shall denote by w_q the involution of $J_{0,\mathrm{ns}}^+(q, p)$ induced by the involution w_q of $X_{0,\mathrm{ns}}^+(q, p)$. Equation (3.1) give us the following equality:
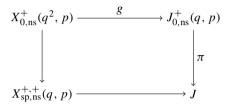
$$w_q \circ g = -g \circ w_{q^2}. \tag{3.2}$$

Consider the abelian subvariety B of $J_{0,\mathrm{ns}}^+(q, p)$ defined by $B := (1 + w_q)J_{0,\mathrm{ns}}^+(q, p)$. Define $J := J_{0,\mathrm{ns}}^+(q, p)/B$ and let π be the canonical projection from $J_{0,\mathrm{ns}}^+(q, p)$ to J. From Eq. (3.2) and Lemma 3.4, we conclude that $\pi \circ g$ factors through $X_{\mathrm{sp,ns}}^{+,+}(q, p)$. Thus, we have the following commutative diagram:

Table 2 Some modular curves

Congruence subgroup	Modular curve	Degree of j-invariant map	Ramification of ∞ w.r.t. j	Field of definition of ∞
$\Gamma_0(N)$	$X_0(N)$	$N\prod_{p\mid N}(1+1/p)$	1	$\mathbb{Q}$
$\Gamma_{\mathrm{sp}}(p)$	$X_{\mathrm{sp}}(p)$	$p(p+1)$	p	$\mathbb{Q}$
$\Gamma_{\mathrm{sp}}^+(p)$	$X_{\mathrm{sp}}^+(p)$	$p(p+1)/2$	p	$\mathbb{Q}$
$\Gamma_{\mathrm{ns}}(p)$	$X_{\mathrm{ns}}(p)$	$p(p-1)$	p	$\mathbb{Q}(\zeta_p)$
$\Gamma_{\mathrm{ns}}^+(p)$	$X_{\mathrm{ns}}^+(p)$	$p(p-1)/2$	p	$\mathbb{Q}(\zeta_p+\zeta_p^{-1})$

$$
\begin{array}{ccc}
X_{0,\mathrm{ns}}^+(q^2,p) & \xrightarrow{\quad g \quad} & J_{0,\mathrm{ns}}^+(q,p) \\
\downarrow & & \downarrow{\scriptstyle \pi} \\
X_{\mathrm{sp},\mathrm{ns}}^{+,+}(q,p) & \longrightarrow & J
\end{array}
$$

The cusp at infinity ∞ of $X_{0,\mathrm{ns}}^+(q^2,p)$ is defined over $\mathbb{Q}(\zeta_p)^+ := \mathbb{Q}(\zeta_p+\zeta_p^{-1})$ (see Table 2). Note that $\pi \circ g(\infty) = 0$.

Proposition 3.5 *There exists a non-trivial optimal quotient A of $J_{0,\mathrm{ns}}^+(q,p)$ such that $A(\mathbb{Q})$ is finite and the kernel of the canonical projection $\pi' : J_{0,\mathrm{ns}}^+(q,p) \to A$ is stable under the Hecke operators T_ℓ, ℓ prime $\neq p$. Moreover, π' factors through π.*

Proof The first part of the proposition has been proved in [6, Proposition 7.1] (even though this is only stated for the case where $q = 2, 3$, it is not hard to see that the same argument shows that the result holds for $q \in \{2, 3, 5, 7, 13\}$). In order to see that π' factors through π, note that A is defined to be the winding quotient of the new part of $J_{0,\mathrm{ns}}^+(q,p)$ (see [6]). Since $1 + w_q$ is an element of the winding ideal, it follows from the definition of J and π that π' factors through π. $\qquad\square$

Let h denote the composition of $\pi \circ g$ with the natural projection from J to A. Now, let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\zeta_p)^+$ and define $R := \mathcal{O}[1/2qp]$. Given a curve X defined over $\mathbb{Q}$, we shall write $X_{/R}$ for the minimal regular model of X over R. Similarly, given an abelian variety B, we shall write $B_{/R}$ for the Néron model of B over R. With this notation, the morphism h extends to a morphism $X_{0,\mathrm{ns}}^+(q^2,p)_{/R} \to A_{/R}$. By abuse of notation, we shall refer to this morphism by h as well.

Before stating our next result, let us recall the definition of formal immersion. Let S_1 and S_2 be two schemes and let $f : S_1 \to S_2$ be a morphism. Let x be a point in S_1 and define $y := f(x)$. Write $\hat{\mathcal{O}}_{S_1,x}$ and $\hat{\mathcal{O}}_{S_2,y}$ for the formal completions of the local rings of S_1 and S_2 at x and y, respectively. We say that f is a formal immersion at x if the induced morphism $\hat{f}_x : \hat{\mathcal{O}}_{S_2,y} \to \hat{\mathcal{O}}_{S_1,x}$ is surjective.

Now, let A be a Dedekind domain and suppose that S_1 and S_2 are schemes over $\mathrm{Spec}(A)$. Let x be a section (over A) of S_1, and let y be the section of S_2 which corresponds to the image of x. We will say that f is a formal immersion at x if f is a formal immersion at $x_{\mathfrak{p}}$ for every non-zero prime ideal $\mathfrak{p}$ of A, where $x_{\mathfrak{p}}$ stands for the special fibre of x at $\mathfrak{p}$.

Proposition 3.6 *The morphism h is a formal immersion at $\infty_{/R}$, where $\infty_{/R}$ stands for the section over R defined by ∞.*

Proof The proof of this result is standard (see, for example, [12]). Indeed, let λ be a prime of $K := \mathbb{Q}(\zeta_p)^+$ not dividing $2qp$. Let $\mathbb{F}_\lambda$ denote the residue field at λ of $\mathbb{Q}(\zeta_p)^+$. Write $\mathrm{Cot}_\infty(X_{0,\mathrm{ns}}^+(q^2, p)_{/\mathbb{F}_\lambda})$ for the cotangent space of $X_{0,\mathrm{ns}}^+(q^2, p)_{/\mathbb{F}_\lambda}$ at $\infty_{/\mathbb{F}_\lambda}$. In a similar manner, write $\mathrm{Cot}(J_{0,\mathrm{ns}}^+(q, p)_{/\mathbb{F}_\lambda})$ for the cotangent space of $J_{0,\mathrm{ns}}^+(q, p)_{/\mathbb{F}_\lambda}$ at $0_{/\mathbb{F}_\lambda}$, and the same thing goes for $\mathrm{Cot}(A)$. Showing that h is a formal immersion at $\infty_{/\mathbb{F}_\lambda}$ is equivalent to showing that the map $\mathrm{Cot}(A_{/\mathbb{F}_\lambda}) \to \mathrm{Cot}_\infty(X_{0,\mathrm{ns}}^+(q^2, p)_{/\mathbb{F}_\lambda})$ is surjective.

As the characteristic of λ is different from 2, $\mathrm{Cot}(A_{/\mathbb{F}_\lambda})$ injects into $\mathrm{Cot}(J_{0,\mathrm{ns}}^+(q, p)_{/\mathbb{F}_\lambda})$ (see [12, Corollary 1.1]). Since A is non-trivial, there exists a non-trivial element $f \in \mathrm{Cot}(A_{/\mathbb{F}_\lambda})$. Regarding f as an element of $\mathrm{Cot}(J_{0,\mathrm{ns}}^+(q, p)_{/\mathbb{F}_\lambda})$, let

$$f = \sum_{n=1}^\infty a_n(f)q^{n/p} \in \mathbb{F}_\lambda[[q^{1/p}]]$$

be the q-expansion of f. The image of f in $\mathrm{Cot}_\infty(X_{0,\mathrm{ns}}^+(q^2, p)_{/\mathbb{F}_\lambda})$ is $a_1(f)$, as can be easily checked. If $a_1(f) \neq 0$ (in $\mathbb{F}_\lambda$), then we are done. Suppose, for the sake of contradiction, that $a_1(f) = 0$ and $a_1(T_\ell f) = 0$ for every prime $\ell \neq p$. Now, $a_1(T_\ell f) = a_\ell(f)$, which yields that $a_n(f) = 0$ for every n coprime to p. Thus,

$$f = \sum_{n=1}^\infty a_{pn}(f)q^n.$$

Therefore, f is the reduction modulo λ of a cusp form in $S_2(\Gamma_0(q))$. However, since $q \in \{2, 3, 5, 7, 13\}$, this vector space is trivial, which is a contradiction. $\square$

Corollary 3.7 *The morphism $X_{\mathrm{sp,ns}}^{+,+}(q, p)_{/R} \to A_{/R}$ is a formal immersion at $\infty_{/R}$.*

Proof of Proposition 1.5 Once again, the argument is standard. We start by noting that, given a $\mathbb{Q}$-rational point P of $X_{\mathrm{sp,ns}}^{+,+}(q, p)$, its image Q in A is torsion, because the morphisms are defined over $\mathbb{Q}$ and A has finite Mordell–Weil group. Let ℓ be a prime congruent to $\pm 1 \bmod p$ (as $p \geq 11$, Proposition 3.3 asserts that these are the only primes we have to worry about). Since $p \geq 11$, we have $\ell > 2$. Note that, since $\ell \equiv \pm 1 \pmod{p}$, ℓ is inert in $\mathbb{Q}(\zeta_p)^+$. Let $\tilde{A}$ stand for the special fibre of the Néron model of A over $\mathbb{Z}_\ell$. It is well-known that the reduction map gives us an injection $\mathrm{Tors}(A(\mathbb{Q})) \hookrightarrow \tilde{A}(\mathbb{F}_\ell)$. Therefore, writing $\tilde{Q}$ for the reduction of Q modulo ℓ, we have $\tilde{Q} = 0$ in $\tilde{A}(\mathbb{F}_\ell)$ if, and only if, $Q = 0$.

Suppose that E has potentially multiplicative reduction at ℓ. Then it gives rise to a $\mathbb{Q}$-rational point P in $X_{\mathrm{sp,ns}}^{+,+}(q, p)$ which meets one of the cusps at the fibre at ℓ. By choosing appropriate bases for $\mathrm{GL}_2(\mathbb{F}_q)$ and $\mathrm{GL}_2(\mathbb{F}_p)$, we may assume that this cusp is ∞. Therefore, writing, as above, Q for the image of P in A, we find that $\tilde{Q} = 0$. Hence, by the observation of the previous paragraph, $Q = 0$. Since the morphism $X_{\mathrm{sp,ns}}^{+,+}(q, p)_{/R} \to A_{/R}$ is a formal immersion at $\infty_{/R}$ in characteristic ℓ, and as P meets ∞ at the fibre of ℓ, we must have $P = \infty$, which is a contradiction. $\square$

We are finally ready to prove Theorem 1.4.

Proof of Theorem 1.4 We will make use of Proposition 1.5. The argument used here is analogous to the one used in the proof of [10, Theorem 1.1]. Suppose that $E/\mathbb{Q}$ and q are as in the statement of Theorem 1.4. Due to Theorem 3.2, we can restrict ourselves to the case

Table 3 Equations for the j-invariants of $X_{\text{sp}}^+(q)$

q	j
3	$\dfrac{((t-9)(t+3))^3}{t^3}$
5	$\dfrac{((t^2-5)(t^2+5t+10)(t+5))^3}{(t^2+5t+5)^5}$
7	$\dfrac{((t^2-5t+8)(t^2-5t+1)(t^4-5t^3+8t^2-7t+7)(t+1))^3 t}{(t^3-4t^2+3t+1)^7}$

$q \in \{2, 3, 5, 7\}$. Moreover, as the normalisers of non-split Cartan subgroups of $\text{GL}_2(\mathbb{F}_2)$ are precisely its Borel subgroups, and as the case of Borel subgroups has already been treated by Theorem 1.3, we can assume that $q \in \{3, 5, 7\}$. Suppose that there exists a prime $p > 37$ for which $\bar{\rho}_{E,p}$ is not surjective. Then the image of $\bar{\rho}_{E,p}$ must be contained in the normaliser of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$. Proposition 1.5 now yields that the j-invariant of E must be integral. Therefore, the elliptic curve E gives rise to a $\mathbb{Q}$-rational point in $X_{\text{sp}}^+(q)$ with integral j-invariant. By an appropriate choice of uniformisers, the j-invariant map $j : X_{\text{sp}}^+(q) \to \mathbb{P}^1$ can be explicitly described by one of the equations of Table 3 (the source of these equations is [5, p. 68]).

Resorting to these equations, we are able to verify that there are only finitely many $\mathbb{Q}$-rational points in $X_{\text{sp}}^+(q)$ with integral j-invariants. Moreover, the finitely many j-invariants associated to these points can be extracted from these equations: these are $-1,22,88,000$, $-8,84,736$, $-32,768$, -5000, -1728, 0, 1728, 8000, $54,000$ and $2,87,496$. Of these, the only ones corresponding to elliptic curves without complex multiplication are -5000 and -1728. Thus, $j(E) \in \{-5000, -1728\}$.

An example of an elliptic curve with j-invariant -5000 is the one given by the equation

$$E_1 : y^2 = x^3 - x^2 - 208x + 1412,$$

and an example of an elliptic curve with j-invariant -1728 is the one given by

$$E_2 : y^2 = x^3 - 54x + 216.$$

Upon consultation on the LMFDB database [19]—where information about the image of mod p Galois representations of elliptic curves was obtained using a method of Sutherland [18]—, we can observe that, if $p > 37$, the representations $\bar{\rho}_{E_1,p}$ and $\bar{\rho}_{E_2,p}$ are both surjective. Recalling that any two elliptic curves without complex multiplication and sharing the same j-invariant are quadratic twists of each other, we conclude that $\bar{\rho}_{E,p}$ is surjective for every prime $p > 37$, yielding a contradiction. □

It is worth highlighting that Theorem 3.2 is only needed here to obtain an explicit upper bound for the non-surjective primes (which turns out to be 37). If we were only interested in showing that there exists a constant C such that $\bar{\rho}_{E,p}$ is surjective for every prime $p > C$ and every elliptic curve E satisfying the conditions of Theorem 1.4, then this could be achieved via Siegel's theorem as follows. Since the j-invariant map $j : X_{\text{sp}}^+(13) \to \mathbb{P}^1$ has more than two distinct points mapping to the point at infinity of $\mathbb{P}^1$, Siegel's theorem asserts that there are only finitely many points in $X_{\text{sp}}^+(13)(\mathbb{Q})$ whose j-invariant is integral. Therefore, even without assuming that all the $\mathbb{Q}$-rational points of $X_{\text{sp}}^+(13)$ are cuspidal or CM-points, we are still able to conclude that there are only finitely many isomorphism classes of elliptic curves satisfying the conditions of Theorem 1.4 and admitting a prime $p > 37$ for which the Galois representation $\bar{\rho}_{E,p}$ is not surjective (recall that, under these conditions, the j-invariant of

such an elliptic curve must be integral). We can now use Theorem 1.1 and the fact that, for elliptic curves without complex multiplication, the surjectivity of the Galois representation only depends on its isomorphism class to conclude the existence of our constant C.

4 The case of $\mathbb{Q}$-curves

We start by proving Theorem 1.10. Let us just remark that if K is a quadratic field and E/K is an elliptic curve completely defined over K and of degree 1, then E is defined over $\mathbb{Q}$. But Theorems 1.6, 1.7 and 1.10 are already known to hold when E is defined over $\mathbb{Q}$ (Theorem 1.7 for elliptic curves over $\mathbb{Q}$ is simply Theorem 1.4, which we have just proved). Therefore, in everything that follows, whenever we speak of a $\mathbb{Q}$-curve, we will mean a $\mathbb{Q}$-curve that is *not* defined over $\mathbb{Q}$. In the terminology of [9], these are known as *strict* $\mathbb{Q}$-curves.

4.1 Proof of Theorem 1.10

In order to obtain Theorem 1.10 from the proposition above, we will use the following result of Le Fourn.

Proposition 4.1 ([9, Proposition 3.3]) *Let K be a quadratic field and let E be a $\mathbb{Q}$-curve completely defined over K and of square-free degree d. Assume, moreover, that the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ for some prime $p = 11$ or $p \geq 17$ such that $p \nmid d$. Then $j(E) \in \mathcal{O}_K$.*

The proof will be essentially an adaptation of an argument due to Mazur that can be found in Sects. 5, 6 and 7 of [12].

From now to the end of this section, K will be a quadratic number field, E/K will be a $\mathbb{Q}$-curve completely defined over K, of square-free degree $d \geq 2$ and without complex multiplication, and $p \geq 13$ will be a prime number such that $p \nmid d$ and for which the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$. We will assume that p does not ramify in K. Consider the Galois representation $\bar{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$. As the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$, we can choose a basis P, Q of $E[p](\bar{K})$ such that $\langle P \rangle$ is a cyclic subgroup of $E(\bar{K})$ defined over K (i.e., $\tau(\langle P \rangle) = \langle P \rangle$ for every $\tau \in G_K$). With respect to this basis, the representation $\bar{\rho}_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ has the shape

$$\begin{pmatrix} \phi & * \\ 0 & \varphi \end{pmatrix},$$

where ϕ and φ are two characters $G_K \to \mathbb{F}_p^\times$.

Lemma 4.2 *Let $\mathfrak{p}$ be a prime of K dividing p. Then there exists a unique element $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ and a character $\alpha : G_K \to \mathbb{F}_p^\times$ unramified at $\mathfrak{p}$ such that $\phi = \alpha \chi_p^k$, where χ_p stands for the mod p cyclotomic character.*

Proof Let $G_{\mathfrak{p}}$ be a decomposition subgroup of G_K associated to $\mathfrak{p}$ and let $\mathcal{O}_{\mathfrak{p}}$ denote the ring of integers of $K_{\mathfrak{p}}$, the completion of K at $\mathfrak{p}$. The Artin map of class field theory gives us a continuous homomorphism $\mathcal{O}_{\mathfrak{p}}^\times \to G_{\mathfrak{p}}^{\mathrm{ab}}$, from where we obtain another continuous map $\mathcal{O}_{\mathfrak{p}}^\times \to \mathbb{F}_p^\times$ by composition with $\phi|_{G_{\mathfrak{p}}}$. Using the assumption that p does not ramify in K, it is easy to see that every continuous homomorphism $\mathcal{O}_{\mathfrak{p}}^\times \to \mathbb{F}_p^\times$ must factor through $N : \mathcal{O}_{\mathfrak{p}}^\times \to \mathbb{Z}_p^\times$, where N stands for the norm map. The result now follows from the fact that

every continuous homomorphism $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ is a power of the cyclotomic character (where we identify $\mathbb{Z}_p^\times$ with the inertia subgroup of $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p)$ via local class field theory). □

Let $\mathfrak{p}$ be a prime of K lying above p. We now know that $\bar\rho_{E,p}$ has the shape

$$\begin{pmatrix} \alpha\chi_p^k & * \\ 0 & \alpha^{-1}\chi_p^{1-k} \end{pmatrix},$$

where α is some character unramified at $\mathfrak{p}$. If p remains prime in K, then, trivially, α is unramified at every prime of K lying above p. The next lemma asserts that this is also true even if p splits.

Lemma 4.3 *Using the above notation, α is unramified at every prime of K lying above p.*

Proof This is only true because we are assuming that the image of $\mathbb{P}\bar\rho_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$. Let us start by recalling the notation introduced in Sect. 2. For each element $\tau \in G_\mathbb{Q}$, we have a K-isogeny $\mu_\tau : {}^\tau E \to E$ satisfying the following conditions: if the restriction of τ to K is the trivial automorphism of K, then μ_τ is the identity; if, on the other hand, the restriction of τ to K is the non-trivial automorphism of K, then μ_τ has degree d and, moreover, if $\tau' \in G_\mathbb{Q}$ is another element restricting to the non-trivial automorphism of K, then $\mu_\tau = \mu_{\tau'}$. Note that as the image of $\mathbb{P}\bar\rho_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$, we have $\mu_\tau({}^\tau P) \in \langle P \rangle$ for every $\tau \in G_\mathbb{Q}$.

As the result trivially holds when p remains prime in K, and as we are assuming that p does not ramify in K, we will assume that p splits in K. If this is the case, let $\mathfrak{q}$ be the other prime of K lying above p. Let $\sigma \in G_\mathbb{Q}$ be an element which restricts to the non-trivial automorphism of K. If $D_\mathfrak{p}$ is a decomposition subgroup of G_K over $\mathfrak{p}$, then $D_\mathfrak{q} := \sigma D_\mathfrak{p}\sigma^{-1}$ is a decomposition subgroup of G_K over $\mathfrak{q}$. Moreover, if $I_\mathfrak{p}$ and $I_\mathfrak{q}$ denote the corresponding inertia subgroups, we have $I_\mathfrak{q} = \sigma I_\mathfrak{p}\sigma^{-1}$. Therefore, every element of $I_\mathfrak{q}$ can be uniquely written in the form $\sigma\tau\sigma^{-1}$ with $\tau \in I_\mathfrak{p}$. Let $\tau \in I_\mathfrak{p}$. As any $\tau \in I_\mathfrak{p}$ acts as $\chi_p(\tau)^k$ on $\langle P \rangle$, and as $\mu_\sigma({}^\sigma P) \in \langle P \rangle$, we get

$$ {}^{\tau\sigma^{-1}}P = {}^\tau({}^{\sigma^{-1}}P) = \chi_p^k(\tau)({}^{\sigma^{-1}}P). $$

But then

$$ {}^{\sigma\tau\sigma^{-1}}P = \chi_p(\tau)^k P $$

for every $\tau \in I_\mathfrak{p}$. Therefore, the restriction of ϕ to $I_\mathfrak{q}$ is χ_p^k, proving that $\phi = \alpha\chi_p^k$ for some character $\alpha : G_K \to \mathbb{F}_p^\times$ unramified at every prime dividing p. □

Lemma 4.4 *Using the above notation, there are integers $e \mid 12$ and $a, b \in \{0, \ldots, e\}$ such that*

(1) $e \le 6$,
(2) $a + b = e$,
(3) $ek \equiv a \pmod{p-1}$ *and*
(4) $e(1-k) \equiv b \pmod{p-1}$.

Proof We know that E has potentially good reduction at $\mathfrak{p}$. Therefore, after taking a field extension L of $K_\mathfrak{p}$ with ramification degree dividing 12, but at most 6, the curve E acquires good reduction at $\mathfrak{p}$. Let e denote the absolute ramification degree of L. As we are assuming that p does not ramify in K, the integer e is the ramification degree of L over $K_\mathfrak{p}$. Let $I_\mathfrak{p}$ and I_L denote the inertia subgroups of $G_{K_\mathfrak{p}}$ and G_L, respectively, and let $I_\mathfrak{p}^t$ and I_L^t denote

the respective tame inertia groups. Of course, ϕ and φ factor through $I_{\mathfrak{p}}^t$. Let θ denote the fundamental character of level 1 for I_L. We have $\chi_p = \theta^e$. Therefore, $\phi|_{I_L} = \theta^{ek}$ and $\varphi|_{I_L} = \theta^{e(1-k)}$. By a theorem of Raynaud, there are integers $a, b \in \{0, \ldots, e\}$ such that

$$ek \equiv a \pmod{p-1} \quad \text{and} \quad e(1-k) \equiv b \pmod{p-1}.$$

In particular, we have $a + b \equiv e \pmod{p-1}$. However, $a + b \leq 2e \leq 12 \leq p-1$, yielding

$$a + b = e \leq 6,$$

as we wanted. $\square$

Following the notation of Mazur [12], we set $m := (p-1)/2$, $n := \text{num}((p-1)/12)$ and $t := m/n$.

Lemma 4.5 (cf. [12, Lemma 5.3]) α^{2t} *is unramified everywhere.*

Proof The proof of this lemma is exactly the same as the one given by Mazur in [12, Lemma 5.3]. For convenience of the reader, we reproduce it here. Let $S := \text{Spec } \mathbb{Z}[1/p]$. Consider the finite flat cyclic covering $X_1(p)_{/S} \to X_0(p)_{/S}$ of degree $(p-1)/2$. There is an intermediate cover

$$X_1(p)_{/S} \to X_2(p)_{/S} \to X_0(p)_{/S}.$$

The only properties of the covering $X_2(p)_{/S} \to X_0(p)_{/S}$ that we are going to use are the following: it is a finite étale morphism of smooth S-schemes and its Galois group is isomorphic to the cyclic group $\mathbb{Z}/n\mathbb{Z}$, where $n := \text{num}((p-1)/12)$. This yields that the degree of $X_1(p) \to X_2(p)$ is t.

Our curve E gives rise to a point $x = [(E, C_p)] \in X_0(p)(K)$. As all the coverings are cyclic, there exists a finite abelian extension L/K for which there is a point $y = [(E', P')] \in X_1(p)(L)$ mapping to x. Moreover, as $X_2(p)_{/S} \to X_0(p)_{/S}$ is finite étale, the ramification degree of L/K at any prime of characteristic different from p divides t, and so it also divides 6. Now, as y maps to x, there is an L-isomorphism $f : E \to E'$ mapping C_p to $\langle P' \rangle$. The L-isomorphism f is associated to an element of $H^1(\text{Gal}(L/K), \text{Aut}_L(E))$. However, $\text{Aut}_L(E) = \{\pm 1\}$, as E does not have complex multiplication. Therefore, given a prime λ of K of characteristic different from p, we find that $\alpha^t|_{I_\lambda}$ is a quadratic character, yielding that α^{2t} is unramified at λ. As we already know that α is unramified at any prime of characteristic p, we get the result. $\square$

Let us just review what we have so far. The mod p Galois representation $\bar{\rho}_{E,p}$ has the shape

$$\begin{pmatrix} \alpha \chi_p^k & * \\ 0 & \alpha^{-1} \chi_p^{1-k} \end{pmatrix},$$

where χ_p is the mod p cyclotomic character, α is a character such that α^{2t} is unramified everywhere, and k satisfies the properties listed in Lemma 4.4.

Let λ be a prime of K of characteristic different from p. Write G_λ for a decomposition subgroup of G_K over λ. Let α_λ denote the restriction of the character α to G_λ. As in Sect. 6 of [12], we are going to split it in its ramified and unramified part. From local class field theory, we have a (non-unique) decomposition

$$G_\lambda^{\text{ab}} \cong \mathcal{O}_\lambda^\times \times \hat{\mathbb{Z}},$$

where $\mathcal{O}_\lambda$ denotes the ring of integers of K_λ. Sticking to the notation of Mazur, we write $\alpha_\lambda = \gamma_\lambda \cdot b_\lambda$, where the character γ_λ factors through $\mathcal{O}_\lambda^\times$ in the decomposition above and b_λ

is unramified. Lemma 4.5 implies that γ_λ has order dividing $2t$. Let L denote the splitting field of γ_λ. This is a totally ramified extension of K_λ of degree dividing $2t$.

Lemma 4.6 *Using the above notation, the elliptic curve E has good reduction over L.*

Proof Suppose, for the sake of contradiction, that E does not have good reduction over L. Let $\mathbb{F}_q$ denote the residue field of K (q being its size) and $\tilde{E}/\mathbb{F}_q$ denote the special fibre of the Néron model of E over $\mathcal{O}_L$ (as L is totally ramified, the residue field of L is that of K). Note that we have

$$\bar{\rho}_{E,p}|_{\mathrm{Gal}(\bar{L}/L)} \sim \begin{pmatrix} b_\lambda \chi_p^k & * \\ 0 & b_\lambda^{-1} \chi_p^{1-k} \end{pmatrix}.$$

Let F be the splitting field of $b_\lambda \chi_p^k$. Then F is an unramified extension of L and $E(F)$ has a p-torsion point. Moreover, as Néron models are stable under étale base change, the special fibre of the Néron model of E over $\mathcal{O}_F$ is $\tilde{E}_{/\mathbb{F}_F}$, where $\mathcal{O}_F$ is the ring of integers of F and $\mathbb{F}_F$ is its residuel field. We conclude that there is a p-torsion point in $\tilde{E}(\mathbb{F}_F)$, which is clearly impossible when E has bad reduction at L. Therefore, E acquires good reduction at L. $\square$

As a consequence, $\bar{\rho}_{E,p}|_{\mathrm{Gal}(\bar{L}/L)}$ factors through $\mathrm{Gal}(L^{\mathrm{unr}}/L)$. The Galois group $\mathrm{Gal}(L^{\mathrm{unr}}/L)$ is generated by the Frobenius automorphism Frob_λ.

Lemma 4.7 *Let c denote the narrow class number of K. Then*

(1) $b_\lambda(\mathrm{Frob}_\lambda)q^k + b_\lambda(\mathrm{Frob}_\lambda)^{-1}q^{1-k} \equiv \mathrm{Tr}(\mathrm{Frob}_\lambda) \pmod{p}$; *and*
(2) $q^{12ck} + q^{12c(1-k)} \equiv \mathrm{Tr}(\mathrm{Frob}_\lambda^{12c}) \pmod{p}$,

where q is the size of the residue field of K_λ and $\mathrm{Tr}(\mathrm{Frob}_\lambda) \in \mathbb{Z}$ is the trace of the action of the Frobenius element of $\mathrm{Gal}(L^{\mathrm{unr}}/L)$ on the p-adic Tate module of E.

Proof Congruence (1) follows from simply taking the trace of $\bar{\rho}_{E,p}(\mathrm{Frob}_\lambda)$. Congruence (2) follows from taking the trace of $\bar{\rho}_{E,p}(\mathrm{Frob}_\lambda^{12c})$ and recalling (see Lemma 4.5) that α^{12} is unramified everywhere (as $2t \mid 12$) and so, from class field theory, we have $\alpha^{12c} = 1$. $\square$

Proof of Theorem 1.10 for $p \equiv 1 \pmod 4$ Let λ be a prime of K dividing 2 and let f denote the residual degree of λ. From Lemma 4.7, we get

$$q^{12ck} + q^{12c(1-k)} \equiv \mathrm{Tr}(\mathrm{Frob}_\lambda^{12c}) \pmod{p},$$

where $q = 2^f$. Using the notation and results of Lemma 4.4, we have $e \mid 12$ and $e \leq 6$. Therefore, we can write $12 = re$ for some integer $2 \leq r \leq 12$. So,

$$q^{rca} + q^{rcb} \equiv \mathrm{Tr}(\mathrm{Frob}_\lambda^{12c}) \pmod{p}, \tag{4.1}$$

where a, b are as in Lemma 4.4. Now, by the Hasse–Weil bounds,

$$|\mathrm{Tr}(\mathrm{Frob}_\lambda^{12c})| \leq 2 \cdot q^{6c}.$$

We are now going to show that if $p \equiv 1 \pmod 4$, then $2 \cdot q^{6c} < q^{rca} + q^{rcb}$. Suppose, for the sake of contradiction, that we have $2 \cdot q^6 \geq q^{rca} + q^{rcb}$. If $ra > 6$ (and so $rb = 12 - ra < 6$), then it is easy to see that $2 \cdot q^{6c} < q^{rca} + q^{rcb}$. By symmetry, we cannot have $ra < 6$ either, nor $rb < 6$, nor $rb > 6$. Therefore, $ra = rb = 6$, yielding one of the following cases:

(1) $r = 2$, $e = 6$ and $a = b = 3$;
(2) $r = 3$, $e = 4$ and $a = b = 2$; or

(3) $r = 6$, $e = 2$ and $a = b = 1$.

Case (1) yields $6k \equiv 3 \pmod{p-1}$, which is not possible, as p is odd. For similar reasons, we cannot have case (3): here we would be forced to have $2k \equiv 1 \pmod{p-1}$. We are only left with case (2). In this case, we obtain the congruence $4k \equiv 2 \pmod{p-1}$. If $p \equiv 1 \pmod 4$, this is not possible. Thus, in this case, we must have

$$2 \cdot q^{6c} < q^{rca} + q^{rcb}.$$

From this and from the congruence (4.1), we obtain a bound

$$p \leq q^{rca} + q^{rcb} + 2 \cdot q^{6c} \leq 2 \cdot q^{12c} + 2 \cdot q^{6c} = 2^{6fc+1}(2^{6fc} + 1),$$

as we wanted. $\qquad\square$

Let us now turn to the case where $p \equiv 3 \pmod 4$. As we have seen in the proof above, if we are not in any of the cases (1), (2) or (3), then we obtain the bound $2^{6fc+1}(2^{6fc} + 1)$. We therefore assume we are in one of these cases. Again, (1) and (3) cannot occur, so let us assume we are in case (2). In other words, we are going to assume, from now on, that $r = 3$, $e = 4$ and $a = b = 2$. As observed above, this yields $2k \equiv 1 \pmod m$ (where, recall, m was defined to be $(p-1)/2$), and, moreover, $t = 1$ or $t = 3$. Analogously to what is done in [12], the aim of what follows is to show that every prime $5 \leq \ell < p/4$ unramified in K and such that $\ell \nmid d$ satisfies

$$\left(\frac{\ell}{p} \right) = -1.$$

After this has been proven, an application of Minkowski's bound for the norm of ideals in a class of the ideal class group will yield the theorem (cf. Sect. 7 of [12]).

Before proceeding, let us make a remark that will be useful later on. Note that, as a consequence of E not having complex multiplication, we have $\mu_\sigma \circ {}^\sigma\mu_\sigma = d$ or $-d$, where $\sigma \in G_{\mathbb{Q}}$ restricts to the non-trivial automorphism of K.

Lemma 4.8 *Let K' be a quadratic extension of K. Let E' be a K'-twist of E, and let $g : E_{/K'} \to E'_{/K'}$ be a K'-isomorphism. Then $\mu'_\sigma := g \circ \mu_\sigma \circ {}^\sigma g^{-1}$ is a K-isogeny from ${}^\sigma E'$ to E' for every $\sigma \in G_{\mathbb{Q}}$. In particular, E' is a $\mathbb{Q}$-curve completely defined over K and of degree d. Moreover, $\mu'_\sigma \circ {}^\sigma\mu'_\sigma = \mu_\sigma \circ {}^\sigma\mu_\sigma$.*

Proof All of these statements are easy to prove. If E' is a trivial twist (i.e., if it is K-isomorphic to E), then the result is trivial. Suppose then that this is not the case. Consider the map $\tau \mapsto g^{-1}({}^\tau g)$, $\tau \in \mathrm{Gal}(K'/K)$. This is a 1-cocycle $\mathrm{Gal}(K'/K) \to \mathrm{Aut}_{K'}(E_{K'})$. As E does not have complex multiplication, $\mathrm{Aut}_{K'}(E_{K'}) = \{\pm 1\}$, and so

$$H^1(\mathrm{Gal}(K'/K), \mathrm{Aut}_{K'}(E_{K'})) = \mathrm{Hom}(\mathrm{Gal}(K'/K), \{\pm 1\}).$$

Thus, $\tau \mapsto g^{-1}({}^\tau g)$ is a quadratic character $\mathrm{Gal}(K'/K) \to \{\pm 1\}$. As we are assuming that E' is not a trivial twist, we conclude that ${}^\tau g = -g$ if $\tau \in \mathrm{Gal}(K'/K)$ is the non-trivial element. Similarly, ${}^\tau({}^\sigma g) = -{}^\sigma g$ for every $\sigma \in G_{\mathbb{Q}}$. Therefore,

$${}^\tau\mu'_\sigma = {}^\tau g \circ {}^\tau\mu_\sigma \circ {}^\tau({}^\sigma g^{-1}) = \mu'_\sigma,$$

meaning that μ'_σ is defined over K. It is clear that μ'_σ has degree d.

Finally,

$$\mu'_\sigma \circ {}^\sigma\mu'_\sigma = g \circ \mu_\sigma \circ {}^\sigma g^{-1} \circ {}^\sigma g \circ {}^\sigma\mu_\sigma \circ g^{-1} = \mu_\sigma \circ {}^\sigma\mu_\sigma,$$

as we wanted. $\qquad\square$

As a consequence of this lemma, we may assume, after taking an appropriate quadratic twist if needed, that E satisfies one of the following statements:

(A) $\mu_\sigma \circ {}^\sigma \mu_\sigma = d$ and $b_\lambda(\mathrm{Frob}_\lambda) \neq -1$ for every prime λ of K of residual degree 2 and of odd characteristic $< p/4$;

(B) $\mu_\sigma \circ {}^\sigma \mu_\sigma = -d$ and $b_\lambda(\mathrm{Frob}_\lambda) \neq 1$ for every prime λ of K of residual degree 2 and of odd characteristic $< p/4$.

In order to treat the case where $p \equiv 3 \pmod 4$, we will resort to some general theory that can be consulted in [15].

Let $A/\mathbb{Q}$ be the abelian surface defined by $A := \mathrm{Res}_{K/\mathbb{Q}}(E)$. This is a $\mathbb{Q}$-simple abelian variety of GL_2-type. Let $F := \mathbb{Q} \otimes \mathrm{End}_\mathbb{Q}(A)$. Then F is either $\mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{-d})$, depending on whether $\mu_\sigma \circ {}^\sigma \mu_\sigma = d$ or $-d$, respectively (see Sect. 7 of [15]). Let $\mathfrak{q}$ be a prime of F over p. If we denote by $\rho_{E,p}$ the Galois representation of E obtained by the Galois action on the Tate module $V_p(E) := T_p(E) \otimes \mathbb{Q}_p$, then we have

$$\rho_{A,\mathfrak{q}}|_{G_K} \cong \rho_{E,p},$$

where $\rho_{A,\mathfrak{q}}$ stands for the Galois representation obtained from the Galois action on $V_\mathfrak{q}(A) := V_p(A) \otimes_{F \otimes \mathbb{Q}_p} F_\mathfrak{q}$ (recall that $V_p(A)$ is free of rank 2 over $F \otimes \mathbb{Q}_p$). The reduction of $\rho_{A,\mathfrak{q}}$ modulo $\mathfrak{q}$ is well-defined up to semi-simplification, so we are going to denote by

$$\bar\rho_{A,\mathfrak{q}} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_\mathfrak{q})$$

this semi-simplified reduction. If we write $\bar\rho_{E,p}^{\mathrm{ss}}$ for the semi-simplification of $\bar\rho_{E,p}$, then $\bar\rho_{A,\mathfrak{q}}|_{G_K}$ is isomorphic to $\bar\rho_{E,p}^{\mathrm{ss}}$. It can be easily verified that the condition that the image of $\mathbb{P}\bar\rho_{E,p}$ is contained in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ implies that the image of $\bar\rho_{A,\mathfrak{q}}$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\mathfrak{q})$, and so is contained in a split Cartan, as $\bar\rho_{A,\mathfrak{q}}$ is semi-simple (see Sect. 6 of [15] and, in particular, [15, Lemma 6.4]).

Let us just mention a standard lemma that will be useful later. This is just a special case of [4, Chapitre III, 9.4, Proposition 6], but it suffices for our purposes.

Lemma 4.9 *Define $R_p := F \otimes \mathbb{Q}_p$. Let $f \in \mathrm{End}_{R_p}(V_p(A))$. Let $P_f(T) \in R_p[T]$ be the characteristic polynomial of f. Regarding f as an element of $\mathrm{End}_{\mathbb{Q}_p}(V_p(A))$, let $Q_f(T) \in \mathbb{Q}_p[T]$ be the characteristic polynomial of f. Let $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ be the non-trivial element. Then τ defines an automorphism of $R_p[T]$. Let $N_{F/\mathbb{Q}} : R_p[T] \to \mathbb{Q}_p[T]$ denote the map obtained by $h(T) \mapsto h(T)^\tau h(T)$. Then*

$$N_{F/\mathbb{Q}}(P_f(T)) = Q_f(T).$$

As p is unramified in K, and as $\bar\rho_{A,\mathfrak{q}}|_{G_K}$ is isomorphic to $\bar\rho_{E,p}^{\mathrm{ss}}$, we find that

$$\bar\rho_{A,\mathfrak{q}} \sim \begin{pmatrix} \beta\chi_p^k & 0 \\ 0 & \theta\beta^{-1}\chi_p^{1-k} \end{pmatrix}$$

for some character $\beta : G_\mathbb{Q} \to \mathbb{F}_\mathfrak{q}^\times$ unramified at p such that $\beta|_{G_K} = \alpha$, and where $\theta : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_\mathfrak{q})$ is a quadratic character defined as follows: if $\sigma \in G_\mathbb{Q}$ restricts to the non-trivial automorphism of K, then

$$\theta(\sigma) = \frac{\mu_\sigma \circ {}^\sigma \mu_\sigma}{d};$$

otherwise, the image is 1 (see Sect. 7 of [15]). In particular, if $\mu_\sigma \circ {}^\sigma \mu_\sigma = d$, then F is real and $\theta = 1$.

Notation In order to simplify exposition, from here on, given a rational prime ℓ, we are going to assume we have fixed an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$. This amounts to choosing a decomposition subgroup G_ℓ of $G_{\mathbb{Q}}$ over ℓ. Moreover, every number field L will be regarded as subfields of $\bar{\mathbb{Q}}$, so that, given a prime λ of L dividing ℓ, we have an embedding of the decomposition subgroup G_λ of L over λ into G_ℓ. Similarly, algebraic extensions of $\mathbb{Q}_\ell$ will be regarded as subfields of $\bar{\mathbb{Q}}_\ell$.

In what follows, λ will be a prime of K and ℓ will be the rational prime lying below λ. We will further assume that $5 \leq \ell < p/4$, $\ell \nmid d$ and that ℓ does not ramify in K. Moreover, we will assume that p is large enough so that it does not ramifiy in F. Write β_ℓ for the restriction of β to G_ℓ. As we did before, we can resort to class field theory to (non-uniquely) decompose G_ℓ^{ab} as

$$G_\ell^{\mathrm{ab}} \cong \mathbb{Z}_\ell^\times \times \hat{\mathbb{Z}},$$

and we obtain a decomposition $\beta_\ell = \eta_\ell \cdot \delta_\ell$, where η_ℓ factors through $\mathbb{Z}_\ell^\times$ and δ_ℓ is unramified. Let L' be the splitting field of η_ℓ. It is a totally ramified extension of $\mathbb{Q}_\ell$. Moreover, if we keep writing L for the splitting field of γ_λ over K_λ in the decomposition of G_λ^{ab}, it can be easily checked that L is an unramified extension of L' of degree equal to that of $K_\lambda/\mathbb{Q}_\ell$. Therefore, the degree of $L'/\mathbb{Q}_\ell$ is the same as the degree of L/K_λ. In particular, it divides $2t$.

Lemma 4.10 *Using the above notation, $\beta^{4t} = 1$. Moreover, if ℓ splits in K, then $\beta_\ell^{2t} = 1$.*

Proof Recall that $\beta|_{G_K} = \alpha$, and that α^{2t} is unramified at every prime of K (see Lemma 4.5). We claim that β^{4t} is unramified everywhere.

Let ℓ be a rational prime and let λ a prime of K dividing ℓ. Let I_ℓ and I_λ denote the inertia subgroups of G_ℓ and G_λ, respectively. Note that $[G_{\mathbb{Q}} : G_K] \leq 2$. Therefore, if $\tau \in I_\ell$, we have $\tau^2 \in I_\lambda$. Therefore, $\beta(\tau)^{4t} = \beta(\tau^2)^{2t} = \alpha(\tau^2)^{2t} = 1$, because α^{2t} is unramified everywhere. This shows that β^{4t} is unramified everywhere.

As β^{4t} is a character defined on $G_{\mathbb{Q}}$, it follows that it is trivial, which proves the first part of the lemma.

If ℓ is a rational prime splitting in K, then $G_\ell = G_\lambda$, and so we have $\beta(\tau) \in \mathbb{F}_p^\times$ for every $\tau \in G_\ell$. As $\beta(\tau)^{4t} = 1$, we must have $\beta(\tau)^{2t} = \pm 1$. Note that -1 is not a quadratic residue modulo p, as $p \equiv 3 \pmod 4$. Therefore, we are forced to have $\beta(\tau)^{2t} = 1$. □

Lemma 4.11 *Using the above notation, A acquires good reduction over L'.*

Proof Denoting the absolute Galois group of L' by $G_{L'}$, what we have to show is that $\rho_{A,p}|_{G_{L'}}$ is unramified, where $\rho_{A,p}$ is the Galois representation of the Tate module $V_p(A)$ of A. As L is unramified over L', it is enough to show that $\rho_{A,p}|_{G_L}$ is unramified. Since A is the Weil restriction of E from K to $\mathbb{Q}$, and noting that $K \subseteq L$, we see that $\rho_{A,p}|_{G_L}$ is the direct sum of the Galois representations (restricted to G_L) associated to $V_p(E)$ and $V_p({}^\sigma E)$, where $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is non-trivial. As these two representations are isomorphic, it is therefore enough to show that $\rho_{E,p}|_{G_L}$ is unramified. But we already know from Lemma 4.6 that E has good reduction over L, which yields that $\rho_{E,p}|_{G_L}$ is unramified, finishing the proof of the lemma. □

As a consequence, $\rho_{A,\mathfrak{q}}|_{G_{L'}}$ factors through $\mathrm{Gal}((L')^{\mathrm{unr}}/L')$. Writing Frob_ℓ for the Frobenius element of $\mathrm{Gal}((L')^{\mathrm{unr}}/L')$, we obtain a result analogous to Lemma 4.7:

$$\delta_\ell(\mathrm{Frob}_\ell)\ell^k + \theta(\mathrm{Frob}_\ell)\delta_\ell(\mathrm{Frob}_\ell)^{-1}\ell^{1-k} \equiv a_\ell \pmod{\mathfrak{q}}, \tag{4.2}$$

where $a_\ell \in \mathcal{O}_F$ stands for the trace of $\rho_{A,\mathfrak{q}}(\mathrm{Frob}_\ell)$. If we denote by $P_\ell(T)$ the characteristic polynomial of $\rho_{A,\mathfrak{q}}(\mathrm{Frob}_\ell)$ (which has coefficients in F), then Lemma 4.9 asserts that $N_{F/\mathbb{Q}}(P_\ell(T))$ is precisely the characteristic polynomial of $\rho_{A,p}(\mathrm{Frob}_\ell)$. As all the roots of the characteristic polynomial of $\rho_{A,p}(\mathrm{Frob}_\ell)$ have complex size $\sqrt{\ell}$ (independently of the embedding into $\mathbb{C}$ chosen), we conclude that $|a_\ell| \le 2\sqrt{\ell}$ for every embedding of F into $\mathbb{C}$.

Proof of Theorem 1.10 for $p \equiv 3 \pmod 4$ Suppose, for contradiction, that ℓ is a quadratic residue modulo p. Then $\ell^m \equiv 1 \pmod p$. As $2k \equiv 1 \pmod m$, we have $\ell^k \equiv \ell^{1-k} \pmod p$. We divide the proof in two parts: one to treat the cases where ℓ splits in K, and the other to treat the cases where ℓ remains prime.

Suppose that ℓ splits in K. Then $\theta(\mathrm{Frob}_\ell) = 1$. Eq. (4.2) yields

$$\ell^k(\delta_\ell(\mathrm{Frob}_\ell) + \delta_\ell(\mathrm{Frob}_\ell)^{-1}) \equiv a_\ell \pmod{\mathfrak{q}}.$$

From Lemma 4.10, and from the fact that $t = 1$ or $t = 3$, we conclude that either $\delta_\ell(\mathrm{Frob}_\ell)$ is a 3rd root of unity, or $-\delta_\ell(\mathrm{Frob}_\ell)$ is. Thus, $\delta_\ell(\mathrm{Frob}_\ell) + \delta_\ell(\mathrm{Frob}_\ell)^{-1} = \pm 1$ or $\delta_\ell(\mathrm{Frob}_\ell) + \delta_\ell(\mathrm{Frob}_\ell)^{-1} = \pm 2$, and we find

$$\pm \ell^k \equiv a_\ell \pmod{\mathfrak{q}} \quad \text{or} \quad \pm 2\ell^k \equiv a_\ell \pmod{\mathfrak{q}}.$$

Taking norms from F to $\mathbb{Q}$, and recalling that $\ell^{2k} \equiv \ell \pmod p$, we get

$$\ell \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod p \quad \text{or} \quad 4\ell \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod p.$$

As $|a_\ell| \le 2\sqrt{\ell}$ for every embedding of F in $\mathbb{C}$ and as $\ell < p/4$, we conclude that we must have $\ell = N_{F/\mathbb{Q}}(a_\ell)$ or $4\ell = N_{F/\mathbb{Q}}(a_\ell)$. In any case, $v_\ell(N_{F/\mathbb{Q}}(a_\ell)) = 1$, which is only possible if ℓ ramifies in F. However, $F = \mathbb{Q}(\sqrt{d})$ or $F = \mathbb{Q}(\sqrt{-d})$, and ℓ is an odd prime not dividing d, so we obtain a contradiction. Therefore, if $3 \le \ell < p/4$, $\ell \nmid d$ and if ℓ splits in K, then ℓ is not a quadratic residue modulo p.

Suppose now that ℓ remains prime in K. Assume that (A) holds. In this case, we have $\theta(\mathrm{Frob}_\ell) = 1$, because $\mu_\sigma \circ {}^\sigma \mu_\sigma = d$. We obtain the congruence

$$\ell^k(\delta_\ell(\mathrm{Frob}_\ell) + \delta_\ell(\mathrm{Frob}_\ell)^{-1}) \equiv a_\ell \pmod{\mathfrak{q}}.$$

Also, from Lemma 4.10, we know that $\delta_\ell^{4t} = 1$, so either $\delta_\ell(\mathrm{Frob}_\ell)^2$ is a 3rd root of unity, or $-\delta_\ell(\mathrm{Frob}_\ell)^2$ is. As, from (A), $b_\lambda(\mathrm{Frob}_\lambda) \ne -1$, and as $b_\lambda(\mathrm{Frob}_\lambda) = \delta_\ell(\mathrm{Frob}_\ell)^2$, we see that $b_\lambda(\mathrm{Frob}_\lambda)$ is either 1, a primitive third root of unity or the negative of a primitive third root of unity. In the first case, we get $\delta_\ell(\mathrm{Frob}_\ell) = \pm 1$, which leads to

$$\pm 2\ell^k \equiv a_\ell \pmod{\mathfrak{q}}.$$

If, on the other hand, $b_\lambda(\mathrm{Frob}_\lambda)$ is a primitive third root of unity, then, in particular, $\delta_\ell(\mathrm{Frob}_\ell)^6 = 1$, which means that $\delta_\ell(\mathrm{Frob}_\ell)^3$ is a square root of 1. The situation where $\delta_\ell(\mathrm{Frob}_\ell) = \pm 1$ takes us to the situation above, so we may assume that either $\delta_\ell(\mathrm{Frob}_\ell)$ is a primitive third root of unity, or $-\delta_\ell(\mathrm{Frob}_\ell)$ is. This leads to

$$\pm \ell^k \equiv a_\ell \pmod{\mathfrak{q}}.$$

Finally, if $-b_\lambda(\mathrm{Frob}_\lambda)$ is a primitive third root of unity, then $\delta_\ell(\mathrm{Frob}_\ell)^6 = -1$, which means that $\delta_\ell(\mathrm{Frob}_\ell) \notin \mathbb{F}_p^\times$, as $p \equiv 3 \pmod 4$. In particular, p remains prime in F. Moreover, as $\delta_\ell(\mathrm{Frob}_\ell)^2 \in \mathbb{F}_p^\times$, we see that the Galois conjugate of $\delta_\ell(\mathrm{Frob}_\ell)$ is $-\delta_\ell(\mathrm{Frob}_\ell)$. Thus, taking norms from $\mathbb{F}_\mathfrak{q}$ to $\mathbb{F}_p$, we get

$$-\ell^{2k}(\delta_\ell(\mathrm{Frob}_\ell)^2 + \delta_\ell(\mathrm{Frob}_\ell)^{-2} + 2) \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod p,$$

and so

$$-3\ell^{2k} \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod{p}.$$

Recalling that $\ell^{2k} \equiv \ell \pmod{p}$, and after taking norms from F to $\mathbb{Q}$ in the appropriate cases, the three cases above give

$$4\ell \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod{p} \quad \text{or} \quad \ell \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod{p} \quad \text{or} \quad -3\ell \equiv N_{F/\mathbb{Q}}(a_\ell) \pmod{p}.$$

Using the same kind of arguments we used above, we conclude that $v_\ell(N_{F/\mathbb{Q}}(a_\ell)) = 1$, implying that ℓ ramifies in F (recall that we are assuming that $\ell > 3$), which it does not.

We omit the proof of the case where ℓ remains prime in K and (B) holds, as it is treated in a similar manner to the case where (A) holds, except that now we have $\theta(\mathrm{Frob}_\ell) = -1$.

We conclude that if ℓ is a prime satisfying $5 \le \ell < p/4$, $\ell \nmid d$ and if ℓ does not ramify in K, then ℓ is not a quadratic residue modulo p. In other words, ℓ remains prime in $\mathbb{Q}(\sqrt{-p})$. If m_d is the number of prime divisors of d and m_K is the number of rational primes that ramify in K, then the number of primes $< p/4$ which do not remain prime in $\mathbb{Q}(\sqrt{-p})$ is $\le m_d + m_K + 2$. Therefore, there is an integer $M_{K,d}$ depending only of K and d such that the number of classes of the ideal class group of $\mathbb{Q}(\sqrt{-p})$ represented by an integral ideal of norm $< p/4$ is $\le M_{K,d}$. However, a well-known result of Minkowski states that each class of the ideal class group is represented by an integral ideal of norm $< 2\sqrt{p}/\pi$, which is a number smaller than $p/4$. This means that the class number of $\mathbb{Q}(\sqrt{-p})$ is bounded above by $M_{K,d}$. As there are only finitely many imaginary quadratic fields of a given class number, we conclude that p can only be one of finitely many possibilities which only depend on K and d. Theorem 1.10 follows. $\qquad\square$

4.2 The Borel case

The aim of this section is to provide a proof of Proposition 1.8 and Theorem 1.6. The arguments used to prove Proposition 1.8 follow closely those of Ellenberg [8].

Let p and q be as in the statement of Proposition 1.8. Define

$$Z_{d,0}(q, p) := X_0(d) \times_{X(1)} X_{0,\mathrm{ns}}^+(q, p).$$

Lemma 4.12 *Let w_d denote the involution of $Z_{d,0}(q, p)$ induced by the Atkin–Lehner involution of $X_0(d)$. Let E be a $\mathbb{Q}$-curve as in the statement of Proposition 1.8. Then E gives rise to a K-point P in $Z_{d,0}(q, p)$ satisfying $w_d P = {}^\sigma P$ for every $\sigma \in G_\mathbb{Q}$ restricting to the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$.*

Proof The proof of this result is identical to the proof of [8, Proposition 2.2]. $\qquad\square$

As in [8], we are going to consider a suitable quadratic twist of $Z_{d,0}(q, p)$ whose $\mathbb{Q}$-rational points will correspond to $\mathbb{Q}$-curves completely defined over K, of degree d, without complex multiplication and with level structures at q and p corresponding to the curve $X_{0,\mathrm{ns}}^+(q, p)$ (i.e., $\mathbb{Q}$-curves satisfying the conditions of Proposition 1.8).

Define the homomorphism $\psi : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}_\mathbb{Q}(Z_{d,0}(q, p))$ by mapping σ, the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$, to w_d, the involution of $Z_{d,0}(q, p)$ induced by the Atkin–Lehner operator associated to $X_0(d)$. Let $Z_{d,0}^\psi(q, p)$ be a quadratic twist associated to ψ. By definition, $Z_{d,0}^\psi(q, p)$ is a curve defined over $\mathbb{Q}$ for which there exists a K-isomorphism $\varphi : Z_{d,0}(q, p)_{/K} \to Z_{d,0}^\psi(q, p)_{/K}$ such that $\varphi \circ w_d = {}^\sigma\varphi$. This isomorphism yields a bijection between the sets $Z_{d,0}^\psi(q, p)(\mathbb{Q})$ and $\{P \in Z_{d,0}(q, p)(K) : w_d P = {}^\sigma P\}$. By

Lemma [4.12], we conclude that a $\mathbb{Q}$-curve as in Proposition [1.8] gives rise to a $\mathbb{Q}$-point in $Z_{d,0}^{\psi}(q, p)$.

There is a natural degeneracy map $\delta : Z_{d,0}(q, p) \to X_{0,\mathrm{ns}}^{+}(q, p)$. Let $f : X_{0,\mathrm{ns}}^{+}(q, p) \to A$ stand for the morphism in [6, Lemma 8.2] (where, as in [6], A is the winding quotient of the Jacobian of $X_{0,\mathrm{ns}}^{+}(q, p)$). Note that this map is only defined over $\mathbb{Q}(\zeta_p)^{+}$. We define two morphisms $\gamma_1, \gamma_2 : Z_{d,0}(q, p) \to A$ by

$$\gamma_1 := f \circ \delta \quad \text{and} \quad \gamma_2 := f \circ \delta \circ w_d.$$

Moreover, we define

$$h_1 := \gamma_1 \circ \varphi^{-1} \quad \text{and} \quad h_2 : \gamma_2 \circ \varphi^{-1}.$$

These two maps are defined over $L := K(\zeta_p + \zeta_p^{-1})$. We finally set $h := h_1 + h_2$.

Denote by $\mathcal{O}_L$ the ring of integers of L and define $R := \mathcal{O}_L[1/6qp]$. Using the notation of Sect. [3], h can be extended to a morphism $Z_{d,0}^{\psi}(q, p)_{/R} \to A_{/R}$. By abuse of notation, we shall denote this morphism by h as well.

In what follows, the point at infinity of $Z_{d,0}^{\psi}(q, p)$ is, of course, defined to be the image of the point at infinity of $Z_{d,0}(q, p)$ via φ.

Lemma 4.13 *The morphism h is a formal immersion at $\infty_{/R}$.*

Proof The arguments of the proof are essentially the ones used in the proof of [8, Proposition 3.2]. For the convenience of the reader, we will present the proof here. We first note that it is enough to show that the morphism $\gamma := \gamma_1 + \gamma_2$ is a formal immersion at $\infty_{/R}$. Let λ be a prime ideal of R and let $\mathbb{F}_\lambda$ be the associated residue field. Writing $\mathrm{Cot}(A_{/\mathbb{F}_\lambda})$ for the cotangent space of $A_{/\mathbb{F}_\lambda}$ at 0, and $\mathrm{Cot}_\infty(Z_{d,0}(q, p)_{/\mathbb{F}_\lambda})$ for the cotangent space of $Z_{d,0}(q, p)_{/\mathbb{F}_\lambda}$ at $\infty_{/\mathbb{F}_\lambda}$, it is enough to show that the map

$$\gamma_{/\mathbb{F}_\lambda}^{*} : \mathrm{Cot}(A_{/\mathbb{F}_\lambda}) \to \mathrm{Cot}_\infty(Z_{d,0}(q, p)_{/\mathbb{F}_\lambda})$$

induced by γ is surjective.

Recall that, by definition, $\gamma_{1/\mathbb{F}_\lambda}$ factors as

$$Z_{d,0}(q, p)_{/\mathbb{F}_\lambda} \xrightarrow{\delta_{/\mathbb{F}_\lambda}} X_{0,\mathrm{ns}}^{+}(q, p)_{/\mathbb{F}_\lambda} \xrightarrow{f_{/\mathbb{F}_\lambda}} A_{/\mathbb{F}_\lambda},$$

while $\gamma_{2/\mathbb{F}_\lambda}$ factors as

$$Z_{d,0}(q, p)_{/\mathbb{F}_\lambda} \xrightarrow{(\delta \circ w_d)_{/\mathbb{F}_\lambda}} X_{0,\mathrm{ns}}^{+}(q, p)_{/\mathbb{F}_\lambda} \xrightarrow{f_{/\mathbb{F}_\lambda}} A_{/\mathbb{F}_\lambda}.$$

Since $(\delta \circ w_d)_{/\mathbb{F}_\lambda}$ is ramified at $\infty_{/\mathbb{F}_\lambda}$, we conclude that the map $\gamma_{2/\mathbb{F}_\lambda}^{*}$ induced on the cotangent spaces is 0. Hence,

$$\gamma_{/\mathbb{F}_\lambda}^{*} = \gamma_{1/\mathbb{F}_\lambda}^{*}.$$

On the other hand, $\delta_{/\mathbb{F}_\lambda}$ is unramified at $\infty_{/\mathbb{F}_\lambda}$. Moreover, the morphism $f : X_{0,\mathrm{ns}}^{+}(q, p) \to A$ has been proven to be a formal immersion at infinity in [6, Lemma 8.2] (once again, we remark that the arguments used in [6] hold when $q \in \{2, 3, 5, 7, 13\}$, even though this result is only stated for $q \in \{2, 3\}$). It follows that $\gamma_{1/\mathbb{F}_\lambda}^{*}$ surjects onto $\mathrm{Cot}_\infty(Z_{d,0}(q, p)_{/\mathbb{F}_\lambda})$, and, consequently, so does $\gamma_{/\mathbb{F}_\lambda}^{*}$. $\square$

Lemma 4.14 *Let P be a $\mathbb{Q}$-rational point in $Z_{d,0}^{\psi}(q, p)$. Then $h(P)$ is a torsion point of $A(\bar{\mathbb{Q}})$.*

Proof This argument was used in the proof of [6, Lemma 8.3]. Let $\tau \in G_{\mathbb{Q}}$. It is easy to check that $^\tau(h(P)) - h(P)$ is a cuspidal divisor. Therefore, by the theorem of Manin–Drinfeld, there exists a positive integer m such that

$$m(^\tau(h(P))) = mh(P).$$

This means that $mh(P)$ is defined over $\mathbb{Q}$. As $A(\mathbb{Q})$ is finite, we conclude that $mh(P)$ is torsion, and so is $h(P)$. □

Proof of Proposition 1.8 Note that if $q \geq 11$ is a prime different from 13, then [8, Proposition 3.2] yields that E has potentially good reduction at every prime of characteristic > 3. As the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$, Proposition 3.3 yields that E cannot have potentially multiplicative reduction at primes above 2 and 3 either. Therefore, E has potentially good reduction everywhere. In other words, the j-invariant of E lies in $\mathcal{O}_K$.

We are reduced to proving the cases where $q \in \{2, 3, 5, 7, 13\}$. As noted above, a $\mathbb{Q}$-curve as in the statement of the Proposition 1.8 gives rise to a $\mathbb{Q}$-rational point P in $Z_{d,0}^\psi(q, p)$. If λ is a non-archimedean prime of K such that $N_{K/\mathbb{Q}}(\lambda)^2 \not\equiv 1 \pmod{p}$, then Proposition 3.3 asserts that E has potentially good reduction at λ, as $p \geq 11$. Suppose that $N_{K/\mathbb{Q}}(\lambda)^2 \equiv 1 \pmod{p}$. Note that under this condition λ remains a prime in L. As $p \geq 11$, the prime λ does not divide 6. Suppose, for the sake of contradiction, that E has potentially multiplicative reduction at λ. Then the section of $Z_{/R}$ corresponding to P meets a cusp in the fibre above λ. By changing bases if needed, we may assume that this cusp is ∞. Now, we know that $h(P) \in \mathrm{Tors}(A(L))$. Moreover, the torsion subgroup of $A(L)$ injects, via reduction modulo λ, into $A(\mathbb{F}_\lambda)$. But $h(P)$ meets $h(\infty)$ in the special fibre above λ. Therefore, $h(P) = h(\infty)$. Since h is a formal immersion at $\infty_{/\mathbb{F}_\lambda}$, we conclude that $P = \infty$, which is absurd. □

Proof of Theorem 1.6 By Theorem 1.10, the prime q belongs to a finite list. For each one of these primes, we obtain a K-rational point in $X_0(d) \times_{X(1)} X_0(q)$, which is a modular curve with at least three cusps. By an argument due to Serre (see [17, Lemme 18]), we know that there exists a constant C_K', depending only on the number field K, such that, for $p > C_K'$, the image of $\mathbb{P}\bar{\rho}_{E,p}$ is not exceptional. By Theorem 1.10, there is another constant $C_{K,d}''$ such that, for $p > C_{K,d}''$, it is also not contained in a Borel subgroup. Therefore, if $p > C_{K,d}''$, the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in the normaliser of a Cartan subgroup (split or non-split). If it is contained in the normaliser of a split Cartan subgroup, then we can use the result of Le Fourn that we stated as Proposittion 1.9 to conclude that $j(E) \in \mathcal{O}_K$. In the case where the image of $\mathbb{P}\bar{\rho}_{E,p}$ is contained in the normaliser of a non-split Cartan, we use Proposition 1.8 that we have just proven in order to, once again, conclude that $j(E) \in \mathcal{O}_K$. In any case, there is a constant $C_{K,d}''$ such that, if p is a prime $> C_{K,d}''$, then either $\mathbb{P}\bar{\rho}_{E,p}$ is surjective, or $j(E)$ is integral. As the modular curve $X_0(d) \times_{X(1)} X_0(q)$ has at least three cusps, Siegel's theorem asserts that there are only finitely many points in $X_0(d) \times_{X(1)} X_0(q)(K)$ whose j-invariants are in $\mathcal{O}_K$. As q is in a finite list of primes, we obtain a finite list of j-invariants of $\mathbb{Q}$-curves satisfying the conditions of the theorem and for which there exists a prime $p > C_{K,d}''$ with $\bar{\rho}_{E,p}$ non-surjective. Noting that surjectiveness only depends on the j-invariant if $j(E) \neq 0, 1728$ (as any two elliptic curves with the same j-invariant are quadratic twists of each other as long as $j \neq 0, 1728$), we can now use the theorem of Serre that we presented in the introduction as Theorem 1.1 for each one of these finitely many j-invariants, and we obtain the result. □

4.3 The normaliser of a split Cartan case

The proof of Theorem 1.7 is a simple exercise using Le Fourn's Proposition 1.9.

Proof of Theorem 1.7 We may assume that $d \geq 2$, as the case $d = 1$ is precisely the one treated by Theorem 1.4. The aim is to show that, for each d as in the statement of the theorem, there are only finitely many points in $X_0(d)(K)$ with j-invariant in $\mathcal{O}_K$. The result follows, as, by the same arguments employed in the proof of Theorem 1.6, there exists a constant $C''_{K,d}$ (keeping up with the notation used in the proof of Theorem 1.6) such that, if p is a prime $> C''_{K,d}$ and E/K is a curve satisfying the conditions of the theorem, then either $\mathbb{P}\bar{\rho}_{E,p}$ is surjective, or $j(E) \in \mathcal{O}_K$, and then we only have to use Serre's Theorem 1.1 for each of the finitely many points of $X_0(d)(K)$ in the same way we used it in the proof of Theorem 1.6.

If the genus of $X_0(d)$ is ≥ 2, then a theorem of Faltings asserts that the set $X_0(d)(K)$ is finite, and we are done. If the genus of $X_0(d)$ is 1, then the finiteness of the number of points in $X_0(d)(K)$ with integral j-invariant comes from a theorem of Siegel. Finally, if the genus $X_0(d)$ is 0, then, as we require d to be square-free and not in the set $\{2, 3, 5, 7, 13\}$, we conclude that d is a product of two distinct primes. Therefore, $X_0(d)$ has at least three cusps, and we can use Siegel's theorem in order to conclude the finiteness of the number of points in $X_0(d)(K)$ with integral j-invariant. □

References

1. Balakrishnan, J.S., Dogra, N., Steffen Müller, J., Tuitman, J., Vonk, J.: Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13. (2017). arXiv:1711.05846
2. Bilu, Y., Parent, P.: Serre's uniformity problem in the split Cartan case. Ann. of Math. **173**(1), 569–584 ((2) 2011,)
3. Bilu, Y., Parent, P., Rebolledo, M.: Rational points on $X_0^+(p^r)$. Ann. Inst. Fourier (Grenoble) **63**(3), 957–984 (2013)
4. Bourbaki, N.: Éléments de Mathématique. Algèbre. Chapitres 1 à 3. Hermann, Paris (1970)
5. Chen, I.: The Jacobian of Modular Curves Associated to Cartan Subgroups. PhD thesis, University of Oxford (1996)
6. Darmon, H., Merel, L.: Winding quotients and some variants of Fermat's last theorem. J. Reine Angew. Math. **490**, 81–100 (1997)
7. Ellenberg, J.S.: $\mathbb{Q}$-curves and Galois representations. In: Cremona, J., Lario, J.C., Quer, J., Ribet, K. (eds.) Modular curves and abelian varieties, volume 224 of Progr. Math., pp. 93–103. Birkhäuser, Basel (2004)
8. Ellenberg, J.S.: Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. Amer. J. Math. **126**(4), 763–787 (2004)
9. Le Fourn, S.: Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves. Math. Ann. **365**(1–2), 173–214 (2016)
10. Lemos, P.: Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies. Trans. Amer. Math. Soc., electronically published on March 21, (2018). https://doi.org/10.1090/tran/7198 (**to appear in print**)

11. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. **47**, 33–186 (1977)
12. Mazur, B.: Rational isogenies of prime degree (with an appendix by D. Goldfeld). Invent. Math. **44**(2), 129–162 (1978)
13. Momose, F.: Rational points on the modular curves $X_{\text{split}}(p)$. Compositio Math. **52**(1), 115–137 (1984)
14. Rebolledo, M., Wuthrich, C.: A moduli interpretation for the non-split Cartan modular curve. ArXiv e-prints, Feb. (2014)
15. Ribet, K.A.: Abelian varieties over **Q** and modular forms. In: Cremona, J., Lario, J.C., Quer, J., Ribet, K. (eds.) Modular Curves and Abelian Varieties, volume 224 of Progr. Math., pp. 241–261. Birkhäuser, Basel, (2004)
16. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
17. Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. Inst. Hautes Études Sci. Publ. Math. **54**, 323–401 (1981)
18. Sutherland, A.V.: Computing images of Galois representations attached to elliptic curves. Forum Math. Sigma **4: e4**, 79 (2016)
19. The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, (2018). Accessed 3 Feb 2018