Strongly modular models of ℚ-curves

Bruin, P.J.; Ferraguti, A.

International Journal of Number Theory
Vol. 15, No. 3 (2019) 505–526
© World Scientific Publishing Company
DOI: 10.1142/S179304211950026X

World Scientific
www.worldscientific.com

Strongly modular models of $\mathbb{Q}$-curves

Peter Bruin

Mathematisch Instituut
Universiteit Leiden, Postbus 9512
2300 RA Leiden, Netherlands
P.J.Bruin@math.leidenuniv.nl

Andrea Ferraguti

DPMMS, University of Cambridge
Wilberforce Road Cambridge, CB3 0WB, UK
af612@dpmms.cam.ac.uk

Received 3 July 2018
Revised 6 September 2018
Accepted 8 October 2018
Published 16 November 2018

Let E be a $\mathbb{Q}$-curve without complex multiplication. We address the problem of deciding whether E is geometrically isomorphic to a strongly modular $\mathbb{Q}$-curve. We show that the question has a positive answer if and only if E has a model that is completely defined over an abelian number field. Next, if E is completely defined over a quadratic or biquadratic number field L, we classify all strongly modular twists of E over L in terms of the arithmetic of L. Moreover, we show how to determine which of these twists come, up to isogeny, from a subfield of L.

Keywords: $\mathbb{Q}$-curves; quadratic twists; strong modularity; Galois cohomology.

Mathematics Subject Classification 2010: 11G05, 11G40, 11R34

1. Introduction

In the study of elliptic curves over number fields, the concept of modularity plays a central role. If E is an elliptic curve over $\mathbb{Q}$ of conductor N, the modularity theorem [1, 21, 22] states that there exists a nontrivial map of algebraic curves $X_0(N) \to E$, called a *modular parametrization*, where $X_0(N)$ is the compact modular curve for $\Gamma_0(N)$. This fact has several important consequences, one of which is the fact that the L-function of E coincides with the L-function of a weight 2 newform of level $\Gamma_0(N)$. This in turn implies for example that the L-function has an analytic continuation to $\mathbb{C}$.

It is natural to ask for a generalization of this fact to elliptic curves over $\overline{\mathbb{Q}}$. Shimura proved [19] that elliptic curves over $\overline{\mathbb{Q}}$ with complex multiplication (CM) admit a modular parametrization from the compact modular curve $X_1(N)$, for an appropriate positive integer N. For curves without CM, the situation was more complicated. In 1992, Ribet [16] proved that under Serre's modularity conjecture, an elliptic curve $E/\overline{\mathbb{Q}}$ without CM admits a modular parametrization from $X_1(N)$ if and only if E is a $\mathbb{Q}$-curve, i.e. it is $\overline{\mathbb{Q}}$-isogenous to all of its Galois conjugates. The subsequent proof, in 2009, of the aforementioned conjecture by Khare and Wintenberger [9] completed the characterization of this class of elliptic curves. Note that since there exists a natural map $X_1(N) \to X_0(N)$, the modularity theorem already shows that all elliptic curves over $\mathbb{Q}$ belong to this class. From now on, all $\mathbb{Q}$-curves will be implicitly assumed to be without CM.

Contrary to what happens for elliptic curves over $\mathbb{Q}$, the L-function $L(E/K, s)$ of a $\mathbb{Q}$-curve E over a number field $K \neq \mathbb{Q}$ is never the L-function of a newform. However, $L(E/K, s)$ may be a *product* of L-functions of newforms. In fact, the proof of Ribet's theorem [16] implies that abelian varieties of GL_2-type are isogenous to products of abelian varieties attached to newforms of weight 2. For example, if E is a $\mathbb{Q}$-curve over a quadratic field K that is K-isogenous to its Galois conjugate, then its restriction of scalars to $\mathbb{Q}$ is an abelian surface of GL_2-type. Since E and its restriction of scalars have the same L-function [11], it follows that $L(E/K, s)$ is a product of two L-functions of newforms of weight 2. This motivates the following definition [7]: a $\mathbb{Q}$-curve is said to be *strongly modular* if its L-function is a product of L-functions of newforms of weight 2.

Guitart and Quer [6, 7] gave necessary and sufficient conditions for a $\mathbb{Q}$-curve (and, more in general, for a building block) over a number field K to be strongly modular: this happens if and only if $K/\mathbb{Q}$ is an abelian extension, E is *completely defined* over K (i.e. all isogenies between conjugates of E are defined over K) and the 2-cocycle attached to E (cf. Sec. 3) is symmetric. It is easy to deduce from the results of [3, 5, 11] that every $\mathbb{Q}$-curve is geometrically isogenous to a strongly modular one. In this paper, we address the following question: what are necessary and sufficient conditions for a $\mathbb{Q}$-curve to be geometrically *isomorphic* to a strongly modular one? We will refer to this property as "to admit a strongly modular model". Our main result is the following.

Theorem 1.1. *A $\mathbb{Q}$-curve admits a strongly modular model if and only if it has a model completely defined over an abelian number field K.*

The paper is structured as follows. In Sec. 2, we review some basic facts about group cohomology and group extensions that will be needed later. In Sec. 3, we recall the construction of two invariants attached to a $\mathbb{Q}$-curve E over a Galois extension $K/\mathbb{Q}$ with Galois group G. Both invariants depend only on the K-isogeny class of E. The first one is a 1-cocycle for G with values in $K^\times/(K^\times)^2$ yielding information about the smallest field over which the curve is completely defined, which we call the *minimal field of complete definition* (Definition 3.2). The second one is a 2-cocycle for G with values in $(\mathrm{End}(E) \otimes \mathbb{Q})^\times \simeq \mathbb{Q}^\times$ carrying information about the strong modularity of E and the field of definition of E up to isogeny (Theorem 5.2

and Proposition 5.3). Section 4 is dedicated to the proof of our main theorem. The proof relies on two preliminary results. The first one is [7, Lemma 6.1], which characterizes strongly modular twists E^γ of a $\mathbb{Q}$-curve E over a number field K in terms of the arithmetic of $K(\sqrt{\gamma})$. The second result is that the 2-torsion of the Brauer group of $\mathbb{Q}$ consists of inflations of symmetric 2-cocycles for $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ with values in $\{\pm 1\}$. This essentially allows us to "twist" the 2-cocycle of a $\mathbb{Q}$-curve over an abelian number field into a symmetric one. Finally, in Sec. 5, we study in detail an instance of the problem above: Theorem 1.1 is not effective in general, but what about $\mathbb{Q}$-curves E over a quadratic field K? We prove that every such curve has a model completely defined over a biquadratic, and hence abelian, number field L containing K; it therefore admits a strongly modular model. We construct explicitly all strongly modular models of E over L (Theorem 5.9), the existence of which is regulated only by the arithmetic of L. We explain how to determine those models that descend to subfields of L, up to isogeny. As a corollary, we show how to construct all strongly modular twists of E over K. We end the section with several examples exhibiting different behaviors.

Notation and Conventions

When A is an abelian variety over a field K and F is an extension of K, the $\mathbb{Q}$-algebra of the F-endomorphisms of A is denoted by $\mathrm{End}^0_F(A)$.

If G and A are abelian groups, we write $\mathrm{Ext}^1(G, A)$ for the group of abelian extensions of G by A.

If F/K is a Galois extension of fields and A is a $\mathrm{Gal}(F/K)$-module, we denote by $\mathrm{H}^i(F/K, A)$ the ith cohomology group of A with coefficients in $\mathrm{Gal}(F/K)$. Analogously, we denote by $\mathrm{Z}^i(F/K, A)$ the group of i-cocycles. If $c \in \mathrm{Z}^i(F/K, A)$, its cohomology class is denoted by $[c]$. If G is a group and A is a G-module, we denote the action of G on A using left superscripts: for $\sigma \in G$ and $a \in A$, the image of a under σ is written as ${}^\sigma a$. We denote by A^G the submodule of G-invariants.

All profinite groups that we mention throughout the paper are endowed with their profinite topology; in particular, finite groups are discrete.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, and write $\mathbb{Q}^{\mathrm{ab}}$ for the maximal abelian extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$. The absolute Galois group of $\mathbb{Q}$ is denoted by $G_{\mathbb{Q}}$ and the Galois group of $\mathbb{Q}^{\mathrm{ab}}$ over $\mathbb{Q}$ is denoted by $G^{\mathrm{ab}}_{\mathbb{Q}}$.

If K is a field, we denote by $\mathrm{Br}(K)$ the Brauer group of K, defined as $\mathrm{H}^2(\overline{K}/K, \overline{K}^\times)$.

For a unitary ring R, we denote by $R^\times$ the group of units.

2. Group Cohomology, Group Extensions and Embedding Problems

In this section, we collect some standard facts and definitions from the theory of group cohomology that we will use later in the paper. For a complete treatment of profinite group cohomology, see for example [12] or [18].

Let G be a profinite group, let N be a normal closed subgroup of G, and let A be a G-module. For every $i \geq 1$, the *restriction map* $\mathrm{Res} : \mathrm{H}^i(G, A) \to \mathrm{H}^i(N, A)$ is the natural map induced by the inclusion $N \subseteq G$, and the *inflation map* $\mathrm{Inf} : \mathrm{H}^i(G/N, A^N) \to \mathrm{H}^i(G, A)$ is the natural map induced by the projection $G \to G/N$.

The group $\mathrm{H}^1(N, A)$ is endowed with an action of G/N defined in the following way: for $g \in G$ and $[c] \in \mathrm{H}^1(N, A)$, let ${}^g[c]$ be the cohomology class represented by the cocycle $h \mapsto {}^gc(g^{-1}hg)$ for all $h \in N$. It is easy to check that N acts as the identity, so that the action factors through the quotient G/N.

Theorem 2.1 ([12, Proposition I.1.6.5]). *There is a natural map*

$$\mathrm{trg} : \mathrm{H}^1(N, A)^{G/N} \to \mathrm{H}^2(G/N, A^N)$$

fitting into an exact sequence

$$\begin{aligned} 0 \ \to \ \mathrm{H}^1(G/N, A^N) &\xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(N, A)^{G/N} \xrightarrow{\mathrm{trg}} \\ &\xrightarrow{\mathrm{trg}} \mathrm{H}^2(G/N, A^N) \xrightarrow{\mathrm{Inf}} \mathrm{H}^2(G, A). \end{aligned}$$

The map trg in Theorem 2.1 is called the *transgression map*, and the exact sequence is called the *inflation-restriction sequence*.

Definition 2.2. Let G be a profinite abelian group and let A be an abelian group regarded as a G-module with trivial action. We say that a cocycle $c \in \mathrm{Z}^2(G, A)$ is *symmetric* if $c(\sigma, \tau) = c(\tau, \sigma)$ for all $\sigma, \tau \in G$.

Note that the property of c being symmetric only depends on the cohomology class of c, because coboundaries are symmetric by the commutativity of G. Moreover, the product of two symmetric cocycles is clearly a symmetric cocycle. Thus, the cohomology classes in $\mathrm{H}^2(G, A)$ represented by a symmetric cocycle form a subgroup of $\mathrm{H}^2(G, A)$, which we denote by $\mathrm{H}^2_{\mathrm{s}}(G, A)$.

Lemma 2.3. *Let G be a finite abelian group, and let A be an abelian group equipped with the trivial G-action. There is a canonical isomorphism of abelian groups*

$$\mathrm{Ext}^1(G, A) \xrightarrow{\sim} \mathrm{H}^2_{\mathrm{s}}(G, A).$$

Proof. There is a well-known isomorphism between $\mathrm{H}^2(G, A)$ and the group of central extensions of G by A; see for example [12, Theorem 1.2.4]. Looking at the definition of this isomorphism, one sees that a cocycle is symmetric if and only if in the associated group extension $0 \to A \to B \to G \to 1$ the group B is abelian. □

Lemma 2.4. *Let G be a finite abelian group, let A be an abelian group equipped with the trivial G-action, and let p be a prime such that $pG = 0$. Then there is a* (*non-canonical*) *isomorphism*

$$\mathrm{Ext}^1(G, A) \simeq \mathrm{Hom}(G, A/pA).$$

Proof. Using the properties of Hom and Ext (see for example [20]), we reduce to the case $G = \mathbb{Z}/p\mathbb{Z}$. From the long exact sequence obtained by applying the Ext functor to

$$0 \to \mathbb{Z} \xrightarrow{p} \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

and the fact that $\mathrm{Ext}^1(\mathbb{Z}, A) = 0$, we get an isomorphism $\mathrm{Ext}^1(\mathbb{Z}/p\mathbb{Z}, A) \simeq A/pA$. The claim follows using the canonical isomorphism $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, A/pA) \simeq A/pA$. □

Theorem 2.5 (Künneth formula [8]). *Let G_1, G_2 be profinite abelian groups acting trivially on a discrete abelian group A. Then there is a canonical isomorphism*

$$\mathrm{H}^2(G_1 \times G_2, A) \simeq \mathrm{H}^2(G_1, A) \oplus \mathrm{H}^2(G_2, A) \oplus \mathrm{Hom}(G_1 \otimes G_2, A).$$

Definition 2.6. Let L/K be a Galois extension of fields with Galois group G. Consider an extension

$$1 \to H \to \widetilde{G} \xrightarrow{\pi} G \to 1 \tag{2.1}$$

of profinite groups. A *solution to the embedding problem* relative to the extension L/K and the group extension (2.1) consists of a Galois extension M/K with $L \subseteq M$ and an isomorphism $\iota : \mathrm{Gal}(M/K) \xrightarrow{\sim} \widetilde{G}$ such that $\pi \circ \iota$ equals the canonical map $\mathrm{Gal}(M/K) \to G$.

It is not hard to see that the solvability of the embedding problem given by the extension (2.1) depends only on the equivalence class of the extension. To conclude this section, we recall a result from [10] that will be useful later.

Lemma 2.7 ([10, pp. 826–827]). *Let L/K be a Galois extension of fields of characteristic different from 2 with Galois group G. Let $1 \to \{\pm 1\} \to \widetilde{G} \to G \to 1$ be an extension of G by $\{\pm 1\}$, and let $c \in \mathrm{H}^2(G, \{\pm 1\})$ be the corresponding cohomology class. Then the embedding problem relative to L/K and the above extension has a solution if and only if c is in the kernel of the natural map*

$$\varphi_L : \mathrm{H}^2(G, \{\pm 1\}) \to \mathrm{H}^2(G, L^\times).$$

3. Strongly Modular Elliptic Curves

The goal of this section is to introduce the main objects of the paper, namely $\mathbb{Q}$-curves and strongly modular $\mathbb{Q}$-curves, and recall some of their basic properties. For more details, see [4, 7, 14, 15].

Definition 3.1. Let K be a Galois extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$. An elliptic curve E/K is called a $\mathbb{Q}$-*curve* if for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ there exists a $\overline{\mathbb{Q}}$-isogeny $\mu_\sigma : {}^\sigma E \to E$. We say that E is *completely defined* over K if in addition all $\overline{\mathbb{Q}}$-isogenies between the ${}^\sigma E$ are defined over K.

From now on, all our $\mathbb{Q}$-curves will be without CM.

Let K be a Galois extension of $\mathbb{Q}$ and let E be a $\mathbb{Q}$-curve over K. We recall the definition of two cohomology classes

$$[\lambda] \in \mathrm{H}^1(K/\mathbb{Q}, K^\times/(K^\times)^2), \quad [\xi_K(E)] \in \mathrm{H}^2(K/\mathbb{Q}, \mathbb{Q}^\times)$$

attached to E (the second under the assumption that E is completely defined over K) that encode arithmetic properties of the curve; see also [13] or [14].

Let $G := \mathrm{Gal}(K/\mathbb{Q})$. For every $\sigma \in G$, we choose a $\overline{\mathbb{Q}}$-isogeny $\mu_\sigma : {}^\sigma E \to E$.

By the argument described in [14, p. 4], if E is given by an equation of the form $y^2 = x^3 + Ax + B$ with $A, B \in K$, then for all $\sigma \in G$ and all isogenies $\mu_\sigma : {}^\sigma E \to E$, we can write

$$\mu_\sigma(x, y) = \left(F(x), \frac{1}{\lambda_\sigma} yF'(x)\right)$$

for some $F(x) \in K(x)$ and $\lambda_\sigma \in \overline{\mathbb{Q}}^\times$ such that $\lambda_\sigma^2 \in K^\times$. Because E has no CM, for all $\sigma, \tau \in G$ there exists $m(\sigma, \tau) \in \mathbb{Q}^\times$ satisfying

$$\lambda_\sigma {}^\sigma\lambda_\tau = m(\sigma, \tau)\lambda_{\sigma\tau}. \tag{3.1}$$

This shows that the map

$$\begin{aligned} \lambda : G &\to K^\times/(K^\times)^2 \\ \sigma &\mapsto \lambda_\sigma^2 \end{aligned}$$

is a 1-cocycle for the natural Galois action of G on $K^\times/(K^\times)^2$. A calculation shows that the cohomology class $[\lambda]$ of λ depends only on the K-isogeny class of E.

Definition 3.2. We call the field $K(\lambda_\sigma : \sigma \in G)$ the *minimal field of complete definition* for E/K.

Proposition 3.3. *Let L be the minimal field of complete definition for E. Then*:

(i) *L is Galois over $\mathbb{Q}$*;
(ii) *E_L is completely defined over L*;
(iii) *L/K is a multiquadratic extension*;
(iv) *if M is a Galois extension of $\mathbb{Q}$ containing K and E_M is completely defined over M, then $L \subseteq M$.*

Proof. We observe that if K/F is any Galois extension of subfields of $\overline{\mathbb{Q}}$ and $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{Q}}$, then the normal closure of $K(\lambda_1, \ldots, \lambda_n)$ over F equals $K({}^\sigma\lambda_i : i \in \{1, \ldots, n\}, \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/F))$. Point (i) follows from this observation together with the identity (3.1). Points (ii), (iii) and (iv) are clear by construction. □

To construct the other cohomology class attached to E, suppose that E is completely defined over K, so that every μ_σ is itself defined over K. The map

$$\begin{aligned} \xi_K(E) : G \times G &\to (\mathrm{End}_K^0(E))^\times \simeq \mathbb{Q}^\times \\ (\sigma, \tau) &\longmapsto \mu_\sigma {}^\sigma\mu_\tau \mu_{\sigma\tau}^{-1} \end{aligned}$$

is a 2-cocycle for the trivial action of G on $\mathbb{Q}^\times$. With a small abuse of notation, we will often talk about "the" 2-cocycle attached to E, without mentioning explicitly the system of isogenies giving rise to it. A direct calculation shows that the cohomology class $[\xi_K(E)]$ of $\xi_K(E)$ depends only on the K-isogeny class of E. When $K = \overline{\mathbb{Q}}$, the 2-cocycle attached to E will be denoted simply by $\xi(E)$. Note that the image of $[\xi_K(E)]$ under the inflation map $\mathrm{H}^2(G, \mathbb{Q}^\times) \to \mathrm{H}^2(G_{\mathbb{Q}}, \mathbb{Q}^\times)$ equals $[\xi(E)]$.

The decomposition $\mathbb{Q}^\times \simeq \mathbb{Q}_+^\times \times \{\pm 1\}$, where $\mathbb{Q}_+^\times$ is the multiplicative group of positive rational numbers, yields a decomposition of ξ_K in a 2-cocycle $\xi_K^{\deg} \in \mathrm{Z}^2(G, \mathbb{Q}_+^\times)$ and a 2-cocycle $\xi_K^{\pm} \in \mathrm{Z}^2(G, \{\pm 1\})$. Similarly, the isomorphism

$$\mathrm{H}^2(G, \mathbb{Q}^\times) \simeq \mathrm{H}^2(G, \mathbb{Q}_+^\times) \times \mathrm{H}^2(G, \{\pm 1\})$$

yields a decomposition of $[\xi_K]$ into a *degree component* $[\xi_K^{\deg}] \in \mathrm{H}^2(G, \mathbb{Q}_+^\times)$ and a *sign component* $[\xi_K^{\pm}] \in \mathrm{H}^2(G, \{\pm 1\})$.

Definition 3.4. A $\mathbb{Q}$-curve E over a number field K is *strongly modular* if its L-function $L(E/K, s)$ can be written as a product of L-functions attached to holomorphic newforms of weight 2 for congruence subgroups of the form $\Gamma_1(N)$.

The newforms in such a product are unique up to ordering [2, Proposition 3.4]. The modularity theorem [1] implies that all elliptic curves over $\mathbb{Q}$ are strongly modular; this is not true for general $\mathbb{Q}$-curves.

Theorem 3.5 ([6, Theorem 2.3]). *Let E be an elliptic curve without CM over a number field K. Then E is strongly modular over K if and only if the following three conditions hold*:

(i) *K is abelian over $\mathbb{Q}$*;
(ii) *E is completely defined over K*;
(iii) *the 2-cocycle ξ_K attached to E is symmetric, i.e. $[\xi_K] \in \mathrm{H}^2_{\mathrm{s}}(\mathrm{Gal}(K/\mathbb{Q}), \mathbb{Q}^\times)$.*

Remark 3.6. A cohomology class in $\mathrm{H}^2(K/\mathbb{Q}, \mathbb{Q}^\times)$ is symmetric if and only if both its sign component and its degree component are symmetric. The degree component of $[\xi_K]$ is always symmetric, since for $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$, the fact that $\xi_K(\sigma, \tau) = \mu_\sigma {}^\sigma\mu_\tau \mu_{\sigma\tau}^{-1}$ implies $\xi_K(\sigma, \tau)^2 = \deg(\mu_\sigma) \cdot \deg(\mu_\tau) \cdot \deg(\mu_{\sigma\tau})^{-1}$, and since $K/\mathbb{Q}$ is an abelian extension, this implies $\xi_K(\sigma, \tau)^2 = \xi_K(\tau, \sigma)^2$. Therefore, condition (iii) above is equivalent to

(iii′) $[\xi_K^{\pm}] \in \mathrm{H}^2_{\mathrm{s}}(K/\mathbb{Q}, \{\pm 1\})$.

4. Strongly Modular $\mathbb{Q}$-Curves Up to Isomorphism

Every $\mathbb{Q}$-curve E is geometrically isogenous to a strongly modular one. In fact, it is proved in [3] that there exists a newform f such that the attached abelian variety A_f admits a nontrivial morphism $(A_f)_{\overline{\mathbb{Q}}} \to E$. If L is the splitting field of f, it is also proved in [3] that A_f is isogenous over L to E'^n for some positive integer n, where E' is a $\mathbb{Q}$-curve over L. Note that E is geometrically isogenous to E' by the uniqueness of the decomposition up to isogeny. By [5, Proposition 2], the restriction of scalars $\operatorname{Res}_{L/\mathbb{Q}}(E')$ is isogenous to a product of abelian varieties of the form A_g for some newform g. It follows that E'/L is strongly modular, because the L-function of E'/L coincides with the L-function of $\operatorname{Res}_{L/\mathbb{Q}}(E')$; see [11].

Therefore, it is natural to ask how strong modularity behaves with respect to geometric *isomorphisms*, rather than isogenies. It turns out that this is a more rigid property. In fact, we will prove the following theorem.

Theorem 4.1. *A $\mathbb{Q}$-curve $E/\overline{\mathbb{Q}}$ has a strongly modular model over a number field if and only if there exist an abelian number field K and a model of E completely defined over K.*

Compared to Theorem 3.5, the above result states that if one considers strong modularity up to geometric isomorphism, then the symmetry of the cocycle attached to the curve is redundant: if a $\mathbb{Q}$-curve is completely defined over an abelian number field, then there exists an appropriate model of the curve whose 2-cocycle is symmetric.

Let us rephrase the theorem above in cohomological terms. Let E be a $\mathbb{Q}$-curve over a Galois number field K with Galois group G, and let $\lambda \in \mathrm{Z}^1(G, K^\times/(K^\times)^2)$ be its associated 1-cocycle. A simple computation shows that for all $\gamma \in K^\times$, the cocycle attached to the twisted curve E^γ is given by $\lambda^\gamma(\sigma) := \lambda(\sigma) \cdot \frac{{}^\sigma\gamma}{\gamma}$ for every $\sigma \in G$, and is thus cohomologous to λ. Now, let L be an extension of K that is abelian over $\mathbb{Q}$, and let

$$\psi_L : \mathrm{H}^1(K/\mathbb{Q}, K^\times/(K^\times)^2) \to \mathrm{H}^1(L/\mathbb{Q}, L^\times/(L^\times)^2)$$

be the composition of the inflation map with the map induced by the natural morphism $K^\times/(K^\times)^2 \to L^\times/(L^\times)^2$. Proposition 3.3 implies that E has a model completely defined over L if and only if $\psi_L([\lambda])$ is trivial. It follows that Theorem 4.1 can be stated in the following way: if E is a $\mathbb{Q}$-curve over $K = \mathbb{Q}(j(E))$, then E has a strongly modular model if and only if K is abelian and $[\lambda]$ belongs to the kernel of the map

$$\mathrm{H}^1(K/\mathbb{Q}, K^\times/(K^\times)^2) \to \mathrm{H}^1(G_{\mathbb{Q}}^{\mathrm{ab}}, {\mathbb{Q}^{\mathrm{ab}}}^\times/({\mathbb{Q}^{\mathrm{ab}}}^\times)^2).$$

Example 4.2. Consider the elliptic curve $E' : y^2 = x^3 + x + 1$ over $\mathbb{Q}$. Let K be the non-Galois number field $\mathbb{Q}(\alpha)$, where α is a root of x^3+x+1. The base-changed curve E'_K has a nontrivial, rational 2-torsion point, namely $P = (\alpha, 0)$. Now, let φ be the isogeny with kernel $\{O, P\}$ and let $E := E'_K/\ker\varphi$. A Weierstrass equation for E is

$$E : y^2 = x^3 - (4 + 15\alpha^2)x + 22 + 14\alpha.$$

One can check that

$$j(E) = \frac{9580464 + 51659856\alpha + 72060192\alpha^2}{961} \notin \mathcal{O}_K,$$

so $\mathbb{Q}(j(E)) = K$ and E has no CM. Moreover, E is a $\mathbb{Q}$-curve: if L is the Galois closure of K, then E_L is L-isogenous to all its Galois conjugates, since by construction all of them are L-isogenous to E'_L. Thus, E is a $\mathbb{Q}$-curve that does not have a strongly modular model.

In order to prove Theorem 4.1, we need two preliminary results. The first one is proved in [7] and characterizes the twists of a $\mathbb{Q}$-curve defined over a Galois number field K that are strongly modular.

Lemma 4.3 ([7, Lemma 6.1]). *Let E be a $\mathbb{Q}$-curve completely defined over a Galois number field K. Let $\gamma \in K^\times$, and let E^γ be the twisted curve. Let ξ_K and ξ_K^γ be the 2-cocycles attached to E and E^γ, respectively. Then E^γ is completely defined over K if and only if the field $K(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$. In this case, the cohomology classes $[\xi_K]$ and $[\xi_K^\gamma]$ in $\mathrm{H}^2(K/\mathbb{Q}, \mathbb{Q}^\times)$ differ by the cohomology class in $\mathrm{H}^2(K/\mathbb{Q}, \{\pm 1\})$ attached to the exact sequence*

$$1 \to \mathrm{Gal}(K(\sqrt{\gamma})/K) \simeq \{\pm 1\} \to \mathrm{Gal}(K(\sqrt{\gamma})/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 1.$$

In particular, twisting by γ affects only the sign component of $[\xi_K]$ and not the degree component.

The second preliminary result shows that the 2-torsion of the Brauer group of $\mathbb{Q}$ is generated by cocycles inflated from certain symmetric ones.

Proposition 4.4. *The following hold*:

(i) *There is a canonical isomorphism $\bigoplus_{p\,\mathrm{prime}} \{\pm 1\} \xrightarrow{\sim} \mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$.*
(ii) *The inflation map $\mathrm{Inf} : \mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{H}^2(G_{\mathbb{Q}}, \{\pm 1\}) = \mathrm{Br}(\mathbb{Q})[2]$ is an isomorphism.*

Proof. To prove (i), recall that $G_{\mathbb{Q}}^{\mathrm{ab}}$ is canonically isomorphic to $\widehat{\mathbb{Z}}^\times$. By Lemma 2.3, we have a canonical isomorphism

$$\varinjlim_n \mathrm{Ext}^1((\mathbb{Z}/n\mathbb{Z})^\times, \{\pm 1\}) \xrightarrow{\sim} \varinjlim_n \mathrm{H}^2_{\mathrm{s}}((\mathbb{Z}/n\mathbb{Z})^\times, \{\pm 1\}) = \mathrm{H}^2_{\mathrm{s}}(\widehat{\mathbb{Z}}^\times, \{\pm 1\}).$$

Furthermore, we can rewrite the left-hand side using the canonical isomorphism

$$\bigoplus_{p\,\mathrm{prime}} \varinjlim_r \mathrm{Ext}^1((\mathbb{Z}/p^r\mathbb{Z})^\times, \{\pm 1\}) \xrightarrow{\sim} \varinjlim_n \mathrm{Ext}^1((\mathbb{Z}/n\mathbb{Z})^\times, \{\pm 1\}).$$

It therefore suffices to prove that for every prime number p, there exists a (unique) isomorphism

$$\{\pm 1\} \xrightarrow{\sim} \varinjlim_r \mathrm{Ext}^1((\mathbb{Z}/p^r\mathbb{Z})^\times, \{\pm 1\}).$$

For odd p, all groups $\mathrm{Ext}^1((\mathbb{Z}/p^r\mathbb{Z})^\times, \{\pm 1\})$, and also their direct limit, are canonically isomorphic to $\mathrm{Ext}^1((\mathbb{Z}/p\mathbb{Z})^\times, \{\pm 1\})$, which has order 2 because $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of even order. For $p = 2$, we recall that there are isomorphisms

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/4\mathbb{Z})^\times \times \mathbb{Z}/2^{r-2}\mathbb{Z} \quad \text{for all } r \geq 2$$

that are compatible in such a way that we obtain an isomorphism

$$\mathrm{Ext}^1((\mathbb{Z}/4\mathbb{Z})^\times, \{\pm 1\}) \times \varinjlim_r \mathrm{Ext}^1(\mathbb{Z}/2^r\mathbb{Z}, \{\pm 1\}) \xrightarrow{\sim} \varinjlim_r \mathrm{Ext}^1((\mathbb{Z}/2^r\mathbb{Z})^\times, \{\pm 1\}).$$

The group $\mathrm{Ext}^1((\mathbb{Z}/4\mathbb{Z})^\times, \{\pm 1\})$ has order 2, and it is well known that for all $r \geq 1$, the groups $\mathrm{Ext}^1(\mathbb{Z}/2^r\mathbb{Z}, \{\pm 1\})$ have order 2 and the maps $\mathrm{Ext}^1(\mathbb{Z}/2^r\mathbb{Z}, \{\pm 1\}) \to \mathrm{Ext}^1(\mathbb{Z}/2^{r+1}\mathbb{Z}, \{\pm 1\})$ are trivial. This implies the claim.

To prove (ii), consider the exact sequence

$$1 \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}) \to G_{\mathbb{Q}} \to G_{\mathbb{Q}}^{\mathrm{ab}} \to 1.$$

The inflation-restriction sequences obtained from the two $G_{\mathbb{Q}}$-modules $\{\pm 1\}$ and $\overline{\mathbb{Q}}^\times$ (with the natural $G_{\mathbb{Q}}$-action) fit into a commutative diagram

$$\begin{tikzcd}
\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}), \{\pm 1\})^{G_{\mathbb{Q}}^{\mathrm{ab}}} \arrow[r, "\mathrm{trg}"] \arrow[d] & \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\varphi_{\mathbb{Q}^{\mathrm{ab}}}"] & \mathrm{Br}(\mathbb{Q})[2] \arrow[d] \\
\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}), \overline{\mathbb{Q}}^\times)^{G_{\mathbb{Q}}^{\mathrm{ab}}} \arrow[r, "\mathrm{trg}"] & \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \mathbb{Q}^{\mathrm{ab}\times}) \arrow[r, "\mathrm{Inf}"] & \mathrm{Br}(\mathbb{Q}).
\end{tikzcd}$$

By Hilbert's theorem 90, $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}}), \overline{\mathbb{Q}}^\times)$ is trivial, so the map

$$\mathrm{Inf} : \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \mathbb{Q}^{\mathrm{ab}\times}) \to \mathrm{Br}(\mathbb{Q})$$

is injective. On the other hand, also the map $\mathrm{Br}(\mathbb{Q})[2] \to \mathrm{Br}(\mathbb{Q})$ is injective, and therefore we have

$$\ker \varphi_{\mathbb{Q}^{\mathrm{ab}}} = \ker(\mathrm{Inf} : \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]). \tag{4.1}$$

By Lemma 2.7, we have $\mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \cap \ker \varphi_{\mathbb{Q}^{\mathrm{ab}}} = \{1\}$, since a nontrivial element in this intersection would correspond to a nontrivial extension of $\mathbb{Q}^{\mathrm{ab}}$ that is Galois and abelian over $\mathbb{Q}$. This shows that the map

$$\mathrm{Inf} : \mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$$

is injective.

To prove surjectivity, we recall that for every place v of $\mathbb{Q}$, we have a canonical homomorphism $\mathrm{inv}_v : \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z}$, and that we have a canonical exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_v \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where v runs over all places of $\mathbb{Q}$; the first nontrivial map is the product of the restriction maps $\mathrm{Res}_v : \mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{Q}_v)$, and the second one is the sum of the maps inv_v. Let ℓ be a prime and consider the element $\varepsilon_\ell \in \mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$ that under the isomorphism from (i) corresponds to the element $(t_p)_p \in \bigoplus_{p \text{ prime}} \{\pm 1\}$ defined by

$$t_p = \begin{cases} -1 & \text{if } p = \ell, \\ 1 & \text{otherwise.} \end{cases}$$

We will show that $\mathrm{Inf}(\varepsilon_\ell) \in \mathrm{Br}(\mathbb{Q})$ [2] is ramified precisely at ℓ and ∞, by looking at the images of $\mathrm{Inf}(\varepsilon_\ell)$ under the restriction maps Res_v.

We write $\mathbb{Q}(\zeta_{\ell^\infty})$ for the field obtained by adjoining all roots of unity of ℓ-power order to $\mathbb{Q}$. Let v be a finite place of $\mathbb{Q}$ different from ℓ, and let $\mathbb{Q}_v^{\mathrm{nr}}$ be the maximal unramified extension of $\mathbb{Q}_v$. Embedding $\mathbb{Q}_v(\zeta_{\ell^\infty})$ into $\mathbb{Q}_v^{\mathrm{nr}}$, we obtain a commutative diagram

$$\begin{tikzcd}
\mathrm{H}^2_{\mathrm{s}}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}, \{\pm 1\}) \arrow[rr, "\mathrm{Inf}"] \arrow[d, "\mathrm{Res}_v"] & & \mathrm{Br}(\mathbb{Q}) \arrow[d, "\mathrm{Res}_v"] \\
\mathrm{H}^2_{\mathrm{s}}(\mathbb{Q}_v(\zeta_{\ell^\infty})/\mathbb{Q}_v, \{\pm 1\}) \arrow[r, "\mathrm{Inf}"] & \mathrm{Br}(\mathbb{Q}_v^{\mathrm{nr}}/\mathbb{Q}_v) \arrow[r, "\sim"] \arrow[d, "v_*"] & \mathrm{Br}(\mathbb{Q}_v) \\
 & \mathrm{H}^2(\mathbb{Q}_v^{\mathrm{nr}}/\mathbb{Q}_v, \mathbb{Z}). &
\end{tikzcd}$$

Here, v_* is induced by the valuation map $v : \mathbb{Q}_v^{\mathrm{nr}\times} \to \mathbb{Z}$, and is an isomorphism because the Brauer group of a finite field is trivial [17, §X.7 and §XII.3]. Now, the composed map $v_* \circ \mathrm{Inf}$ vanishes because units have valuation 0, so the map Inf in the middle row vanishes as well. Since ε_ℓ is inflated from $\mathrm{H}^2_{\mathrm{s}}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}, \{\pm 1\})$, it follows that for all finite places v of $\mathbb{Q}$ different from ℓ we have $\mathrm{Res}_v(\mathrm{Inf}(\varepsilon_\ell)) = 0$ in $\mathrm{Br}(\mathbb{Q}_v)$. Because $\varepsilon_\ell \in \mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$ is nontrivial and the map $\mathrm{Inf} : \mathrm{H}^2_{\mathrm{s}}(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$ is injective as shown above, it follows that $\mathrm{Inf}(\varepsilon_\ell) \in \mathrm{Br}(\mathbb{Q})[2]$ is ramified precisely at ℓ and ∞, which is what we wanted to show. □

Proof of Theorem 4.1. The first implication is clear from Theorem 3.5.

Let us now prove the converse. Assume that E has a model E_0 completely defined over an abelian number field K. Let $\xi_K = \xi_K(E_0) \in \mathrm{Z}^2(K/\mathbb{Q}, \mathbb{Q}^\times)$ be the 2-cocycle attached to E_0. For every extension L/K that is Galois over $\mathbb{Q}$, we denote by $[\xi_L]$ the inflation of $[\xi_K]$ to $\mathrm{H}^2(L/\mathbb{Q}, \mathbb{Q}^\times)$. For every Galois extension $M/\mathbb{Q}$, we denote by

$$\varphi_M : \mathrm{H}^2(M/\mathbb{Q}, \{\pm 1\}) \to \mathrm{H}^2(M/\mathbb{Q}, M^\times)$$

the canonical map induced by the inclusion $\{\pm 1\} \subseteq M^\times$.

We will show that there exists an abelian extension $L/\mathbb{Q}$, containing K, such that $(E_0)_L$ has a strongly modular twist over L. By Theorem 3.5, Lemma 4.3 and Remark 3.6, this happens if and only if there exists an abelian number field L containing K and an element $\gamma \in L^\times$ such that:

- $L(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$;
- if $c \in \mathrm{H}^2(L/\mathbb{Q}, \{\pm 1\})$ is the cohomology class attached to the exact sequence

$$1 \to \{\pm 1\} \to \mathrm{Gal}(L(\sqrt{\gamma})/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1,$$

then the class $[\xi_L^\pm] \cdot c$ in $\mathrm{H}^2(L/\mathbb{Q}, \{\pm 1\})$ is symmetric.

By Lemma 2.7, these conditions are satisfied for a given L if and only if there exists $c \in \ker \varphi_L$ such that $[\xi_L^{\pm}] \cdot c$ is symmetric. Writing $\mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$ and $\mathrm{H}_{\mathrm{s}}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$ as direct limits indexed by finite abelian extensions of $\mathbb{Q}$ containing K, we see that there exist L and c as above if and only if there exists $c' \in \ker \varphi_{\mathbb{Q}^{\mathrm{ab}}}$ such that $[\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm}] \cdot c' \in \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$ is symmetric.

By (4.1), the kernel of $\varphi_{\mathbb{Q}^{\mathrm{ab}}}$ equals the kernel of $\mathrm{Inf} : \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2]$. Therefore, it remains to prove that there exists $c \in \ker(\mathrm{Inf} : \mathrm{H}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\}) \to \mathrm{Br}(\mathbb{Q})[2])$ such that $[\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm}] \cdot c$ is symmetric. This amounts to saying that the image of $[\xi_{\mathbb{Q}^{\mathrm{ab}}}^{\pm}]$ in $\mathrm{Br}(\mathbb{Q})[2]$ belongs to the image of $\mathrm{H}_{\mathrm{s}}^2(G_{\mathbb{Q}}^{\mathrm{ab}}, \{\pm 1\})$. By Proposition 4.4, this is always the case, and the proof is complete. □

5. Twists of Quadratic $\mathbb{Q}$-Curves

Theorem 4.1 is not effective: it only gives necessary and sufficient conditions for the existence of strongly modular twists, without providing an actual construction of them. In this section, for a $\mathbb{Q}$-curve over a quadratic field K, we will make the existence of strongly modular twists over the minimal field of complete definition L effective in terms of the arithmetic of L. For certain purposes, such as studying L-functions of elliptic curves, it is useful to understand when the curve "comes from a subfield" up to isogeny. We will show how to distinguish twists coming from subfields of L; this distinction will allow us to characterize all strongly modular twists of E over K (Corollary 5.10).

Definition 5.1. Let E be a $\mathbb{Q}$-curve completely defined over a number field L. If there exist a subfield K of L that is Galois over $\mathbb{Q}$ and a $\mathbb{Q}$-curve C completely defined over K such that E is L-isogenous to C_L, we say that E is *inflated from* K. If no such K and C exist, we say that E is *primitive*.

The reason for the terminology "inflated" will be clarified by Proposition 5.3. We recall the following theorem.

Theorem 5.2 ([16, Theorem 8.2]). *Let L/K be a Galois extension of number fields, and let E be a $\mathbb{Q}$-curve completely defined over L. Then the following are equivalent*:

(i) *there exist isomorphisms $\mu_\sigma : {}^\sigma E \to E$ of elliptic curves up to isogeny over L such that*

$$\mu_\sigma {}^\sigma\mu_\tau = \mu_{\sigma\tau} \quad \text{for all } \sigma, \tau \in \mathrm{Gal}(L/K);$$

(ii) *there exists an elliptic curve C over K such that E is L-isogenous to C_L.*

Now, let K and L be Galois number fields with $K \subseteq L$, and consider the inflation map $\mathrm{Inf}_L^K : \mathrm{H}^2(K/\mathbb{Q}, \mathbb{Q}^\times) \to \mathrm{H}^2(L/\mathbb{Q}, \mathbb{Q}^\times)$.

Proposition 5.3. *Let E be a $\mathbb{Q}$-curve completely defined over L and let $\xi_L(E)$ be its associated 2-cocycle.*

(i) *If E is inflated from K, then $[\xi_L(E)] \in \mathrm{Im}(\mathrm{Inf}_L^K)$.*
(ii) *If $\mathrm{Gal}(L/K)$ is contained in the center of $\mathrm{Gal}(L/\mathbb{Q})$ and $[\xi_L(E)] \in \mathrm{Im}(\mathrm{Inf}_L^K)$, then E is inflated from K.*

Proof. First assume that E is inflated from K. Let C be a $\mathbb{Q}$-curve completely defined over K such that C_L is isogenous to E. For all $\overline{\sigma} \in \mathrm{Gal}(K/\mathbb{Q})$, we fix a K-isogeny $\mu_{\overline{\sigma}} : {}^{\overline{\sigma}}C \to C$. Let $\xi_K(C) \in \mathrm{Z}^2(K/\mathbb{Q}, \mathbb{Q}^\times)$ be the 2-cocycle attached to C via the system of isogenies $\{\mu_{\overline{\sigma}}\}_{\overline{\sigma}}$, so that $\xi_K(C)(\overline{\sigma},\overline{\tau}) = \mu_{\overline{\sigma}}{}^{\overline{\sigma}}\mu_{\overline{\tau}}\mu_{\overline{\sigma\tau}}^{-1}$. Now for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, we set $\mu_\sigma = \mu_{\overline{\sigma}} : {}^{\sigma}C_L \to C_L$, for $\overline{\sigma}$ the class of σ in $\mathrm{Gal}(K/\mathbb{Q})$. Then the cocycle $\xi_L(C)$ corresponding to the system of isogenies $\{\mu_\sigma\}_\sigma$ represents the inflation of $[\xi_K(C)]$; since C_L and E are L-isogenous, we have $[\xi_L(C_L)] = [\xi_L(E)]$ and the claim follows.

To prove (ii), note that since $\mathrm{Res}_K^L \circ \mathrm{Inf}_L^K = 0$, we have $[\xi_L(E)] \in \ker(\mathrm{Res}_K^L)$. Thus by Theorem 5.2, there exists a $\mathbb{Q}$-curve C over K such that C_L is L-isogenous to E. Choose a system of isogenies $\{\mu_\sigma : {}^{\sigma}C_L \to C_L\}_{\sigma\in\mathrm{Gal}(L/\mathbb{Q})}$ with the following properties:

- $\mu_\sigma = 1$ whenever $\sigma \in \mathrm{Gal}(L/K)$;
- $\mu_\sigma = \mu_\tau$ whenever $\sigma \equiv \tau \bmod \mathrm{Gal}(L/K)$.

Let $\xi_L(C_L)$ be the 2-cocycle attached to C_L via the above system of isogenies. Now, suppose that C is not completely defined over K. Then there exist $\nu \in \mathrm{Gal}(L/\mathbb{Q})$, $\vartheta \in \mathrm{Gal}(L/K)$ such that ${}^{\vartheta}\mu_\nu = -\mu_\nu$; this implies

$$\xi_L(C_L)(\vartheta,\nu) = -1 \quad \text{and} \quad \xi_L(C_L)(\nu,\vartheta) = 1. \tag{5.1}$$

On the other hand, by hypothesis $[\xi_L(C_L)] = [\xi_L(E)]$ is inflated, so there exists a cocycle $c \in \mathrm{Z}^2(K/\mathbb{Q}, \mathbb{Q}^\times)$ such that $[\xi_L(C_L)] = \mathrm{Inf}_L^K([c])$. Let $\widetilde{c} \in \mathrm{Z}^2(L/\mathbb{Q}, \mathbb{Q}^\times)$ be the cocycle defined by $\widetilde{c}(\sigma,\tau) = c(\overline{\sigma},\overline{\tau})$ for all $\sigma,\tau \in \mathrm{Gal}(L/\mathbb{Q})$, where $\overline{\cdot}$ denotes the equivalence class modulo $\mathrm{Gal}(L/K)$. Let $\alpha : \mathrm{Gal}(L/\mathbb{Q}) \to \mathbb{Q}^\times$ be a map such that

$$\widetilde{c} = \xi_L(C_L) \cdot \delta\alpha.$$

Note that the cocycle condition for c implies $c(1,\nu) = c(\nu,1)$ for every $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$. Thus, $\widetilde{c}(\nu,\vartheta) = \widetilde{c}(\vartheta,\nu)$ and by (5.1), this yields $\alpha(\nu\vartheta) = -\alpha(\vartheta\nu)$, a contradiction since $\nu\vartheta = \vartheta\nu$. □

From now on, E is a $\mathbb{Q}$-curve without CM over a quadratic field $K = \mathbb{Q}(\sqrt{d})$, for $d \neq 0,1$ a square-free integer. The nontrivial automorphism of K will be denoted by ν. Moreover, we assume that E/K is not strongly modular, i.e. that there exists an isogeny $\mu_\nu : {}^{\nu}E \to E$ of degree m that is not defined over K.

Lemma 5.4. *The minimal field of complete definition L of E has Galois group $C_2 \times C_2$ over $\mathbb{Q}$.*

Proof. It is clear from the construction of L in the proof of Proposition 3.3 that L is a quadratic extension of K.

Suppose that $\mathrm{Gal}(L/\mathbb{Q}) \simeq C_4$. Write $\mathrm{Gal}(L/\mathbb{Q}) = \{1, \nu, \nu^2, \nu^3\}$, where by a slight abuse of notation, $\nu \in \mathrm{Gal}(L/\mathbb{Q})$ is a lift of $\nu \in \mathrm{Gal}(K/\mathbb{Q})$. We can set $\mu_{\nu^2} = \mathrm{id}$ and $\mu_{\nu^3} = \mu_\nu$. Let $\xi_L^\pm$ be the sign part of the 2-cocycle attached to E_L via this system of isogenies. Since $\mathrm{H}^2(C_4, \{\pm 1\}) \simeq C_2 \simeq \mathrm{H}^2_{\mathrm{s}}(C_4, \{\pm 1\})$, the cocycle $\xi_L^\pm$ is symmetric. Then $\xi_L^\pm(\nu, \nu^2) = \mu_\nu {}^{\nu}\mu_{\nu^2}\mu_{\nu^3}^{-1} = \mu_\nu \mu_\nu^{-1} = 1$. On the other hand, note that ${}^{\nu^2}\mu_\nu$, which is an isogeny ${}^{\nu}E \to E$, cannot coincide with μ_ν, since this would imply that μ_ν is defined over K. But μ_ν and ${}^{\nu^2}\mu_\nu$ have the same degree, and therefore ${}^{\nu^2}\mu_\nu = -\mu_\nu$. Thus, $\xi_L^\pm(\nu^2, \nu) = \mu_{\nu^2} {}^{\nu^2}\mu_\nu \mu_{\nu^3}^{-1} = -\mu_\nu \mu_\nu^{-1} = -1$, which contradicts the symmetry of $\xi_L^\pm$. □

Let $e \neq 0, 1$ be a squarefree integer such that $L = \mathbb{Q}(\sqrt{d}, \sqrt{e})$ is the minimal field of complete definition for E. From now on, we set

$$K_e := \mathbb{Q}(\sqrt{e}), \quad K_{de} := \mathbb{Q}(\sqrt{de}) \quad \text{and} \quad G := \mathrm{Gal}(L/\mathbb{Q}) = \{1, \nu, \vartheta, \nu\vartheta\},$$

where ϑ is the generator of $\mathrm{Gal}(L/K)$ and by a small abuse of notation the element $\nu \in G$ restricts to the nontrivial automorphism of K, which we also call ν.

Let us compute the 2-cocycle $\xi_L := \xi_L(E_L) \in \mathrm{H}^2(L/\mathbb{Q}, \mathbb{Q}^\times)$ attached to E_L. Let $\mu_\vartheta \colon {}^{\vartheta}E_L = E_L \to E_L$ be the identity and let $\mu_{\nu\vartheta} = \mu_\nu : {}^{\nu\vartheta}E_L = {}^{\nu}E_L \to E_L$. Note that ${}^{\vartheta}\mu_\nu : {}^{\nu\vartheta}E_L = {}^{\nu}E_L \to E_L = {}^{\vartheta}E_L$ is an isogeny of the same degree as μ_ν; since E_L has no CM, ${}^{\vartheta}\mu_\nu$ coincides with μ_ν up to sign. However, if it were ${}^{\vartheta}\mu_\nu = \mu_\nu$, then μ_ν would be defined over K, a contradiction; thus we have ${}^{\vartheta}\mu_\nu = -\mu_\nu$, and hence ${}^{\nu\vartheta}\mu_\nu = -{}^{\nu}\mu_\nu$. The isogeny $\mu_\nu {}^{\nu}\mu_\nu$ equals multiplication by an integer $m \in \mathbb{Z} \setminus \{0, 1\}$. By an easy computation, we end up with the following table for the cocycle ξ_L:

$\xi_L(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	-1	-1
ν	1	1	m	m
$\nu\vartheta$	1	1	$-m$	$-m$

The sign component $[\xi_L^\pm] \in \mathrm{H}^2(L/\mathbb{Q}, \mathbb{Q}^\times)$ is represented by one of the following two non-cohomologous cocycles, depending on the sign of m.

$\eta_1(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	-1	-1
ν	1	1	1	1
$\nu\vartheta$	1	1	-1	-1

$\eta_2(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	-1	-1
ν	1	1	-1	-1
$\nu\vartheta$	1	1	1	1

The table of ξ_L shows that the curve E_L is not strongly modular over L, because of Theorem 3.5. The question we want to address is: which quadratic twists of E_L are strongly modular? A first answer is provided by the following lemma.

Lemma 5.5. *Let $\gamma \in L^\times$. Then the twisted curve E_L^γ is strongly modular over L if and only if $L(\sqrt{\gamma})$ is Galois and non-abelian over $\mathbb{Q}$.*

Proof. Let ξ_L^γ be the cocycle attached to E_L^γ. By Theorem 3.5, Lemma 4.3 and Remark 3.6, the curve E_L^γ is strongly modular if and only if $L(\sqrt{\gamma})$ is Galois over $\mathbb{Q}$ and $[\xi_L^{\gamma,\pm}] \in \mathrm{H}^2_{\mathrm{s}}(L/\mathbb{Q}, \{\pm 1\})$. The group $\widetilde{G} := \mathrm{Gal}(L(\sqrt{\gamma})/\mathbb{Q})$ is abelian if and only if the 2-cocycle attached to the exact sequence $1 \to \pm 1 \to \widetilde{G} \to G \to 1$ is symmetric. Therefore, when $\widetilde{G}$ is abelian, by Lemma 4.3, the symmetry of the cocycle ξ_L attached to E_L does not change under twisting by γ, and this shows that E_L^γ cannot be strongly modular. On the other hand, by Lemmas 2.3 and 2.4 we have $\mathrm{H}^2_{\mathrm{s}}(G, \{\pm 1\}) \simeq C_2 \times C_2$, while by Theorem 2.5 we have $\mathrm{H}^2(G, \{\pm 1\}) \simeq C_2^3$. This shows that $\mathrm{H}^2(G, \{\pm 1\})/\mathrm{H}^2_{\mathrm{s}}(G, \{\pm 1\}) \simeq C_2$, which means that the product of two asymmetric classes in $\mathrm{H}^2(G, \{\pm 1\})$ is symmetric. Whenever $\widetilde{G}$ is non-abelian, we therefore have $[\xi_L^\gamma] \in \mathrm{H}^2_{\mathrm{s}}(G, \{\pm 1\})$. □

Remark 5.6. Let us describe the structure of $\mathrm{H}^2(L/\mathbb{Q}, \{\pm 1\})$ more in detail. Recall that elements of this group correspond to equivalence classes of central extensions of the form $1 \to \{\pm 1\} \to \widetilde{G} \to G \to 1$. There are four symmetric cohomology classes and four asymmetric ones. The symmetric classes correspond to extensions with $\widetilde{G} \simeq C_2 \times C_2 \times C_2$ or $\widetilde{G} \simeq C_4 \times C_2$. The asymmetric classes correspond to extensions with $\widetilde{G} \simeq D_4$, the dihedral group of order 8, or $\widetilde{G} \simeq H_8$, the group of quaternions. All extensions with $\widetilde{G} \simeq H_8$ are equivalent to each other, and the corresponding cohomology class is represented by the following cocycle:

$h_0(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	-1	1
ν	1	1	-1	-1
$\nu\vartheta$	1	-1	1	-1

On the other hand, there are three non-equivalent extensions with $\widetilde{G} \simeq D_4$. These are uniquely determined by the image in G of the cyclic subgroup of order 4 in D_4. If $\gamma \in L^\times$ is such that $\widetilde{G} = \mathrm{Gal}(L(\sqrt{\gamma})/\mathbb{Q}) \simeq D_4$, $\sigma \in \widetilde{G}$ is an element of order 4 and $\overline{\sigma}$ is its image in G, then $L^{\overline{\sigma}}$ is the unique subextension such that $\mathrm{Gal}(L(\sqrt{\gamma})/L^{\overline{\sigma}}) \simeq C_4$. The following three cocycles represent these classes. The C_4-subextension is $L(\sqrt{\gamma})/K, L(\sqrt{\gamma})/K_e, L(\sqrt{\gamma})/K_{de}$, respectively.

$h_d(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	1	-1
ν	1	-1	1	-1
$\nu\vartheta$	1	1	1	1

$h_e(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	-1	-1	1
$\nu\vartheta$	1	-1	-1	1

$h_{de}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	-1	1	-1
$\nu\vartheta$	1	-1	1	-1

5.1. *Distinguishing inflated and primitive twists*

Let $\gamma \in L^\times$ be such that E_L^γ is strongly modular. By Lemma 5.5, $L(\sqrt{\gamma})$ is a non-abelian Galois extension of $\mathbb{Q}$, and $\widetilde{G} := \mathrm{Gal}(L(\sqrt{\gamma})/\mathbb{Q})$ falls in precisely one of the following cases:

(A) $\widetilde{G} \simeq H_8$;
(B) $\widetilde{G} \simeq D_4$ and the unique C_4-subextension is $L(\sqrt{\gamma})/K$;
(C) $\widetilde{G} \simeq D_4$ and the unique C_4-subextension is $L(\sqrt{\gamma})/K_e$;
(D) $\widetilde{G} \simeq D_4$ and the unique C_4-subextension is $L(\sqrt{\gamma})/K_{de}$.

Recall that the sign component $\xi_L^\pm$ of the 2-cocycle attached to E_L equals one of the two classes $[\eta_1]$ and $[\eta_2]$ described below Lemma 5.4.

Lemma 5.7. *If* $|m| \in (\mathbb{Q}^\times)^2$, *the curve* E_L^γ *is inflated from the subfield* $F \subseteq L$, *according to the following table*:

case $[\xi_L^\pm]$	(A)	(B)	(C)	(D)
$[\eta_1]$	K_{de}	K_e	K	$\mathbb{Q}$
$[\eta_2]$	K_e	K_{de}	$\mathbb{Q}$	K

If $|m| \notin (\mathbb{Q}^\times)^2$, *the curve* E_L^γ *is inflated from* K *if and only if* (C) *or* (D) *holds, and it is primitive if and only if* (A) *or* (B) *holds.*

Proof. By Proposition 5.3 and the fact that the inflation map preserves the degree and the sign components and the subgroup of symmetric classes, E_L^γ is inflated from a Galois subfield $F \subseteq L$ if and only if $[\xi_L^{\gamma,\pm}]$ is the inflation of a cohomology class in $\mathrm{H}^2_{\mathrm{s}}(F/\mathbb{Q}, \{\pm 1\})$ and $[\xi_L^{\gamma,\deg}]$ is the inflation of a cohomology class in $\mathrm{H}^2_{\mathrm{s}}(F/\mathbb{Q}, \mathbb{Q}_+^\times)$.

By Lemma 4.3, $[\xi_L^\gamma]$ is the product of $[\xi_L]$ with the class $[t]$ corresponding to the exact sequence

$$1 \to \mathrm{Gal}(L(\sqrt{\gamma})/L) \to \mathrm{Gal}(L(\sqrt{\gamma})/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q}) \to 1.$$

The elements h_0, h_d, h_e and h_{de} described in Remark 5.6 represent cases (A), (B), (C) and (D), respectively.

The degree component of ξ_L coincides with that of ξ_L^γ and is represented by the following cocycle:

$\xi_L^{\mathrm{deg}}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	1	$\lvert m\rvert$	$\lvert m\rvert$
$\nu\vartheta$	1	1	$\lvert m\rvert$	$\lvert m\rvert$

If $|m| \in (\mathbb{Q}^\times)^2$, then $[\xi_L^{\mathrm{deg}}]$ is trivial. Thus, $[\xi_L^\gamma]$ is inflated if and only if $[\xi_L^{\gamma,\pm}]$ is inflated. The nontrivial symmetric classes in $\mathrm{H}^2(L/\mathbb{Q}, \{\pm 1\})$ are represented by the following cocycles b_d, b_e, b_{de}:

$b_d(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	1	1	1
ν	1	1	-1	-1
$\nu\vartheta$	1	1	-1	-1

$b_e(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	1	-1
ν	1	1	1	1
$\nu\vartheta$	1	-1	1	-1

$b_{de}(\cdot,\cdot)$	1	ϑ	ν	$\nu\vartheta$
1	1	1	1	1
ϑ	1	-1	-1	1
ν	1	-1	-1	1
$\nu\vartheta$	1	1	1	1

It is immediately clear that $[b_d]$ (respectively, $[b_e]$, $[b_{de}]$) is the inflation of the unique nontrivial element in $\mathrm{H}^2(K/\mathbb{Q}, \{\pm 1\})$ (respectively, $\mathrm{H}^2(K_e/\mathbb{Q}, \{\pm 1\})$, $\mathrm{H}^2(K_{de}/\mathbb{Q}, \{\pm 1\})$). Thus, our claim is equivalent to showing that the multiplication table of $[\eta_1], [\eta_2]$ by $[h_0], [h_d], [h_e], [h_{de}]$ is the following:

$\cdot$	$[h_0]$	$[h_d]$	$[h_e]$	$[h_{de}]$
$[\eta_1]$	$[b_{de}]$	$[b_e]$	$[b_d]$	1
$[\eta_2]$	$[b_e]$	$[b_{de}]$	1	$[b_d]$

and it is easy to check that this is the case.

Assume now that $|m| \notin (\mathbb{Q}^\times)^2$. The class $[\xi_L^{\mathrm{deg}}]$ is the inflation from $\mathrm{H}^2(K/\mathbb{Q}, \mathbb{Q}_+^\times)$ of the class $[c]$, where $c(1,1) = c(1,\nu) = c(\nu,1) = 1$ and $c(\nu,\nu) = |m|$, while it is not the inflation of a class lying in $\mathrm{H}^2(F/\mathbb{Q}, \mathbb{Q}_+^\times)$ for any $F \in \{\mathbb{Q}, K_e, K_{de}\}$. Thus, E_L^γ is inflated if and only if it is inflated from K.

Therefore, it is enough to check when $[\xi_L^{\gamma,\pm}]$ coincides with $[b_K]$. Since $[b_K] = [\eta_1] \cdot [\eta_2]$, the class $[\xi_L^{\gamma}]$ is inflated if and only if the class $[t]$ equals either $[\eta_1]$ or $[\eta_2]$. It is immediate to see that $[\eta_1] = [h_{de}]$ and $[\eta_2] = [h_e]$, and the proof is complete. □

The next step is to give necessary and sufficient conditions for the existence of primitive or inflated twists of E_L. Recall that $L = \mathbb{Q}(\sqrt{d}, \sqrt{e})$ is a $C_2 \times C_2$-extension of $\mathbb{Q}$ and $G = \mathrm{Gal}(L/\mathbb{Q}) = \langle \nu, \vartheta \rangle$ where ${}^{\nu}\sqrt{d} = -\sqrt{d}$, ${}^{\vartheta}\sqrt{e} = -\sqrt{e}$. For $a, b \in \mathbb{Q}$, we will denote by (a, b) the quaternion algebra over $\mathbb{Q}$ with basis $\{1, i, j, ij\}$ such that $i^2 = a$, $j^2 = b$, $ij = -ji$. Recall that the *reduced discriminant* of a quaternion algebra B over $\mathbb{Q}$ is the product of the finite primes of $\mathbb{Q}$ where B ramifies. A quaternion algebra is trivial in $\mathrm{Br}(\mathbb{Q})$ if and only if it has reduced discriminant 1.

Theorem 5.8 ([10, Theorems 4 and 5]). *The following hold*:

(i) *Let $H_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the group of quaternions. The embedding problem* (*cf. Definition* 2.6) *relative to $L/\mathbb{Q}$ and the group extension*

$$1 \to C_2 \to H_8 \xrightarrow{\pi} G \to 1$$

is solvable if and only if $(d, de)(e, de)(d, e) = 1$ in $\mathrm{Br}(\mathbb{Q})$, *if and only if there exist $v_1, v_2, v_3, w_1, w_2, w_3 \in \mathbb{Q}$ such that*

$$\begin{cases} d = v_1^2 + v_2^2 + v_3^2, \\ e = w_1^2 + w_2^2 + w_3^2, \\ v_1w_1 + v_2w_2 + v_3w_3 = 0. \end{cases}$$

In this case, setting $t = 1 + \frac{v_1}{\sqrt{d}} + \frac{w_3}{\sqrt{e}} + \frac{v_1w_3 - v_3w_1}{\sqrt{de}}$, the extensions solving the problem are exactly the ones of the form $L(\sqrt{qt})$, for $q \in \mathbb{Q}^{\times}$.

(ii) *Let $D_4 = \langle \sigma, \tau : \sigma^4 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \rangle$ be the dihedral group of order* 8. *The embedding problem relative to $L/\mathbb{Q}$ and the group extension*

$$1 \to C_2 \to D_4 \xrightarrow{\pi} G \to 1,$$

where $\pi(\sigma) = \vartheta$ and $\pi(\tau) = \nu$ is solvable if and only if $(-d, e) = 1$ in $\mathrm{Br}(\mathbb{Q})$.

In this case, if $x, y \in \mathbb{Q}$ are such that $d = ey^2 - x^2$, the extensions solving this problem are exactly the ones of the form $L(\sqrt{q(ey + x\sqrt{e})})$ for $q \in \mathbb{Q}^{\times}$.

Recall that the class $[\xi_L^{\gamma,\pm}]$ equals one of the classes η_1, η_2 described below Lemma 5.4.

Theorem 5.9. *There exists $\gamma \in L^{\times}$ such that E^{γ} is strongly modular if and only if at least one of the following conditions is satisfied*:

(A) *the quaternion algebra $(-d, -e)$ has reduced discriminant* 2;
(B) *the quaternion algebra $(-d, e)$ is trivial in* $\mathrm{Br}(\mathbb{Q})$;
(C) *the quaternion algebra $(d, -e)$ is trivial in* $\mathrm{Br}(\mathbb{Q})$;
(D) *the quaternion algebra $(d, -de)$ is trivial in* $\mathrm{Br}(\mathbb{Q})$.

In particular, if $m \in (\mathbb{Q})^{\times 2}$ then there exists γ such that E^γ is inflated from the subfield F, according to the following table:

case $[\xi_L^{\pm}]$	(A)	(B)	(C)	(D)
$[\eta_1]$	K_{de}	K_e	K	$\mathbb{Q}$
$[\eta_2]$	K_e	K_{de}	$\mathbb{Q}$	K

If $m \notin (\mathbb{Q})^{\times 2}$, then there exists γ such that E^γ is primitive if and only if (A) *or* (B) *holds, while there exists γ such that E^γ is inflated from K if and only if* (C) *or* (D) *holds.*

Proof. By Lemma 5.5, E^γ is strongly modular if and only if $L(\sqrt{\gamma})/\mathbb{Q}$ is a non-abelian Galois extension. Thus, there exists γ such that E^γ is strongly modular if and only if the embedding problem

$$1 \to \mathrm{Gal}(L(\sqrt{\gamma})/L) \to \widetilde{G} \to \mathrm{Gal}(L/\mathbb{Q}) \to 1 \tag{5.2}$$

has a solution with $\widetilde{G}$ non-abelian.

When $\widetilde{G} \simeq H_8$, by Theorem 5.8 and the discussion at [10, p. 239], the embedding problem (5.2) is solvable if and only if the quadratic forms $S_{d,e} = \frac{1}{de}X^2 + dY^2 + eZ^2$ and $T = X^2 + Y^2 + Z^2$ are equivalent over $\mathbb{Q}$. This implies immediately that $d, e > 0$ because $S_{d,e}$ and T must have the same signature. Since the rank and the discriminant obviously coincide, it only remains to check that the Hasse–Witt invariants coincide. If p is a prime, the Hasse–Witt invariant of T at p is 1, while the Hasse–Witt invariant of $S_{d,e}$ at p is

$$\begin{aligned}(de,d)_p(de,e)_p(d,e)_p &= (de,d)_p(de,e)_p(-d,-e)_p(d,-1)_p(-1,e)_p(-1,-1)_p \\ &= (de,-de)_p(-d,-e)_p(-1,-1)_p \\ &= (-d,-e)_p(-1,-1)_p,\end{aligned}$$

where we used bilinearity of the Hilbert symbol and the fact that $(a,-a)_p = 1$ for every $a \in \mathbb{Q}^\times$ and every prime p. Since $(-1,-1)$ ramifies precisely at 2 and ∞, we see that this instance of the embedding problem is solvable if and only if (A) holds.

When $\widetilde{G} \simeq D_4$, point (ii) of Theorem 5.8 shows that the embedding problem (5.2) is solvable if and only if (B), (C) or (D) holds.

The other claims follow immediately from Lemma 5.7. □

Corollary 5.10. *The curve E has a strongly modular quadratic twist over K if and only if the curve E_L has a strongly modular twist that is inflated from K.*

Proof. First recall that, by Theorem 3.5, a $\mathbb{Q}$-curve over a quadratic field K is strongly modular if and only if it is completely defined over K.

Let $\gamma \in K^\times$ be such that E^γ is strongly modular over K. Then the base-changed curve $(E^\gamma)_L$ is strongly modular over L since its attached cocycle is the inflation of a symmetric one, and is therefore symmetric. On the other hand, $(E^\gamma)_L$ is isomorphic to $(E_L)^\gamma$, and hence E_L has a strongly modular twist inflated from K.

Conversely, if E_L has a strongly modular twist $(E_L)^\gamma$ inflated from K, then by Theorem 5.9 at least one of $(d, -e)$ or $(d, -de)$ is trivial. Theorem 5.8 shows that we can choose $\gamma \in K^\times$: it is enough to use point (ii) of the theorem, replacing the map π by the one given by $\pi(\tau) = \vartheta$ and $\pi(\sigma) = \nu$ or $\pi(\sigma) = \nu\vartheta$. Then d plays the role of e in the notation of the theorem, and it is clear that $\gamma \in K^\times$. Therefore, $(E_L)^\gamma$ is L-isomorphic to $(E^\gamma)_L$. Now, E^γ is completely defined over K, otherwise E_L^γ would not be strongly modular since its attached cocycle would not be symmetric (cf. the discussion below Lemma 5.4). □

5.2. *Examples*

We will now give examples of $\mathbb{Q}$-curves with different behaviors with respect to the existence of primitive and inflated strongly modular quadratic twists.

Example 1. The following example is borrowed from [13]. Let E be the following elliptic curve without CM over $K = \mathbb{Q}(\sqrt{-3})$:

$$E : y^2 = x^3 + 2x^2 + bx,$$

where $b \in \mathcal{O}_K$ is any element of trace 1. There is an isogeny $\mu_\nu : {}^\nu E \to E$ such that $\mu_\nu {}^\nu\mu_\nu = -2$. The minimal field of definition of E is $L = \mathbb{Q}(\sqrt{-3}, \sqrt{-2})$. Since $(3, -2)$ is trivial in $\mathrm{Br}(\mathbb{Q})$, by Theorem 5.9, there are quadratic extensions of L of type D_4 over $\mathbb{Q}$ with C_4-subextension $L(\sqrt{\gamma})/K$. Since $\alpha = 1 + \sqrt{-2} \in \mathbb{Q}(\sqrt{e})$ has norm $3 = -d$, by Theorem 5.8, the set of all these extensions is $\{L(\sqrt{r + r/\sqrt{-2}}) : r \in \mathbb{Q}^\times\}$. The one found in [13] corresponds to $r = 2$. Let $\gamma = 2 - \sqrt{-2}$. An integral model for E_L^γ is

$$E_L^\gamma : y^2 = x^3 + (4 - 2\sqrt{-2})x^2 + b(2 - 4\sqrt{-2})x.$$

By Theorem 5.9, there are no quadratic extensions of L that are of type H_8 over $\mathbb{Q}$, nor quadratic extensions of type D_4 with C_4-subextension $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{6})$. Thus, all strongly modular quadratic twists of E are primitive over L. Note also that [13, Proposition 6.2], which asserts that there are no quadratic twists of E that are completely defined over K, follows immediately from Corollary 5.10.

To construct other examples, consider the following family of $\mathbb{Q}$-curves given in [14]:

$$E_a : y^2 = x^3 - 3\sqrt{a}(4 + 5\sqrt{a}\,)x + 2\sqrt{a}(2 + 14\sqrt{a} + 11a),$$

where $a \in \mathbb{Z}$ is not a square. Then E_a is defined over $K_a \coloneqq \mathbb{Q}(\sqrt{a})$, but its minimal field of complete definition is $L_a \coloneqq K_a(\sqrt{3})$.

Example 2. Consider the curve $(E_6)_{L_6}$. With the notation of Theorem 5.9, we have $d = 6$ and $e = 3$. Since $j(E_6) = \frac{27625536+10768896\sqrt{6}}{125}$, it follows that E_6 has no CM.

The quaternion algebra $(-6,-3) = (-2,-3)$ has reduced discriminant 2, and therefore by Theorem 5.9 it follows that L_6 has a quadratic extension of type H_8 over $\mathbb{Q}$. Following the notation of Theorem 5.8, we can pick $v_1 = 2$, $v_2 = v_3 = 1$, w_1 and $w_2 = w_3 = -1$. Thus, $t = 1 + \frac{2}{\sqrt{6}} - \frac{1}{\sqrt{3}} - \frac{1}{\sqrt{2}}$ and all extensions of type H_8 of L_6 are of the form $L_6(\sqrt{qt})$ with $q \in \mathbb{Q}^{\times}$. For example, letting $q = 1$ and $\gamma = t$, an integral model for $(E_6)^{\gamma}_{L_6}$ is

$$(E_6)^{\gamma}_{L_6} : y^2 = x^3 + Ax + B,$$

where

$$A = 4080384\alpha^3 - 13616640\alpha^2 - 412416\alpha + 1375488,$$

$$B = -25868537856\alpha^3 + 82215567360\alpha^2 + 2613252096\alpha - 8305459200$$

and $\alpha = \sqrt{2} + \sqrt{3}$. This is a primitive strongly modular curve over L_6.

Since $(-6,3)$ and $(6,-3)$ both have reduced discriminant 6, there are no extensions of L_6 that are of type D_4 over $\mathbb{Q}$ with C_4-subextension $L_6/\mathbb{Q}(\sqrt{6})$ or $L_6/\mathbb{Q}(\sqrt{3})$. On the other hand, $(6,-18)$ is trivial in $\mathrm{Br}(\mathbb{Q})$, so by Corollary 5.10 there exist strongly modular twists of E_6. To find them, note that by Theorem 5.8 it is enough to find $x, y \in \mathbb{Q}$ with $6y^2 - x^2 = 18$. As $x = 6$, $y = 3$ solve this equation, letting $t = 18 + 6\sqrt{6}$ we get that all extensions of L_6 of type D_4 over $\mathbb{Q}$ are of the form $L_6(\sqrt{qt})$ with $q \in \mathbb{Q}^{\times}$. Let us choose for example $q = 1/6$ and $\gamma' = qt$. Then an integral model for $E_6^{(\gamma')}$ is

$$E_6^{(\gamma')} : y^2 = x^3 - (28512 + 11520\sqrt{6})x + 2594304 + 1059840\sqrt{6}.$$

Example 3. The curve E_7 is not strongly modular, but since $(7,-3)$ is trivial, by Corollary 5.10 it has strongly modular quadratic twists. For example setting $\gamma = 7 + 2\sqrt{7}$, the curve E^{γ} is strongly modular over K_7. An integral model is

$$E_7^{\gamma} : y^2 = x^3 - (166992 + 61824\sqrt{7})x + 36452864 + 13804672\sqrt{7}.$$

Since $(-7,-3)$ has reduced discriminant 3 and $(-7,3)$ has reduced discriminant 21, Theorem 5.9 shows that $(E_7)_{L_7}$ has no primitive strongly modular twists.

Example 4. Finally, the curve $(E_5)_{L_5}$ has no strongly modular twists at all, since $(3,-5)$ has reduced discriminant 10, $(-3,-5)$ has reduced discriminant 5 and both $(5,-3)$ and $(5,-15)$ have reduced discriminant 15.

Acknowledgments

The first author was partially supported by the Netherlands Organisation for Scientific Research (NWO) through Veni grant 639.031.346. The second author was supported by Swiss National Science Foundation grant number 168459.

References

[1] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14**(4) (2001) 843–939.

[2] P. J. Bruin and A. Ferraguti, On L-functions of quadratic $\mathbb{Q}$-curves, *Math. Comp.* **87**(309) (2018) 459–499.

[3] J. González and J.-C. Lario, $\mathbb{Q}$-Curves and their Manin ideals, *Amer. J. Math.* **123**(3) (2001) 475–503.

[4] J. González, J.-C. Lario and J. Quer, Arithmetic of $\mathbb{Q}$-curves, in *Modular Curves and Abelian Varieties*, Progress in Mathematics, Vol. 224 (Birkhäuser, Basel, 2004), pp. 125–139.

[5] E. González-Jiménez and X. Guitart, On the modularity level of modular abelian varieties over number fields, *J. Number Theory* **130** (2010) 1560–1570.

[6] X. Guitart and J. Quer, Remarks on strongly modular Jacobian surfaces, *J. Théor. Nombres Bordeaux* **23**(1) (2011) 171–182.

[7] X. Guitart and J. Quer, Modular abelian varieties over number fields, *Canad. J. Math.* **66**(1) (2014) 170–196.

[8] U. Jannsen, The splitting of the Hochschild–Serre spectral sequence for a product of groups, *Canad. Math. Bull.* **33** (1990) 181–183.

[9] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture. I, *Invent. Math.* **178**(3) (2009) 485–504.

[10] I. Kiming, Explicit classification of some 2-extensions of a field of characteristic different from 2, *Canad. J. Math.* **42**(5) (1990) 825–855.

[11] J. S. Milne, On the arithmetic of abelian varieties, *Invent. Math.* **17** (1972) 177–190.

[12] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Vol. 323 (Springer-Verlag, Berlin, 2000).

[13] E. E. Pyle, Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$, *in Modular Curves and Abelian Varieties*, Progress in Mathematics, Vol. 224 (Birkhäuser, Basel, 2004), pp. 189–239.

[14] J. Quer, $\mathbb{Q}$-curves and abelian varieties of GL_2-type, *Proc. London Math. Soc.* (*3*) **81**(2) (2000) 285–317.

[15] J. Quer, Fields of definition of $\mathbb{Q}$-curves, *J. Théor. Nombres Bordeaux* **13**(13) (2001) 275–285.

[16] K. A. Ribet, Abelian varieties over $\mathbb{Q}$ and modular forms, in *Algebra and Topology* (Korea Advanced Institute of Science and Technology, Taejon, 1992), pp. 53–79.

[17] J.-P. Serre, *Corps Locaux*, Deuxième édition, Publications de l'Université de Nancago, Vol. VIII (Hermann, Paris, 1968).

[18] J.-P. Serre, *Cohomologie Galoisienne*, 5th edition, Lecture Notes in Mathematics, Vol. 5 (Springer-Verlag, Berlin, 1994).

[19] G. Shimura, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, *Nagoya Math. J.* **43**(171) (1971) 199–208.

[20] C. Weibel, *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics, Vol. 38 (Cambridge University Press, Cambridge, 1994).

[21] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141**(3) (1995) 443–551.

[22] A. Wiles and R. Taylor, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141**(3) (1995) 553–572.