TORSION OF $\mathbb{Q}$-CURVES OVER QUADRATIC FIELDS

SAMUEL LE FOURN AND FILIP NAJMAN

Abstract. We determine all the possible torsion groups of $\mathbb{Q}$-curves over quadratic fields and determine which groups appear finitely and which appear infinitely often.

1. Introduction

In the study of elliptic curves over number fields, describing the possible torsion groups plays an important role. This subject has a long history in which probably the most famous results are Mazur's torsion theorem [20] and Merel's proof of the uniform boundedness conjecture [22].

Historically, people have mostly studied the possible torsion groups of all elliptic curves over degree d number fields. One might however be interested in a more precise classification of possible properties of elliptic curves over degree d number fields, in the sense that one wants to find the properties of some subset of all elliptic curves defined over degree d number fields. This is both interesting in its own right and might be useful for applications, especially in Diophantine equations, as the curves that arise there often have some special property. To give two (out of many) examples, Pila [27] uses results about possible isogenies of non-CM elliptic curves with $\mathbb{Q}$-rational j-invariants [26] (no such results exist for all elliptic curves over degree d fields) to prove results about some diophantine problems arising out of "unlikely intersections" and Dieulefait and Urroz [8] use properties of $\mathbb{Q}$-curves over quadratic fields to solve the equation $x^4 + dy^2 = z^p$ for $d = 2$ and 3 and for large p.

The classification of all possible torsion groups of elliptic curves over quadratic fields was done in two steps, by Kenku and Momose [14] and by Kamienny [13]. All the possible torsion groups have been determined for the following subsets of all elliptic curves over quadratic fields: for elliptic curves with integral j-invariants [24], elliptic curves that are base changes of elliptic curves defined over $\mathbb{Q}$ [25] and elliptic curves with complex multiplication [7].

In this paper we determine the possible torsion groups of $\mathbb{Q}$-curves over quadratic fields. Recall that a $\mathbb{Q}$-curve is an elliptic curve isogenous (over $\overline{\mathbb{Q}}$) to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. These properties are obviously satisfied by elliptic curves defined over $\mathbb{Q}$, so $\mathbb{Q}$-curves can be thought of as generalizations of elliptic curves defined over $\mathbb{Q}$. Moreover, Ribet [28] proved (assuming Serre's conjecture, which has since been proved [15, 16]) that $\mathbb{Q}$-curves are exactly the elliptic curves over number fields that are modular, in the sense of being a quotient of $J_1(N)$ for some N.

Torsion groups of $\mathbb{Q}$-curves over quadratic (and higher degree) fields have already been studied by Sairaiji and Yamauchi [29], but they imposed a number of additional conditions on their curves: the isogeny $\phi : E \to E^\sigma$ must be of squarefree degree and defined over the quadratic field and $j(E) \notin \mathbb{Q}$

Date: February 2, 2019.

2010 *Mathematics Subject Classification.* 11G05.

Key words and phrases. Elliptic curves, $\mathbb{Q}$-curves, torsion.

Le Fourn was supported by the European Union's Horizon 2020 research and programme under the Marie Sklodowska-Curie grant agreement No 793646, titled LowDegModCurve. Najman was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.

(here, as in the remainder of the paper, σ denotes the generator of $\mathrm{Gal}(K/\mathbb{Q})$). Moreover, they determine only the possible orders N of points in $E(K)_{tors}$, for a $\mathbb{Q}$-curve over a quadratic field K with the additional property that N is divisible by the degree of the isogeny $\phi : E \to E^\sigma$.

Throughout the paper $\mathcal{C}_n$ will denote a cyclic group of order n. Our main result is the following theorem.

Theorem 1.1. *Let E be a $\mathbb{Q}$-curve defined over a quadratic field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups*

$$\begin{aligned}
&\mathcal{C}_n, \text{ where } 1 \leq n \leq 18, \ n \neq 11, 17\\
&\mathcal{C}_2 \times \mathcal{C}_{2n}, \text{ where } n = 1, \ldots, 6,\\
&\mathcal{C}_3 \times \mathcal{C}_{3n}, \text{ where } n = 1, 2,\\
&\mathcal{C}_4 \times \mathcal{C}_4.
\end{aligned}$$

There are infinitely many $\mathbb{Q}$-curves with each of these torsion groups, except for $\mathcal{C}_{14}$ and $\mathcal{C}_{15}$ of which there are finitely many.

Remark 1.2. For a precise definition of what we mean by "finitely many" and "infinitely many", see Definition 1.

Proposition 3.2, Proposition 4.4 and Proposition 4.5, together with the results presented in Section 2 will prove Theorem 1.1.

The only group that can be a torsion group of any elliptic curve over a quadratic field, but *not* of a $\mathbb{Q}$-curve is $\mathcal{C}_{11}$. Note that some authors define $\mathbb{Q}$-curve to be curves without complex multiplication (CM). We will allow $\mathbb{Q}$-curves to have CM, although none of the results of the paper would be changed if we restricted to non-CM $\mathbb{Q}$-curves.

A surprising amount of different ingredients (which will be explained in detail in the next section), of which most are very recent, go into the proof of Theorem 1.1: the results of Sairaiji and Yamauchi about central $\mathbb{Q}$-curves [29]; classification of possible torsion groups of elliptic curves over quadratic fields that are base changes by Najman [25]; and of those with integral j-invariants by Müller, Ströher and Zimmer [24]; Le Fourn's results about the surjectivity of mod p Galois representations attached to quadratic $\mathbb{Q}$-curves and consequences on their reduction types [17]; the results of Bosman, Bruin, Dujella and Najman showing that all elliptic curves with $\mathcal{C}_{13}$, $\mathcal{C}_{16}$ and $\mathcal{C}_{18}$ torsion are $\mathbb{Q}$-curves [3] and Bars' results about which classical modular curves $X_0(n)$ have infinitely many quadratic points [2].

2. Definitions and useful results form other papers

Although it is probably clear to the reader what we mean by saying that there are finitely many $\mathbb{Q}$-curves with some torsion group "up to isomorphism", we give a rigorous definition below.

Definition 1. We say that there are finitely many elliptic curves over number fields of degree d with a property P, if there are finitely many pairs (E, K) with that property P up to isomorphism, where isomorphism means the following: a pair (E_1, K_1) with E_1/K_1 an elliptic curve is isomorphic to (E_2, K_2), where E_2/K_2 is an elliptic curve, if there exists an isomorphism of fields $\phi_1 : K_1 \to K_2$ and a K_2-isomorphism of elliptic curves $\phi_2 : \phi_1(E_1) \to E_2$. Here $\phi(E_1)/K_2$ is the elliptic curve obtained by taking a model of E_1 over K_1 and then mapping the coefficients of E_1 to K_2 via ϕ_1, thereby obtaining a model of $\phi(E_1)$ over K_2.

Definition 2. Let E be a $\mathbb{Q}$-curve, $\phi_\sigma : E \to E^\sigma$ be an isogeny of degree d_σ. We then say that E is a $\mathbb{Q}$-curve of degree d_σ. If d_σ is square-free, we say that E is a central $\mathbb{Q}$-curve.

Throughout the paper d_σ will always denote the degree of a $\mathbb{Q}$-curve, often without explicit mention.

The modular curve $X_0^+(N) = X_0(N)/w_N$ is a moduli space whose non-cuspidal points correspond to a set of two elliptic curves which are N-isogenous to each other. Points in $X_0^+(N)(\mathbb{Q})$ correspond to a pair of $\mathbb{Q}$-curves of degree N defined over a quadratic field. Quadratic central $\mathbb{Q}$-curves correspond to rational points on $X_0^+(N)$, where N is square free.

First, it is useful to know which groups can appear as torsion groups of all elliptic curves over quadratic fields.

Theorem 2.1. [13, 14] *Let E be an elliptic curve defined over a quadratic field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups*

$$\begin{aligned}&\mathcal{C}_n, \text{ where } n = 1, \ldots, \ldots 16, 18,\\ &\mathcal{C}_2 \times \mathcal{C}_{2n}, \text{ where } n = 1, \ldots, 6,\\ &\mathcal{C}_3 \times \mathcal{C}_{3n}, \text{ where } n = 1, 2,\\ &\mathcal{C}_4 \times \mathcal{C}_4.\end{aligned}$$

Remark 2.2. For all groups T in the list there exist infinitely many (up to isomorphism) pairs (E, K) such that $E(K)_{tors} \simeq T$.

The following theorem tells us which torsion groups are possible for elliptic curves with integral j-invariant over quadratic fields.

Theorem 2.3. [24, Theorem 4] *Let E be an elliptic curve with integral j-invariant over a quadratic field K. Then, up to isomorphism, the torsion group of E over K is one of the following groups*

$$\begin{aligned}&\mathcal{C}_n, \text{ where } n = 1, \ldots, \ldots 8, 10,\\ &\mathcal{C}_2 \times \mathcal{C}_{2n}, \text{ where } n = 1, 2, 3,\\ &\mathcal{C}_3 \times \mathcal{C}_3.\end{aligned}$$

To prove Theorem 1.1, we need to show:

1) That $\mathcal{C}_{11}$ does not appear as the torsion of a $\mathbb{Q}$-curve over a quadratic field.
2) That each group from Theorem 2.1 except $\mathcal{C}_{11}$ does appear as a torsion group of a $\mathbb{Q}$-curve, and determine whether it appears infinitely often.

The first place where one wants to start looking for $\mathbb{Q}$-curves is among elliptic curves defined over $\mathbb{Q}$.

Theorem 2.4. [25, Theorem 2] *Let E be an elliptic curve defined over $\mathbb{Q}$ and let K be a quadratic field. Then $E(K)_{tors}$ is isomorphic to one of the following groups*

$$\begin{aligned}&\mathcal{C}_n, \text{ where } n = 1, \ldots, 10, 12, 15, 16,\\ &\mathcal{C}_2 \times \mathcal{C}_{2n}, \text{ where } n = 1, \ldots, 6\\ &\mathcal{C}_3 \times \mathcal{C}_{3n}, \text{ where } n = 1, 2,\\ &\mathcal{C}_4 \times \mathcal{C}_4.\end{aligned}$$

For all groups T in the list, except for $\mathcal{C}_{15}$, there exist infinitely many (up to isomorphism) pairs (E, K), with $E/\mathbb{Q}$, such that $E(K)_{tors} \simeq T$. The elliptic curves with Cremona label 50b1 and 50a3 have 15-torsion over $\mathbb{Q}(\sqrt{5})$, and 50b2 and 450b4 have 15-torsion over $\mathbb{Q}(\sqrt{-15})$; these are the only elliptic curves defined over $\mathbb{Q}$ having non-trivial 15-torsion over any quadratic field.

Bosman, Bruin, Dujella and Najman [3, Theorem 4.1] proved that all elliptic curves over quadratic fields with torsion $\mathcal{C}_{13}$, $\mathcal{C}_{16}$ and $\mathcal{C}_{18}$ are $\mathbb{Q}$-curves. Moreover, in [5, Theorem 1.1.] it is shown that all elliptic curves with torsion $\mathcal{C}_{16}$ over quadratic fields are base changes of elliptic curves over $\mathbb{Q}$. Recall that there exist infinitely many elliptic curves with these torsion groups.

Combining these results, we see that all that remains is to show that $\mathcal{C}_{11}$ does not appear, that $\mathcal{C}_{14}$ does appear, but only finitely often, and that $\mathcal{C}_{15}$ appears finitely often.

The relationship between $\mathbb{Q}$-curves and central $\mathbb{Q}$-curves is nicely explained in the following proposition.

Proposition 2.5. [17, Proposition 1.3.] *For every $\mathbb{Q}$-curve E without CM defined over a number field K, there exists an isogeny $\psi : E \to E'$ towards a central $\mathbb{Q}$-curve E' defined over K such that the degree of ψ divides d_σ and is squarefree.*

Sairaji and Yamauchi proved the following result (which we specialize to quadratic fields) that we will find useful.

Theorem 2.6. [29, Proposition 3.4.] *Let E be a central $\mathbb{Q}$-curve of degree d_σ defined over a quadratic field K such that $j(E) \notin \mathbb{Q}$ with a point of prime order N in $E(K)$. If N divides d_σ, then N is either 2 or 3.*

We will also need the following result of Le Fourn.

Proposition 2.7. [17, Proposition 2.3] *Let K be a quadratic field and E/K a $\mathbb{Q}$-curve of degree d_σ. Let $p \geq 11$, $p \neq 13, 17, 41$, where p is a prime not dividing d_σ, such that the mod p Galois representation attached to E is reducible. Then E has potentially good reduction at all prime ideals of $\mathcal{O}_K$.*

We will make use of which modular curves $X_0(n)$ have infinitely many quadratic points when proving the finiteness of quadratic $\mathbb{Q}$-curves with $\mathcal{C}_{14}$ and $\mathcal{C}_{15}$ torsion.

Theorem 2.8. [2, Theorem 4.3] *If $X_0(n)$ is of genus ≥ 2 and has infinitely many quadratic points then n is one of the following values:*

$$22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 43, 46, 47, 48, 50, 53, 59, 61, 65, 71, 79, 83, 89, 101 \text{ or } 131.$$

3. There are no quadratic $\mathbb{Q}$-curves with $\mathcal{C}_{11}$ torsion.

Before proceeding with the proof of our results, we prove a general lemma that we will need.

Lemma 3.1. *Let F be a number field, let E_1, E_2 be elliptic curves both defined over F without complex multiplication, and suppose E_1 and E_2 are isogenous over $\overline{F}$. Then there exists a quadratic extension F'/F such that E_1 and E_2 are isogenous over F'.*

Proof. Let $f_1 \in \mathrm{Hom}(E_1, E_2)$ be an isogeny of degree n. We can suppose that f_1 is cyclic, as otherwise it would be a composition of multiplication-by-m for some m on E_1 and some cyclic isogeny. The absolute Galois group group $G_F := \mathrm{Gal}(\overline{F}/F)$ acts on $\mathrm{Hom}(E_1, E_2)$ and preserves the degree, i.e $\deg f_1^\sigma = n$ for all $\sigma \in G_F$.

Let $f_2 := f_1^\sigma$. As $\widehat{f_2} \circ f_1 \in \mathrm{End}\, E_1 = \mathbb{Z}$, it follows that $\widehat{f_2} \circ f_1 = [m]_{E_1}$ for some integer m. By taking degrees, we see that $m = n$ or $m = -n$. Since the dual isogeny is unique, we have $f_2 = f_1$ or $f_2 = [-1] \circ f_1$. Hence, we have a homomorphism from G_F into $\{\pm 1\}$. The kernel of this map is an index 2 subgroup of G_F, hence is $G_{F'}$ for some quadratic extension F'/F. It follows that f_1 is defined over F'. □

We first deal with the torsion group $\mathcal{C}_{11}$.

Proposition 3.2. *There does not exist a $\mathbb{Q}$-curve with torsion C_{11} over a quadratic field.*

Proof. Suppose such a curve, E/K exists, with $E(K)_{tors} \simeq C_{11}$, where E is a $\mathbb{Q}$-curve. The proof will proceed by proving a series of claims, of which each is used in the next. The strategy is to show that we can assume that E satisfies the assumptions of Theorem 2.6, which we then use to show that the curve satisfies the assumptions of Proposition 2.7, which we then use to prove the result.

Claim 1: E does not have complex multiplication.
This follows from [7, Section 4], as an elliptic curve with CM cannot have a point of order 11 over a quadratic field.

Claim 2: $j(E) \notin \mathbb{Q}$.
Suppose $j(E) \in \mathbb{Q}$. First note that if $j(E) \in \mathbb{Q}$, then it does not necessarily mean that E is a base change of an elliptic curve defined over $\mathbb{Q}$, but we do know that there exists an elliptic curve $E'/\mathbb{Q}$ such that $j(E) = j(E')$. Since, by Claim 1, $j(E) \neq 0$ or 1728, it follows that E' is a quadratic twist (over K) of E. So $E' = E^d$, for some square-free integer d. It follows that E^d has a point of order 11 over a quartic field (since E and E^d become isomorphic over $K(\sqrt{d})$), contradicting [11, Corollary 8.7.] or [19, Corollary 1.1.], proving the claim.

Claim 3: d_σ is coprime to 11.
If E was a central $\mathbb{Q}$-curve, then by Claim 2, it would satisfy the assumptions of Theorem 2.6, and hence prove the claim. Suppose E is not a central $\mathbb{Q}$-curve. Then, it is isogenous to a central $\mathbb{Q}$-curve E' by a degree $d|d_\sigma$ isogeny by Proposition 2.5. Note that the isogeny in question does not have to be defined over K, but this causes no problem because if E and E' are two curves defined over K which do not have complex multiplication and are isogenous over $\overline{K}$, then E is isogenous over K to a quadratic twist $(E')^d$ of E' by Lemma 3.1, and this quadratic twist is also a central $\mathbb{Q}$-curve. Thus, we can assume that E is K-isogenous to a central $\mathbb{Q}$-curve E' by an isogeny of degree $d|d_\sigma$.

We have the following isogeny diagram:

$$E \xrightarrow{\psi_1} E' \xrightarrow{\psi_2} (E')^\sigma \xrightarrow{\psi_3} E^\sigma.$$

We may assume all of these isogenies are defined over K after replacing by a twist if necessary. So, ψ_1 and ψ_3 which are both of the same degree d, and let ψ_2 be of degree d'. Then we have $d_\sigma = d^2 d'$.

If 11 does not divide d, $E'(K)$ has a point of order 11, and from Theorem 2.6, we see that 11 also does not divide d', so 11 does not divide d_σ.

Suppose 11 does divide d. But then E corresponds to a non-CM point in $X_0^+(N)(\mathbb{Q})$, where N is divisible by 121, contradicting [23, Theorem (0.1) (i)], proving the claim.

3.1. **Proof of the proposition.** By what we have proved, d_σ is coprime to 11. By Proposition 2.7, E has potentially good reduction at all primes of $\mathcal{O}_K$ since d_σ is coprime to 11 and the mod 11 representation is reducible. Let $\wp$ be the prime of K over 2.

Suppose E has good reduction at $\wp$. The residue field $k(\wp)$ of $\wp$ is either $\mathbb{F}_2$ or $\mathbb{F}_4$, and since $E(K)_{tors}$ injects into $E(k(\wp))$ (since $E(K)$ has no 2-torsion), we arrive to a contradiction with the Hasse bound.

We conclude that E has additive reduction at $\wp$. Denote by $\widetilde{E}$ the reduction of E mod $\wp$, i.e. the special fibre of the Néron model of E at $\wp$. Reduction mod $\wp : E(K) \to \widetilde{E}(k(\wp))$ is injective on the odd order torsion of $E(K)$, hence the image of the point $P \in E(K)$ of order 11 has order 11 in $\widetilde{E}(k(\wp))$. But by the Kodaira-Néron theorem [30, Theorem 6.1, p.200], $\widetilde{E}(k(\wp))$ is a product of the additive group of $k(\wp)$ and a group of order ≤ 4, which is a contradiction.

□

4. The finiteness of $\mathbb{Q}$-curves with $\mathcal{C}_{14}$ and $\mathcal{C}_{15}$

We first show that there exist only finitely many elliptic curves with $\mathcal{C}_{14}$ and $\mathcal{C}_{15}$ over quadratic fields with $j(E) \in \mathbb{Q}$.

Lemma 4.1. *There exist no elliptic curves with complex multiplication with torsion $\mathcal{C}_{14}$ and $\mathcal{C}_{15}$ over quadratic fields.*

Proof. This follows immediately from [7]. □

Lemma 4.2. [21, Lemma 5.5] *For each $j \in K$, there exist only finitely many elliptic curves E/K (up to K-isomorphism) with an odd order point and $j(E) = j$.*

Lemma 4.3. *There exist finitely many elliptic curves over quadratic fields E/K such that $j(E) \in \mathbb{Q}$ and such that $E(K)_{tors} \simeq \mathcal{C}_{15}$ and no such curves with $E(K)_{tors} \simeq \mathcal{C}_{14}$.*

Proof. Suppose that there exists an elliptic curve E/K over a quadratic field with $E(K)_{tors} \simeq \mathcal{C}_{14}$ and $j(E) \in \mathbb{Q}$. As in the proof of Claim 2 in the proof of Proposition 3.2, we can conclude that there exists a quadratic twist E^d of E such that E^d is defined over $\mathbb{Q}$ and $E^d(K(\sqrt{d}))$ contains $\mathcal{C}_{14}$. As E^d and E become isomorphic over a quadratic extension $K(\sqrt{d})$ of K, it follows that $E^d(K(\sqrt{d}))$ contains $\mathcal{C}_{14}$ as a subgroup. But this is impossible by [11, Corollary 8.7].

Let now E/K be an elliptic curve over a quadratic field with $E(K)_{tors} \simeq \mathcal{C}_{15}$ and $j(E) \in \mathbb{Q}$. Let E^d be a quadratic twist of E such that E^d is defined over $\mathbb{Q}$ and $E^d(K(\sqrt{d}))$ contains $\mathcal{C}_{15}$. Let $G(p)$ denote the image of the mod p representation attached to E^d.

From [11, Table 1], we see that if E^d gains a point of order 3 over a number field whose degree divides 4, then $G(3)$ is contained in either the Borel subgroup or the normalizer of the split Cartan subgroup. If E^d gains a point of order 5 over a number field whose degree divides 4, then $G(5)$ is contained in the Borel subgroup. So if $G(3)$ is contained in a Borel subgroup, then E^d has a 15-isogeny over $\mathbb{Q}$; there are only finitely many such j-invariants (see [20]), and hence only finitely many such curves by Lemma 4.2. If $G(3)$ is contained in the normalizer of the split Cartan subgroup, then E^d corresponds to a rational point on the modular curve $X(s3, b5)$ (using the notation of [10]) which is an elliptic curve of conductor 15 with finitely many points [10, Lemma 5.7].

It remains to prove that for each fixed j, there exist only finitely many quadratic fields K such that there exists an elliptic curve E/K with $j(E) = j$ and $E(K)_{tors} \simeq \mathcal{C}_{15}$. Suppose E/K is such a curve. Let $E_0/\mathbb{Q}$ be an elliptic curve with $j(E_0) = j$, and $E_0 = E^\delta$ for some $\delta \in K^\times$. If E_0 gains a 15-torsion point over a quadratic field, then by Theorem 2.4, E_0 is one of 4 curves with Cremona label $50b1$, $50a3$, $50b2$ or $450b4$ and K is either $\mathbb{Q}(\sqrt{5})$ or $\mathbb{Q}(\sqrt{-15})$. Suppose now E_0 is not one of those curves. Then E_0 gains a point of order 15 over $K(\sqrt{\delta})$, but not over a subfield of $K(\sqrt{\delta})$. This means that $K(\sqrt{\delta}) \subseteq \mathbb{Q}(E_0[15])$. But $\mathbb{Q}(E_0[15])$ is a number field, so has only finitely many quartic subfields. We conclude that there are finitely many quadratic fields K with our property (that there exists a curve E' with $j(E') = j$ and torsion $\mathcal{C}_{15}$ over K). Now for each such K, there exist only finitely many (up to K-isomorphism) elliptic curves with $j(E') = j$ with torsion $\mathcal{C}_{15}$ over K by Lemma 4.2, proving the lemma. □

From now until the end of this section, to avoid repetition, we suppose that all elliptic curves have $j(E) \notin \mathbb{Q}$. From this it follows that $d_\sigma \neq 1$, as $d_\sigma = 1$ would imply that $j(E) \in \mathbb{Q}$.

Proposition 4.4. *There exists finitely many $\mathbb{Q}$-curves E over quadratic fields K such that $E(K)_{tors} \simeq \mathcal{C}_{15}$.*

Proof. By Lemma 4.2 and Lemma 4.3, it is enough to show that there are finitely many quadratic j-invariants j such that there exists an elliptic curve E over a quadratic field K with $j(E) = j \in K \backslash \mathbb{Q}$ with torsion $E(K)_{tors} \simeq \mathcal{C}_{15}$ over K.

First suppose that E is a central $\mathbb{Q}$-curve. Then by [29, Theorem 1.2], it is not possible that $d_\sigma|15$. On the other hand, by Lemma A.3, there are finitely many central $\mathbb{Q}$-curves such that d_σ does not divide 15.

Suppose now that E is not a central $\mathbb{Q}$-curve. By Proposition 2.5, E is isogenous to a central $\mathbb{Q}$-curve E'.

If $E'(K)$ has a point of order 15 over K, by what we have shown, E' is one of finitely many such central $\mathbb{Q}$-curves. In each isogeny class over K there are finitely many elliptic curves, so we can conclude that there are finitely many curves E satisfying these assumptions.

If $E'(K)$ does not have a point of order 15, then there must exist an isogeny from E towards E' of degree 3 or 5 (or both). By using the same argumentation as in the proof of Proposition 3.2, we see that if the isogeny $\psi_1 : E \to E'$ is of degree d, then E has an isogeny of degree d^2. If 3 divides d, then E has both an 9-isogeny and a 5-isogeny, hence a 45-isogeny. On the other hand if 5 divides d, using the same argumentation, we see that E has a 75-isogeny. In both cases, there are only finitely many quadratic points on $X_0(45)$ and $X_0(75)$ by Theorem 2.8, so again there can be only finitely many curves E satisfying these conditions.

□

Proposition 4.5. *There exist finitely many $\mathbb{Q}$-curves E over quadratic fields K such that $E(K)_{tors} \simeq \mathcal{C}_{14}$.*

Proof. By Lemma 4.2 and Lemma 4.3, it is enough to show that there are finitely many quadratic j-invariants j such that there exists an elliptic curve E over a quadratic field K with $j(E) = j \in K\backslash\mathbb{Q}$ with torsion $E(K)_{tors} \simeq \mathcal{C}_{14}$ over K.

Let E be a central $\mathbb{Q}$-curve such that $d_\sigma|14$. First note that By Theorem 2.6, we have $d_\sigma = 2$. This means that E corresponds to a $\mathbb{Q}$-rational point on the curve $X = X_0(14)/w_2$. By [12, Appendix, p.29] we see that X is an elliptic curve. As X is 2-isogenous to $X_0(14)$, which has rank 0 over $\mathbb{Q}$, it follows that $X(\mathbb{Q})$ is finite.

Suppose now that E is a $\mathbb{Q}$-curve such that d_σ does not divide 14. By Lemma A.2 it follows that, with finitely many exceptions, E has potentially good reduction everywhere, and in particular the j-invariant is integral, giving a contradiction with Theorem 2.3.

Suppose now that E is not a central $\mathbb{Q}$-curve. By Proposition 2.5, E is isogenous to a central $\mathbb{Q}$-curve E'. We can suppose that E' does not have a 14-torsion point over K, for otherwise, by what we have already proved, E lies in one of finitely many isogeny classes containing a central $\mathbb{Q}$-curve with a point of order 14. We can see that there is an isogeny $E \to E'$ whose degree is divisible by 7; using the same argumentation as in the proof of Proposition 4.4, we see that E has a 49-isogeny. There are only finitely many quadratic points on $X_0(49)$ by Theorem 2.8, so we have that E is one of finitely many such curves.

□

Remark 4.6. In [29, p.467], the authors say in passing that the curve

$$y^2 + (2+\sqrt{-7})xy + (5+\sqrt{-7})y = x^3 + (5+\sqrt{-7})x^2$$

is the unique central $\mathbb{Q}$-curve over a quadratic field of degree dividing 14 with 14-torsion, but they give no proof of the claim.

ACKNOWLEDGEMENTS. We are grateful to the anonymous referee for his/her useful suggestions and careful review.

Appendix A. Integrality of j-invariants of $\mathbb{Q}$-curves with $\mathcal{C}_{14}$ and $\mathcal{C}_{15}$ torsion

The proofs of Propositions 4.4 and 4.5 require using Mazur's method to imply potentially good reduction for elliptic curves at (almost) all prime ideals. To be more precise, we will prove the following lemmas, which are needed in the proofs of Propositions 4.4 and 4.5.

Lemma A.1. *Let $n = 14$ or $n = 15$, K be a quadratic field and E a central $\mathbb{Q}$-curve without CM defined over K and of degree d not dividing n. We denote by E^σ the conjugate of E by the nontrivial automorphism σ of K, μ an isogeny from E to E^σ of degree d and C_d its kernel. Define $n' = n/(n,d)$ (always prime to d) and assume that E has a subgroup $C_{n'}$ of order n' defined over K, and that $C_{n'}^\sigma = \mu(C_{n'})$ as subgroups of E^σ. Then:*

- *If $n = 14$ then E has potentially good reduction at every prime ideal of K.*
- *If $n = 15$ then E has potentially good reduction at every prime ideal not dividing 2.*

Proof. Let E be an elliptic curve satisfying the hypotheses of the lemma. Let us first assume that d is prime to n, hence $n' = n$. The Atkin-Lehner involution w_d acts on the noncuspidal points of $X_0(dn)$ by

$$w_d(E, C_d, C_n) = (E/C_d, E[d]/C_d, (C_n + C_d)/C_d),$$

and by hypothesis one has $P^\sigma = w_d \cdot P$ for the point $P = (E, C_d, C_n)$ coming from our choice of elliptic curve. Let us then define $\pi : X_0(dn) \to X_0(n)$ to be the natural degeneracy morphism, and $f = \pi + \pi \circ w_d$, so that $f(P)$ is clearly a rational point on $X_0(n)$.

Now, by classical arguments (see the complex case, or more precisely look at the q-expansions at the cusps), the degeneracy morphism $X_0(d) \to X(1)$ is a formal immersion for all prime ideals at the cusp $\infty \in X_0(d)$ and ramified at every other cusp, and this holds similarly for π: amongst the cusps of $X_0(dn)$ above $\infty \in X_0(n)$, the morphism π is a formal immersion at $\infty \in X_0(dn)$ and ramified at the other cusps. Consequently, f is a formal immersion at the cusp $\infty \in X_0(dn)$ for all prime ideals.

Now, let us assume that the point P associated to our $\mathbb{Q}$-curve reduces to a cusp at some prime λ dividing the prime number $\ell > 2$. As the Atkin-Lehner involutions act transitively on the cusps because dn is squarefree, we can assume that P reduces to the cusp ∞ modulo λ (in particular, its reduction lands in the smooth part of the Néron model of $X_0(dn)$), and it does not change the fact that $w_d \cdot P = P^\sigma$ as the Atkin-Lehner involutions acts through an abelian group and are defined over $\mathbb{Q}$. Now, f is a formal immersion at ∞, sends P to a rational point, and the group of rational points of $X_0(n)$ is finite. One can thus apply Raynaud's lemma in the form given in [17, Proposition 2.4] as $1 < \ell - 1$, and P must be equal to ∞ which is obviously a contradiction. Therefore, E has potentially good reduction at all prime ideals of $\mathcal{O}_K$ not above 2.

Let us now consider the case where the prime ideal λ is above $\ell = 2$. Following step by step the previous argument is straightforward up to the moment we apply [17, Proposition 2.4]. In this case, for $\ell = 2$, $1 = \ell - 1$ therefore one needs to know that $f(P)$ does not generate a subgroup scheme μ_2 over $\mathbb{Z}_2$, i.e. it is not a point or order 2 reducing to 0 modulo 2. The modular curve $X_0(14)(\mathbb{Q})$ is 14a6 in the LMFDB [18], $X_0(14)(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$, and we readily check that the unique point of order 2 does not reduce to 0 in the reduction modulo 2 of this elliptic curve (which is nonsplit multiplicative in this case). Therefore, we can again apply [17, Proposition 2.4], which completes the proof for all prime ideals in the case $n = 14$.

Assume now that $(d, n) \neq 1$ (recall we have assumed that d does not divide n therefore n' is a prime number). By the hypothesis and with the notations of the Lemma, the triple $(E, C_d, C_{n'})$ defines a quadratic point P on $X_0(dn')$ (which is of squarefree level by construction), which furthermore satisfies

$$P^\sigma = w_d \cdot P.$$

We define the morphism $\pi : X_0(dn') \to X_0(n)$ as the natural degeneracy morphism which functorially sends a triple $(E, C_d, C_{n'})$ to the unique cyclic subgroup of order n of $C_d + C_{n'}$, and again we define $f = \pi + \pi \circ w_d$. The degeneracy morphism $X_0(d) \to X(1)$ is again ramified at all cusps except ∞, and a formal immersion at ∞ for all primes. Let us now assume that E has potentially bad reduction at some prime ideal λ of $\mathcal{O}_K$. One can again use the Atkin-Lehner involutions to assume that P reduces to the pole $\infty \in X_0(dn')$. Now, the morphism π is ramified at the image of this pole by w_d. Indeed, writing $d' = d/(n,d)$, cusps of $X_0(dn')$ can be seen as triples of cusps of respectively $X_0(d'), X_0((n,d)), X_0(n')$ in a way compatible with the action of Atkin-Lehner involutions $w_{d'}, w_{(n/d)}, w_{n'}$ (this can be worked out straightforwardly from the definitions of Atkin-Lehner involutions, e.g. [1, Lemma 9], the levels here being squarefree). In particular, $w_d \cdot (\infty, \infty, \infty) = (0, 0, \infty)$ and π sends $(0, 0, \infty)$ to $(0, \infty)$, whence it is ramified at this point (as $X_0(d') \to X(1)$ is ramified at 0). It is, as before, a formal immersion at ∞ for the λ, so we again have that f is a formal immersion at the cusp $\infty \in X_0(dn')$ (it works even though the images of $\pi(\infty)$ and $\pi(w_d(\infty))$ are not the same by a straightforward computation of the differential), and can reproduce the argument above word for word, which concludes the proof of the Lemma. □

To apply Lemma A.1 to the proofs of Propositions 4.4 and 4.5 we still need to show that we can suppose that $C_{n'}^\sigma = \mu(C_{n'})$ in the sense that there will be finitely many $\mathbb{Q}$-curves that do not satisfy these assumptions.

Lemma A.2. *Let all the assumptions be as in Lemma A.1, except we do not assume that $C_{n'}^\sigma = \mu(C_{n'})$. Then for all but finitely many such $\mathbb{Q}$-curves, the following is true:*

- *If $n = 14$ then E has potentially good reduction at every prime ideal of K.*
- *If $n = 15$ then E has potentially good reduction at every prime ideal not dividing 2.*

Proof. Assume that E is a central $\mathbb{Q}$-curve of degree d, defined over K quadratic and admitting a point of order $n = 14$ or 15 over K. We define μ to be the isogeny of degree d from E to its conjugate. By assumption d does not divide n, so $(n, d) \in \{1, 2, 3, 5, 7\}$.

Let us first assume that $(n, d) \neq 1$ so that n' is prime. Let C_n be the cyclic subgroup of order n generated by a n-torsion point, and $C_{n'}$ its n'-torsion subgroup. As d is prime to n', $\widehat{\mu}(C_{n'}^\sigma)$ is a subgroup of order n' of E defined over K, and if it is not $C_{n'}$, the elliptic curve E is thus endowed with two distinct subgroups of order n' and one subgroup of order n/n', all defined over K, from which we obtain a point of $X_0(nn')$. Such a modular curve has only finitely many quadratic points unless $n = 14$ and $n' = 2$ by Theorem 2.8, but this implies that there is a point of order 7 on the $\mathbb{Q}$-curve, which is impossible by Theorem 2.6 (note that one can suppose $j(E) \notin \mathbb{Q}$ by Lemma 4.3).

Consider now the case $(d, n) = 1$. The previous argument holds up until considering the possibility that $\widehat{\mu}(C_n^\sigma) \neq C_n$. In this case, E is endowed with an additional k-subgroup for a prime number k dividing n, which defines (after possibly considering an isogenous elliptic curve) a quadratic point of $X_0(kn)$ where $kn \in \{28, 49, 45, 75, 196, 225\}$. For all cases but the first, there are only finitely many quadratic points on those curves by Theorem 2.8. In the first case, it follows from [4] that, up to finitely many exceptions, the quadratic points of $X_0(28)$ correspond to $\mathbb{Q}$-curves of degree 7, which cannot happen here as we assumed $(d, n) = 1$.

□

Unfortunately, one cannot apply Lemma A.2 to prove Proposition 4.4 directly, as there exists the issue of the j-invariant possibly not being integral at the primes above 2. For $n = 15$, the group of rational points of $X_0(n)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the reduction modulo 2 is good, and there *is* one point generating a μ_2: in the LMFDB database, a Weierstrass equation for $X_0(15)$ is given by the elliptic curve defined by the affine equation

$$y^2 + xy + y = x^3 + x^2 - 10x - 10,$$

and this point is then given by the coordinates $(-13/4, 9/8)$. A natural workaround would be to use here the strengthened hypothesis that there is a point of order 15 defined over K, not merely a subgroup (hence to argue with $X_1(15)$ instead of $X_0(15)$). The problem is that it does not behave that well with respect to the structure of $\mathbb{Q}$-curves, in particular there does not seem to be a clear general way to define a morphism $X_0(d) \times X_1(n) \to X_1(n)$ which sends our point associated to E to a rational point and is a formal immersion at the cusp ∞ at the same time.

After some time of reflection, we could not come to an argument making use of an additional property of P (relatively to more general quadratic points of $X_1(n)$) to ensure that $f(P)$ is not this point. We instead settle this case by applying Runge's method.

Lemma A.3. *There exist finitely many central $\mathbb{Q}$-curves E over quadratic fields, without CM, with a point of order 15 and of degree d not dividing 15.*

Proof. Let E/K be such a curve, where K is a quadratic field. Notice that E must be semistable because it has a point of order 15 defined over K, hence it has good reduction at every prime ideal not dividing 2 by Lemma A.2. Consider the set of places S of K made up of the infinite places and the places above 2, so that E defines an $\mathcal{O}_{K,S}$-integral point of $X_1(15)$. Clearly, $|S| < 5$, which is less than the number of orbits of cusps of $X_1(15)$ by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (hence $\mathrm{Gal}(\overline{K}/K)$).

This allows us to apply Runge's method to our integral point, and thus get an *absolute* bound on the height of its j-invariant - see [6, Theorem 1.2] for details. In particular, there are only finitely many such elliptic curves, which is what we wanted to prove. □

References

[1] A. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(m)$* Math. Ann., **185** (1970), 134–160. A

[2] F. Bars, *Bielliptic modular curves,* J. Number Theory, **76** (1999), 154–165. 1, 2.8

[3] J. G. Bosman, P. J. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Notices 2014 (2014), 2885–2923. 1, 2

[4] P. Bruin and F. Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), 578–602. A

[5] P. Bruin and F. Najman, *Fields of definition of elliptic curves with prescribed torsion*, Acta Arith. **181** (2017), 85–95. 2

[6] Y. Bilu and P. Parent, *Runge's method and modular curves* Int. Math. Res. Not. IMRN **9** (2011), 1997–2027. A

[7] P. L. Clark, P. Corn, A. Rice, J. Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), 509–539. 1, 3, 4

[8] L. Dieulefait and J. J. Urroz, *Solving Fermat-type equations via modular $\mathbb{Q}$-curves over polyquadratic fields*, J. Reine Angew. Math. **633** (2009), 183–195. 1

[9] J. S. Ellenberg and C. Skinner, *On the modularity of $\mathbb{Q}$-curves*, Duke Math. J. **109** (2001), 97–122.

[10] N. Freitas, B. V. Le Hung and S. Siksek, *Elliptic Curves over Real Quadratic Fields are Modular*, Invent. Math. **201** (2015), 159–206. 4

[11] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, preprint. 3, 4

[12] J. González and J-C. Lario, *Rational and elliptic parametrizations of Q-curves*, J. Number Theory **72** (1998), 13–31. 4

[13] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229. 1, 2.1

[14] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. 1, 2.1

[15] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. **178** (2009), 485-–504. 1

[16] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), 505-–586. 1

[17] S. Le Fourn, *Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves,* Math. Ann. **365** (2016), 173–214. 1, 2.5, 2.7, A

[18] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, `http://www.lmfdb.org`, 2013, [Online; accessed 10 October 2018]. A

[19] A. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals,* Math. Ann. **357** (2013), 279–305. 3

[20] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), pp. 129–162. 1, 4
[21] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575. 4.2
[22] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449. 1
[23] F. Momose, *Rational points on the modular curves $X_0^+(N)$*, J. Math. Soc. Japan, **39** (1987), 269-286. 3
[24] H. H. Müller, H. Ströher and H. G. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over quadratic fields,* J. reine angew. Math. **397** (1989), 100–161. 1, 1, 2.3
[25] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$,* Math. Res. Letters **23** (2016) 245–272. 1, 1, 2.4
[26] F. Najman, *Isogenies of non-CM elliptic curves with rational j-invariants over number fields,* Math. Proc. Cambridge Philos. Soc. **164** (2018), 179–184. 1
[27] J. Pila, *On a modular Fermat equation*, Comment. Math. Helv. **92** (2017), 85–103. 1
[28] K. A. Ribet, *Abelian Varieties over $\mathbb{Q}$ and Modular Forms*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser Basel, 2004, 241–261. 1
[29] F. Sairaiji and T. Yamauchi, *On rational torsion points of central $\mathbb{Q}$-curves,* J. Théor. Nombres Bordeaux, **20** (2008),465–483. 1, 1, 2.6, 4, 4.6
[30] J. H. Silverman, Arithmetic of elliptic curves, Second Edition, Springer-Verlag, New York, 2009. 3.1

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom.
Email address: Samuel.Le-Fourn@warwick.ac.uk

University of Zagreb, Faculty of Science, Department of Mathematics, Bijenička cesta 30, 10000 Zagreb, Croatia
Email address: fnajman@math.hr