$\mathbb{Q}$-CURVES OVER ODD DEGREE NUMBER FIELDS

J. E. CREMONA AND FILIP NAJMAN

Abstract. By reformulating and extending results of Elkies, we prove some results on $\mathbb{Q}$-curves over number fields of odd degree. We show that, over such fields, the only prime isogeny degrees ℓ which an elliptic curve without CM may have are those degrees which are already possible over $\mathbb{Q}$ itself (in particular, $\ell \leq 37$), and we show the existence of a bound on the degrees of cyclic isogenies between $\mathbb{Q}$-curves depending only on the degree of the field. We also prove that the only possible torsion groups of $\mathbb{Q}$-curves over number fields of degree not divisible by a prime $\ell \leq 7$ are the 15 groups that appear as torsion groups of elliptic curves over $\mathbb{Q}$. Complementing these theoretical results we give an algorithm for establishing whether any given elliptic curve E is a $\mathbb{Q}$-curve, which involves working only over $\mathbb{Q}(j(E))$.

1. Introduction

In the study of elliptic curves over number fields, $\mathbb{Q}$-curves are of special interest. An elliptic curve is called a $\mathbb{Q}$-*curve* if it is isogenous to all of its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugates. Here and throughout the paper "isogenous", when said without specifying the field, will always mean isogenous over $\overline{\mathbb{Q}}$.

This property is obviously satisfied by all elliptic curves defined over $\mathbb{Q}$, and more generally all elliptic curves with rational j-invariants; also, all curves with complex multiplication (CM) are $\mathbb{Q}$-curves. The property of being a $\mathbb{Q}$-curve is preserved under isogeny, and $\mathbb{Q}$-curves not isogenous to an elliptic curve with rational j-invariant are called *strict* $\mathbb{Q}$-curves. Thus, $\mathbb{Q}$-curves can be thought of as generalizations of elliptic curves defined over $\mathbb{Q}$ (or, more generally, elliptic curves with rational j-invariants). Moreover, Ribet proved in [37] (assuming Serre's conjecture, which has since been proved [21, 22]) that $\mathbb{Q}$-curves are exactly the elliptic curves over number fields that are modular, in the sense of being quotients of $J_1(N)$ for some N.

As can be seen from [14] and as will be later explained in more detail, $\mathbb{Q}$-curves in a sense most naturally "exist" over number fields of degree 2^n. In particular, the first place one looks for $\mathbb{Q}$-curves which are not just elliptic curves defined over $\mathbb{Q}$, are among those defined over quadratic fields. Already, over quadratic fields, there is a plethora of results showing that $\mathbb{Q}$-curves have certain special properties, of which we list some examples. Le Fourn [24] showed that for every strict $\mathbb{Q}$-curve E over a fixed quadratic imaginary quadratic field K, there exists a uniform bound C_K such that for $\ell > K$, the mod ℓ representation attached to E is surjective. Bruin and Najman [12] and Box [11] show that for all N such that the modular curve $X_0(N)$ is hyperelliptic, for all but finitely many explicitly listed exceptions, an elliptic curve over a quadratic field with an N-isogeny is a $\mathbb{Q}$-curve. Bosman, Bruin, Dujella and Najman [7] showed that all elliptic curves with $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$-torsion over quadratic fields are again $\mathbb{Q}$-curves. Le Fourn and Najman [24] determined all the possible torsion groups of $\mathbb{Q}$-curves over quadratic fields.

The main purpose of this paper is to expand on the existing theory of $\mathbb{Q}$-curves and study their properties, especially over odd degree number fields. To this end, we reformulated and expanded on the work of Elkies [14] concerning $\mathbb{Q}$-curves and their generalisations. A summary of the definitions and results about properties of $\mathbb{Q}$-curves obtained by this reformulation can be found in Section 2, with detailed proofs in the Appendix. A key result here (Theorem 2.6) is that every non-CM $\mathbb{Q}$-curve E defined over a number field K is isogenous over K to a *central* $\mathbb{Q}$-curve defined over a polyquadratic subfield of K. This result is established through the concept of the *core* of the isogeny class of a $\mathbb{Q}$-curve, which is defined over a polyquadratic field. We thereby obtain the main new results in this section, Theorem 2.4 and Theorem 2.5, which state that $\mathbb{Q}$-curves defined over number fields of odd degree, or without quadratic subfields, are always isogenous to elliptic curves defined over $\mathbb{Q}$.

In Section 3 we study the possible degrees of isogenies of $\mathbb{Q}$-curves over odd degree number fields. Theorem 2.4 allows us to bound both the degree of the isogeny and the size of the torsion group of a $\mathbb{Q}$-curve over an odd degree number field. These results fit into the long-standing program, initiated by Mazur's torsion and isogeny theorems [30, 31], of describing the possible torsion groups and isogeny structures of elliptic curves

Date: August 26, 2020.

over number fields. We will obtain bounds on degrees of isogenies depending only on the degree of the fields, which is reminiscent of Merel's uniform boundedness theorem [32].

In Section 3 we obtain the following results.

Theorem 1.1. *Let E be $\mathbb{Q}$-curve without complex multiplication defined over an odd degree number field K. Then*

a) *If E has a K-rational isogeny of prime degree ℓ, then $\ell \in \{2, 3, 5, 7, 11, 13, 17, 37\}$.*
b) *If $d = [K : \mathbb{Q}]$ is not divisible by any prime $\ell \in \{2, 3, 5, 7, 11, 13, 17, 37\}$, and E has a cyclic isogeny of degree n, then $n \leq 37$.*

However, we can show that over odd degree number fields there exists a uniform bound, depending only on the degree of the number field, on the degree of isogenies of all $\mathbb{Q}$-curves, including those with CM.

Theorem 1.2. *For every odd positive integer d, there exists a bound C_d depending only on d such that all cyclic isogenies of all $\mathbb{Q}$-curves over all number fields of degree d are of degree at most C_d.*

By Theorem 2.4, for elliptic curves without CM, our problem is equivalent to studying isogenies of elliptic curves E with $j(E) \in \mathbb{Q}$ over odd degree number fields. Isogenies of elliptic curves E with $j(E) \in \mathbb{Q}$ without CM have been studied by Najman in [34], but over general number fields. As we will see, if one restricts to odd degree number fields, we get much sharper results. In [35], Propp also studied the degrees of extensions over which an elliptic curve with $j(E) \in \mathbb{Q}$ have certain kinds of Galois images.

In Section 4, we study the possible torsion groups of elliptic curves over odd degree number fields. While studying torsion groups of $\mathbb{Q}$-curves over number fields of prime degree, we will not need to restrict to elliptic curves with CM. Our main result in Section 4 is the following theorem.

Theorem 1.3. *Let d be a prime > 7, let K be a number field of degree d and E/K a $\mathbb{Q}$-curve. Then $E(K)_{\mathrm{tors}}$ is one of the groups from Mazur's theorem (listed in (4.1)), i.e. a torsion group of an elliptic curve over $\mathbb{Q}$.*

Since elliptic curves with rational j-invariants are $\mathbb{Q}$-curves, these theorems apply to all such curves.

In Section 5 we address the question of how to test a given elliptic curve E defined over a number field K for the property of being a $\mathbb{Q}$-curve. Using the results of Section 2 proved in the Appendix, we are able to give an algorithm which solves this problem without needing to extend the base field (for example, to the Galois closure of K). We assume that we can detect CM, and compute the complete K-isogeny class of any elliptic curve defined over a number field K, both of which are already implemented in `SageMath`[38], the former also in `Magma`[29]. One special case we establish (see Theorem 2.7) is that, if E does not have CM and K has no quadratic subfields, then E is a $\mathbb{Q}$-curve if and only if it is isogenous over K to a curve with rational j-invariant. We have implemented this algorithm in `SageMath` and used it to establish which of the curves in the LMFDB database (see [28]), which (as of August 2020) are defined over fields of degree at most 6, are $\mathbb{Q}$-curves.

Acknowledgments. We thank Samuel Le Fourn for helpful conversations and suggestions. The first-named author was supported by the Heilbronn Institute for Mathematical Research. The second-named author 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.

2. Properties of $\mathbb{Q}$-curves

We recall here the definition of a $\mathbb{Q}$-curve and various related concepts. Proofs of all the properties stated in this section are given in the Appendix.

Let $\overline{\mathbb{Q}}$ be the field of algebraic numbers, and $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A $\mathbb{Q}$-*curve* is an elliptic curve E defined over $\overline{\mathbb{Q}}$ such that E is isogenous (over $\overline{\mathbb{Q}}$) to all its Galois conjugates. A $\mathbb{Q}$-*number* is an algebraic number j which is the j-invariant of a $\mathbb{Q}$-curve. If j is a $\mathbb{Q}$-number then so are all its Galois conjugates (see Proposition A.10). All CM curves are $\mathbb{Q}$-curves; however, here we will mainly be interested in non-CM $\mathbb{Q}$-curves.

Two algebraic numbers j_1, j_2 are *isogenous* if there are two isogenous elliptic curves E_i defined over $\overline{\mathbb{Q}}$ with $j(E_i) = j_i$, in which case every pair of elliptic curves with these j-invariants are isogenous over $\overline{\mathbb{Q}}$. Isogeny is an equivalence relation on $\overline{\mathbb{Q}}$. If j_1 and j_2 are isogenous and not CM, then there is a unique positive integer d which is the degree of a *cyclic* isogeny $E_1 \to E_2$, where again $j(E_i) = j_i$, denoted $d(j_1, j_2)$ (see Lemma A.1).

A $\mathbb{Q}$-*class* is an isogeny class $\mathcal{Q} \subset \overline{\mathbb{Q}}$ consisting of $\mathbb{Q}$-numbers. The *degree* of a $\mathbb{Q}$-number j is the least common multiple of the degrees $d(j, g(j))$ for $g \in G_{\mathbb{Q}}$. A $\mathbb{Q}$-number is *central* if it has square-free degree, in which case its Galois conjugacy class is called a *central class*. The existence of a central class in every $\mathbb{Q}$-class is established in Theorem A.18, and in Theorem A.14 and Proposition A.19 we prove the other assertions of the following theorem:

Theorem 2.1. *Let $\mathcal{Q}$ be a non-CM $\mathbb{Q}$-class in $\overline{\mathbb{Q}}$. Then $\mathcal{Q}$ contains at least one central class, and each central class C in $\mathcal{Q}$ satisfies the following properties:*

1. *$|C| = 2^\rho$ for some $\rho \geq 0$;*
2. *$\mathbb{Q}(C)$ is a polyquadratic field with $\mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^\rho$;*
3. *the square-free degree N of one (and hence all) $j \in C$ has r prime factors, where $r \geq \rho$ and $r = 0 \iff \rho = 0$.*

The quantities N, r and ρ, and the central field $\mathbb{Q}(C)$, are the same for each central class in $\mathcal{Q}$.

We denote the integers N, r, and ρ attached to any central class C in the $\mathbb{Q}$-class $\mathcal{Q}$ by $N(\mathcal{Q})$, $r(\mathcal{Q})$ and $\rho(\mathcal{Q})$; similarly, the central polyquadratic field $\mathbb{Q}(C)$ of degree 2^ρ is denoted $L_{\mathcal{Q}}$. We call $N(\mathcal{Q})$ the *level* of the $\mathbb{Q}$-class $\mathcal{Q}$. The set of degrees of the isogenies between elements of each central class C in $\mathcal{Q}$ has size $2^{\rho(\mathcal{Q})}$, and forms a subgroup under multiplication modulo squares of the group of all $2^{r(\mathcal{Q})}$ divisors of $N(\mathcal{Q})$.

By applying Atkin-Lehner involutions (see Appendix A.1.3) to the isogenies between elements of a central class C we obtain a *core* of the $\mathcal{Q}$-class. This has cardinality $2^{r(\mathcal{Q})}$ and consists of $2^{r(\mathcal{Q})-\rho(\mathcal{Q})}$ disjoint central classes. The degrees of the isogenies between elements of the core are all $2^{r(\mathcal{Q})}$ divisors of the level.

Note that when we refer to the degree of algebraic numbers j in the remainder of this section, we mean the usual degree of the extension $\mathbb{Q}(j)/\mathbb{Q}$, and not its degree as a $\mathbb{Q}$-number j (defined above).

Proposition 2.2. *Let j be a $\mathbb{Q}$-number in the $\mathbb{Q}$-class $\mathcal{Q}$. Then $L_{\mathcal{Q}} \subseteq \mathbb{Q}(j)$, and the degree of the field $\mathbb{Q}(j)$ is divisible by $2^{\rho(\mathcal{Q})}$.*

Proof. The inclusion $L_{\mathcal{Q}} \subseteq \mathbb{Q}(j)$ is part of Theorem A.14, and $L_{\mathcal{Q}}$ has degree $2^{\rho(\mathcal{Q})}$. □

Proposition 2.3. *For a $\mathbb{Q}$-class $\mathcal{Q}$, the following are equivalent:*

1. *$r(\mathcal{Q}) = 0$;*
2. *$\rho(\mathcal{Q}) = 0$;*
3. *$N(\mathcal{Q}) = 1$;*
4. *$L_{\mathcal{Q}} = \mathbb{Q}$;*
5. *$\mathcal{Q} \cap \mathbb{Q} \neq \emptyset$.*

Proof. The first four are equivalent by Theorem 2.1, and the last by Proposition 2.2. □

A $\mathbb{Q}$-class is called *rational* when it satisfies these conditions.

Theorem 2.4 (The odd degree theorem)**.** *If the non-CM $\mathbb{Q}$-class $\mathcal{Q}$ contains an element j such that $\mathbb{Q}(j)$ has odd degree, then $\mathcal{Q}$ is rational.*

Proof. $[\mathbb{Q}(j) : \mathbb{Q}]$ is an odd multiple of $2^{\rho(\mathcal{Q})}$ by Proposition 2.2, so $\rho(\mathcal{Q}) = 0$. □

Remark. The assumption in Theorem 2.4 that $\mathcal{Q}$ does not have CM is necessary, as any elliptic curve E with $\mathrm{End}\, E = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, for $p \equiv 3 \pmod 4$ and $p > 163$, will be defined over a number field of odd degree, will not be isogenous to an elliptic curve over $\mathbb{Q}$, and will have a p-isogeny over its field of definition (the endomorphism $\sqrt{-p}$).

More generally:

Theorem 2.5 (The no-quadratic-subfields theorem)**.** *If the $\mathbb{Q}$-class $\mathcal{Q}$ contains an element j such that $\mathbb{Q}(j)$ has no quadratic subfields, then $\mathcal{Q}$ is rational.*

Proof. If $\rho(\mathcal{Q}) \geq 1$ then $L_{\mathcal{Q}}$ has a quadratic subfield, hence so does $\mathbb{Q}(j)$, by Proposition 2.2. □

A non-CM $\mathbb{Q}$-curve E is *central* if its j-invariant is central; that is, if the least common multiple of the degrees of the cyclic isogenies between E and its Galois conjugates is squarefree. By Theorem 2.1, the j-invariant of a central $\mathbb{Q}$-curve is always of degree a power of 2, and the field $\mathbb{Q}(j)$ is polyquadratic. In the simplest case of a rational $\mathbb{Q}$-class, the central j-invariants are actually rational, so the corresponding elliptic curves are quadratic twists of curves defined over $\mathbb{Q}$.

In the Appendix, we show that, for every $\mathbb{Q}$-curve E defined over a number field K, the K-isogeny class of E itself contains a central $\mathbb{Q}$-curve (see Corollary A.20). This will enable us to show whether or not an elliptic curve is a $\mathbb{Q}$-curve without needing to extend the base field; this is important algorithmically.

Theorem 2.6. *Let K be a number field and let E be a non-CM $\mathbb{Q}$-curve defined over K. Then there exists a central $\mathbb{Q}$-curve E_0 with an isogeny $\phi : E \to E_0$, where both E_0 and ϕ are also defined over K.*

The following are immediate consequences.

Theorem 2.7. *Let E be a non-CM $\mathbb{Q}$-curve defined over a number field K. If either $\mathbb{Q}(j(E))$ has odd degree, or more generally if $\mathbb{Q}(j(E))$ has no quadratic subfields, then E is isogenous over K to an elliptic curve with rational j-invariant.*

Corollary 2.8. *Let E be a non-CM $\mathbb{Q}$-curve defined over a number field K. If $\mathbb{Q}(j(E))$ has degree 4, with Galois closure of isomorphic to either S_4 or A_4, then E is isogenous over K to an elliptic curve with rational j-invariant.*

Proof. The one-point stabilisers in both S_4 and A_4 have index 4 but are maximal, so $\mathbb{Q}(j(E))$ has no quadratic subfields. □

3. Application 1: isogenies of $\mathbb{Q}$-curves over odd fields

Let K be a number field and $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ its absolute Galois group. Let E/K be an elliptic curve, $P \in E[\ell]$ be a point of order ℓ and $C = \langle P \rangle$ be the subgroup of E generated by P. We define $K(P)$ to be the field obtained by adjoining the coordinates of P to K and $K(C)$ to be smallest extension of K such that the ℓ-isogeny ϕ with kernel C is defined over K, or in other words, the smallest number field such that $\mathrm{Gal}(\overline{K(C)}/K(C))$ acts on C. Now $K(C)$ and $K(P)$ lie in a tower of extensions of number fields $K(E[\ell])/K(P)/K(C)/K$.

Let $\{P, R\}$ be a basis of $E[p]$ and define $\overline{\rho}_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ to be the mod ℓ representation attached to E with respect to the basis $\{P, R\}$, and $\mathbb{P}\overline{\rho}_{E,\ell}$ to be the associated projective representation. Let B denote the Borel subgroup $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ of $\mathrm{GL}_2(\mathbb{F}_\ell)$, which has index $\ell+1$, and let B_1 denote the subgroup $\{\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)\}$, which is normal of index $\ell - 1$ in B. Then

a) $K(C)$ is the fixed field of $B \cap \overline{\rho}_{E,\ell}(G_K) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$;
b) $K(P)$ is the fixed field of $B_1 \cap \overline{\rho}_{E,\ell}(G_K) \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$.

The isogeny with kernel C is defined over K if and only if $K(C) = K$; that is, if and only if $\overline{\rho}_{E,\ell}(G_K) \subseteq B$. We say that the prime ℓ is *reducible* for E/K if $\overline{\rho}_{E,\ell}(G_K)$ is contained in a Borel subgroup, that is, if the representation $\overline{\rho}_{E,\ell}$, or equivalently the projective representation $\mathbb{P}\overline{\rho}_{E,\ell}$, is reducible. Note that the projective representation is unchanged under quadratic twist; hence the set of reducible primes only depends on the j-invariant of E, provided that $j(E) \neq 0, 1728$.

In general, we have the following.

Lemma 3.1. *$[K(P) : K(C)]$ divides $\ell - 1$, and $[K(C) : K] \leq \ell + 1$.*

Proof. By Galois theory, $[K(P) : K(C)] = [B \cap \overline{\rho}_{E,\ell}(G_K) : B_1 \cap \overline{\rho}_{E,\ell}(G_K)]$, which divides $[B : B_1] = \ell - 1$. Similarly, $[K(C) : K] = [\overline{\rho}_{E,\ell}(G_K) : B \cap \overline{\rho}_{E,\ell}(G_K)] \leq \ell + 1$. □

The set of reducible primes is invariant under isogeny:

Proposition 3.2. *Let E_1 and E_2 be elliptic curves defined over the number field K which are isogenous over K. Then E_1 and E_2 have the same sets of reducible primes: that is, E_1 has an ℓ-isogeny defined over K if and only if E_2 does.*

Proof. By Proposition A.7 we may assume that the given isogeny $\phi : E_1 \to E_2$ has prime degree p. Since the dual isogeny has the same degree, p is reducible for both curves. Let ℓ be a prime not equal to p which is reducible for E_1/K. Then E_1 has a cyclic subgroup C of order ℓ defined over K, and $\phi(C)$ is a subgroup of E_2 also defined over K and of order ℓ, since the kernel of ϕ has order coprime to ℓ. □

Apart from small primes ℓ, elliptic curves over $\mathbb{Q}$ cannot acquire ℓ-isogenies over extensions of odd degree.

Proposition 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve without CM, and $\ell \neq 2, 7$ be a prime such that E has no ℓ-isogenies defined over $\mathbb{Q}$. Then all ℓ-isogenies of E are defined over number fields of* even *degree.*

Proof. If $\overline{\rho}_{E,\ell}$ is surjective then all ℓ-isogenies are defined over fields of degree $\ell+1$ (which is even), since this is the index of the Borel subgroups in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Otherwise, since $\ell \geq 17$ and E does not have an ℓ-isogeny over $\mathbb{Q}$, by the results of [5, 6, 31, 39] the projective image $\mathbb{P}\overline{\rho}_{E,\ell}(G_K)$ is contained in the normaliser of a non-split Cartan subgroup, which is the dihedral group $D_{\ell+1}$ of order $2(\ell+1)$. By [43, Proposition 1.13], the projective image is either the whole normaliser or an index 3 subgroup, hence has order either $2(\ell+1)$ or $2(\ell+1)/3$, and its intersection with any Borel subgroup has even index in the image.

For $\ell = 13$, all the possibilities for the image of Galois are now understood by the results of [2]. All the possibilities and the corresponding possibilities for $[\mathbb{Q}(P):\mathbb{Q}]$ for $P \in E[13]$ can be found in [16, Table 2] (where all the non-surjective possibilities are listed), and we can see that if E does not have a 13-isogeny and $\overline{\rho}_{E,13}$ is not surjective, then $[\mathbb{Q}(P):\mathbb{Q}]$ is either 72 or 96, implying that $[\mathbb{Q}(C):\mathbb{Q}]$ is a multiple of 6 or 8.

For $\ell = 11$, all the possibilities for $\overline{\rho}_{E,\ell}(G_K)$ are known and from [16, Table 1] we deduce that if E has no 11-isogeny over $\mathbb{Q}$, then $[\mathbb{Q}(C):\mathbb{Q}] = 12$.

For $\ell = 3$ and 5, the result of the proposition holds over any field K (of characteristic not ℓ), provided that $\sqrt{5} \notin K$ when $\ell = 5$. The fields of definition of the ℓ-isogenies are determined by the roots of a polynomial $f(X)$ over K of degree $\ell+1$; for example one may take $f(X) = \Phi_\ell(X, j(E))$ where Φ_ℓ denotes the modular polynomial. Moreover, the discriminant of f modulo squares is $\pm\ell$, the sign being taken so that $\pm\ell \equiv 1 \pmod 4$. By assumption, f has no roots in K itself. When $\ell = 3$ this means that either f is irreducible or the product of two irreducible quadratics, so the roots always have even degree. When $\ell = 5$ we must exclude the possibility that $f = gh$, where g and h are both irreducible of degree 3. In this case, g and h have the same splitting field, since over any field for which three different ℓ-isogenies are defined, all $\ell+1$ are defined (by looking at the action of $\mathrm{PGL}(2,\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$). But then $\mathrm{disc}(f)$ is a square, so 5 must be a square in K. □

Corollary 3.4. *Let E be an elliptic curve without CM defined over a number field of odd degree d, such that $j(E) = j \in \mathbb{Q}$, and let $\ell \neq 2, 7$ be a prime. Then ℓ is reducible for E/K if and only if ℓ is reducible for $E_0/\mathbb{Q}$, for any elliptic curve $E_0/\mathbb{Q}$ with $j(E_0) = j$.*

Proof. Let E_0 be any elliptic curve defined over $\mathbb{Q}$ with $j(E_0) = j$. By Proposition 3.3, ℓ is reducible for $E_0/\mathbb{Q}$ if and only if it is reducible for E_0/K, which is if and only if it is reducible for E/K by the invariance under quadratic twist. □

Remark. Let $E/\mathbb{Q}$ be an elliptic curve without CM with square discriminant, but with trivial 2-torsion over $\mathbb{Q}$, such as the one with LMFDB label 196a1. Equivalently, the image of the mod 2 representation to E is a cyclic group of order 3. Let K be the cyclic cubic field over which the 2-torsion of E is defined. Then the 3 points of order 2 are Galois conjugates of each other, and as each is the generator of a kernel of a 2-isogeny to a curve E_i, the three curves E_i, $i = 1, 2, 3$ are also Galois conjugates. Since E does not have CM, their j-invariants are distinct, and hence not defined over $\mathbb{Q}$. We conclude that each E_i is a $\mathbb{Q}$-curve, but not defined over $\mathbb{Q}$.

This example shows that Corollary 3.4 is not true for $\ell = 2$ and $d = 3$.

For $\ell = 7$, if we try to apply the argument used in the proof of Proposition 3.3 for $\ell = 3$ and $\ell = 5$, we find the possibility that f (which now has degree 8) may factor as $f = gh_1h_2$ where g as degree 2 and h_1, h_2 both have degree 3, all factors having discriminant -7 modulo squares. This can happen, specifically for curves with j-invariant 2268945/128. For example, the elliptic curve with LMFDB label 2450y1 is an example: it has no 7-isogenies over $\mathbb{Q}$, but has 7-isogenies defined over each of the conjugate cubic fields generated by roots of $x^3 - 5x - 5$, and two defined over $\mathbb{Q}(\sqrt{-7})$.

We can now prove Theorem 1.1 a), that the only primes ℓ which are reducible for a non-CM $\mathbb{Q}$-curve defined over a number field of odd degree are $\{2, 3, 5, 7, 11, 13, 17, 37\}$.

Proof of Theorem 1.1 a). By Theorem 2.4, the curve E is isogenous to an elliptic curve E' with $j(E') \in \mathbb{Q}$, and ℓ is also reducible for E'/K by Proposition 3.2. By Corollary 3.4, ℓ is reducible for any curve $E_0/\mathbb{Q}$ with $j(E_0) = j(E')$, and hence ℓ is one of the primes listed. □

Remark. As can be seen in [13, Theorem 1.2], all elliptic curves with $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$-torsion over cubic fields are base changes of elliptic curves defined over $\mathbb{Q}$. Hence there exists a $\mathbb{Q}$-curve that is 2-isogenous to such a curve with a 28-isogeny over that cubic field. But there are no elliptic curves with 28-isogenies over $\mathbb{Q}$. This shows that the restriction to prime degree isogenies in Theorem 1.1 a) is necessary.

Definition 1. We define $J_{\mathbb{Q}}(d)$ to be the set of prime numbers ℓ for which there exists an ℓ-isogeny of a non-CM elliptic curve with $\mathbb{Q}$-rational j-invariant without CM over a number field of degree d. Define $I_{\mathbb{Q}}(d)$ to be the union of all $J_{\mathbb{Q}}(k)$, $k \leq d$.

Results about $I_{\mathbb{Q}}(d)$ can be found in [34]. Recall that by [31], we have that

$$J_{\mathbb{Q}}(1) = I_{\mathbb{Q}}(1) = \{2, 3, 5, 7, 11, 13, 17, 37\}.$$

Proposition 3.5. *Let ℓ be a prime, E/K be an elliptic curve over a number field and C a cyclic subgroup of E of order ℓ^n for some integer $n \geq 2$. Then $[K(C) : K(\ell C)]$ either equals ℓ or divides $\ell - 1$.*

Proof. Fix a basis for $E[\ell^\infty]$ and let $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the ℓ-adic representation attached to E/K. Without loss of generality we may assume that the basis is chosen so that $\rho_{E,\ell}(G_{K(C)}) \subseteq G_n$ and $\rho_{E,\ell}(G_{K(\ell C)}) \subseteq G_{n-1}$, where for $m \geq 0$ we define

$$G_m = \left\{ \begin{pmatrix} a & b \\ \ell^m c & d \end{pmatrix} \right\} \subset \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Now G_n has index ℓ in G_{n-1}, coset representatives being $g_x = \begin{pmatrix} 1 & 0 \\ \ell^{n-1}x & 1 \end{pmatrix}$ for $x \pmod{\ell}$, and the image of C under these g_x are the ℓ subgroups C_x such that $\ell C_x = \ell C$. The action of $g = \begin{pmatrix} a & b \\ \ell^{n-1}c & d \end{pmatrix} \in G_{n-1}$ takes C_x to C_y where $y \equiv a^{-1}(c + dx) \pmod{\ell}$, and G_{n-1} acts the set $\{C_x \mid x \in \mathbb{F}_\ell\}$ through its image in the projective affine linear group of order $\ell(\ell-1)$. To see this, observe that the conjugate of G_{n-1} by $\begin{pmatrix} \ell^{n-1} & 0 \\ 0 & 1 \end{pmatrix}$ reduces modulo ℓ to $\left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \right\} \cong \mathbb{P}\,\mathrm{AGL}_1(\mathbb{F}_\ell)$, acting on $\left\{ \begin{pmatrix} 1 \\ x \end{pmatrix} \mid x \in \mathbb{F}_\ell \right\}$.

Let H be the image of $\rho_{E,\ell}(G_{K(C)})$ in this affine group. If H has an element of order ℓ then the action is transitive and $[K(C) : K(\ell C)] = \ell$; otherwise the image is cyclic of order dividing $\ell - 1$, hence the orbits also have sizes dividing $\ell - 1$, so that $[K(C) : K(\ell C)] \mid \ell - 1$.

□

We will need a result about degrees of fields of definition of isogenies which is in certain instances more precise than Proposition 3.5. Before stating and proving it, we introduce a definition.

Definition 2. We say that the ℓ-adic representation $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ of E is *defined modulo* ℓ^n if the image $\rho_{E,\ell}(G_K)$ contains the kernel of the reduction map $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)$.

Proposition 3.6. *Let E be an elliptic curve defined over a number field K such that its ℓ-adic representation is defined modulo ℓ^{n-1} for some $n \geq 1$. Then for any cyclic subgroup C of $E(\overline{K})$ of order ℓ^n, we have $[K(C) : K(\ell C)] = \ell$.*

Proof. In the notation of the proof of Proposition 3.5, the image of G_{n-1} in the affine group contains elements of order ℓ, and hence acts transitively. □

Let $G_E(\ell^n)$ be the reduction modulo ℓ^n of the image of the ℓ-adic representation attached to E, that is, of the composite $G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Remark. The result of Proposition 3.5 is best possible, in the sense that there exist $E/\mathbb{Q}$ and cyclic subgroups $C \in E(\overline{\mathbb{Q}})$ of order ℓ^2 such that each of the cases $[\mathbb{Q}(C) : \mathbb{Q}(\ell C)] = \ell$ and $[\mathbb{Q}(C) : \mathbb{Q}(\ell C)] = \ell - 1$ occur. The first case is generic, and occurs for any cyclic subgroup C of ℓ-power order when the ℓ-adic representation attached to E is surjective.

The case when $[\mathbb{Q}(C) : \mathbb{Q}(\ell C)] = \ell - 1$ occurs for example when $G_E(\ell^2)$ is the reduction of $\Gamma_0(\ell^2) \cap \Gamma_1(\ell)$ mod ℓ^2. Then there is one cyclic subgroup C of E order ℓ^2 defined over $\mathbb{Q}$. The other $\ell - 1$ cyclic subgroups of order ℓ^2, which are solutions of the equation (in groups) $\ell X = \ell C$, form a single orbit under the action of $G_{\mathbb{Q}}$, and hence are defined over an extension of degree $\ell - 1$. An example in the case $\ell = 5$ is the elliptic curve with LMFDB label 11a3.

If we impose additional conditions on the degree of the number field, then we get an absolute bound on the possible degrees of isogenies.

Proposition 3.7. *Let d be an integer not divisible by any $\ell \in J_{\mathbb{Q}}(1)$. Let E be a $\mathbb{Q}$-curve without CM over a number field K of degree d and $\phi : E \to E'$ a cyclic isogeny of degree n. Then E is isogenous to an elliptic curve $E''/\mathbb{Q}$ which has a cyclic n-isogeny over $\mathbb{Q}$, and in particular $n \leq 37$.*

Proof. As before, using the same arguments as in the proof of Proposition 3.3, E is isogenous to an elliptic curve $E''/\mathbb{Q}$ and these two curves have K-isogenies of the same prime degrees.

Since d is not divisible by any prime $\ell \leq 17$, by Lemma 3.1 we have that E'' does not gain any ℓ-isogenies for $\ell \leq 7$. From Proposition 3.3, we conclude that E'' does not gain any ℓ-isogeny for $\ell > 7$.

Finally, the ℓ-power degrees of isogenies of E'' do not change when extending to K by Proposition 3.5. □

Proof of Theorem 1.1 b). This follows directly from Proposition 3.7. □

Proof of Theorem 1.2. We must show that for each odd d, the degrees of isogenies of all $\mathbb{Q}$-curves over all number fields of degree d are bounded.

By the theory of complex multiplication, there are finitely many orders $\mathcal{O}$ of quadratic imaginary fields such that elliptic curves with CM by $\mathcal{O}$ are defined over a number field of degree d. For elliptic curves with CM the result now follows from [8, Theorem 5.3. b)]. In the assumptions of this theorem, there is the condition that K does not contain the field of definition of an elliptic curve with CM by an order of conductor divisible by ℓ, but if this happens then there is an isogeny from E to an elliptic curve with CM by the ring of integers of the CM field of E; a bound on the degree of the ℓ-power isogeny on E now follows from this fact.

Suppose now that E does not have CM. By Proposition 3.3 we have that the primes ℓ such that there exist ℓ isogenies over number fields of degree d are bounded (by 37). It remains to show that the ℓ-power degrees of isogenies are bounded.

Let N be the degree of a cyclic isogeny of E over a number field of degree K. Then, by [1, Theorem 1.2], there exists B_ℓ such that for all non-CM elliptic curves defined over $\mathbb{Q}$ the ℓ-adic representation of E is defined modulo ℓ^m for some $m \leq B_\ell$. Now from Proposition 3.6, we can conclude that if E has an isogeny of degree ℓ^k for $k > B_\ell$, then d is divisible by ℓ^{k-B_ℓ}. It follows that $\nu_\ell(N) \leq \nu_\ell(d) + B_\ell$. □

Remark. If one knows all the B_ℓ in the proof of the previous theorem, then C_d can be effectively computed. In fact one can take, for elliptic curves without CM:

$$C_d^{nonCM} := \prod_{\ell \in J(\mathbb{Q})} \ell^{\nu_\ell(d)+B_\ell}.$$

For elliptic curves with CM, one can produce a bound C_d^{CM} using the results of [8]. Finally, set

$$C_d := \max\{C_d^{nonCM}, C_d^{CM}\}.$$

Remark. It is not possible to bound the size of the prime power torsion, and hence the degree of prime power degree isogenies, over the union of all number fields of degree not divisible by some finite set of primes. To see this, let E be over $\mathbb{Q}$ a non-CM elliptic curve with a $\mathbb{Q}$-rational point of order $\ell = 3, 5$ or 7 for which the image of the ℓ-adic representation is as large as the point of order ℓ allows (this is the generic case, so infinitely many elliptic curves will satisfy this). Then E will have a point of order ℓ^{n+1} over a number field of degree ℓ^{2n}, as can be seen from [17, Proposition 2.2].

4. Torsion of $\mathbb{Q}$-curves over odd degree number fields

The following three sets of finite abelian groups are defined (see [20, 18, 19]) for each positive integer d:

- $\Phi(d)$ is the set of all possible torsion groups of elliptic curves over number fields of degree d.
- $\Phi_{\mathbb{Q}}(d)$ is the set of all possible torsion groups of elliptic curves defined over $\mathbb{Q}$ base changed to number fields of degree d.
- $\Phi_{j\in\mathbb{Q}}(d)$ is the set of all torsion groups of elliptic curves over number fields of degree d, with rational j-invariant.

Thus, $\Phi_{\mathbb{Q}}(d) \subseteq \Phi_{j\in\mathbb{Q}}(d) \subseteq \Phi(d)$. By Mazur's theorem [30], we have that

$$\Phi_{j\in\mathbb{Q}}(1) = \Phi_{\mathbb{Q}}(1) = \Phi(1) = \{\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \dots 10, 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 1, \dots, 4\}. \tag{4.1}$$

Proposition 4.1. *Let d be an odd integer not divisible by any prime ≤ 7. For all non-CM $\mathbb{Q}$-curves defined over number fields K of degree d, if $E(K)$ has a point of prime order ℓ then $\ell \in \{2, 3, 5, 7\}$.*

Proof. Suppose that E/K is a $\mathbb{Q}$-curve without CM over a number field K of degree d, and that $E(K)$ has a point of prime order ℓ. Then by Theorem 2.7 we have that E is isogenous (over K) to an elliptic curve E' defined over $\mathbb{Q}$. Since $E(K)$ has a point of order ℓ, by Proposition 3.2, E' has an ℓ-isogeny over K. By Proposition 3.3 it follows that either $\ell \in \{2, 7\}$ or ℓ is the degree of an isogeny over $\mathbb{Q}$; so $\ell \in \{2, 3, 5, 7, 11, 13, 17, 37\}$

It remains to show that $\ell \neq 11, 13, 17, 37$, so suppose that ℓ is one of these primes. By [16, Theorem 7.2 a)] we know that $E'(K)$ cannot have a point of order ℓ. Then by [36, Proposition 1.4] up to conjugation we have

$$\overline{\rho}_{E',\ell}(G_K) = \begin{pmatrix} \chi_\ell(G_K) & * \\ 0 & 1 \end{pmatrix},$$

with $*$ nonzero. It then follows from Galois theory that there exists a cyclic extension K'/K of degree ℓ such that

$$\overline{\rho}_{E',\ell}(G_{K'}) = \begin{pmatrix} \chi_\ell(G_{K'}) & 0 \\ 0 & 1 \end{pmatrix}.$$

But then E' has a point of order ℓ over the number field K', of degree not divisible by any prime ≤ 7, contradicting [16, Theorem 7.2 a)]. □

Recall the following result of Gužvić.

Theorem 4.2 ([19, Theorem 1.1])**.** *Let p be a prime ≥ 7. Then if E with $j(E) \in \mathbb{Q}$ has a point of order n over a number field of degree p, then $\mathbb{Z}/n\mathbb{Z} \in \Phi(1)$.*

We now prove a slightly stronger result.

Theorem 4.3. *Let d be an odd integer not divisible by any prime ≤ 7. Then $\Phi_{j\in\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(1)$.*

Proof. First note that $\Phi_{\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(1)$ by [16, Corollary 7.3]. Hence we need to show that $\Phi_{j\in\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(d)$. Certainly $\Phi_{j\in\mathbb{Q}}(d) \supseteq \Phi_{\mathbb{Q}}(d)$, so we must show that if E is an elliptic curve over K, a number field whose degree d satisfies the stated condition, with $j(E) \in \mathbb{Q}$, then the torsion subgroup of $E(K)$ also occurs as the torsion subgroup of $E_0(K)$ where E_0 is an elliptic curve defined over $\mathbb{Q}$.

If E has CM, then the result follows by [10, Theorem 1.2], so suppose now that E does not have CM.

Let E_0 be an elliptic curve defined over $\mathbb{Q}$ with $j(E_0) = j(E)$, so E_0 is a quadratic twist E_0 of E, and we have $E \simeq E_0^\delta$ for some $\delta \in (K^*)/(K^*)^2$.

We first prove that if $E(K)$ has a point of order n, then n already occurs as the order of an element of a group in $\Phi_{\mathbb{Q}}(d)$. Assume the opposite, i.e $E(K)$ has a point of order n but no group in $\Phi_{\mathbb{Q}}(d)$ has a point of order n. We will derive a contradiction by showing that E is the base-change of a curve defined over $\mathbb{Q}$.

Since $E_0 \simeq E$ over $K(\sqrt{\delta})$, it follows that $E_0(K(\sqrt{\delta}))$ has a point of order n. Since there are no elements of order n in any group in $\Phi_{\mathbb{Q}}(1)$ (since $\Phi_{\mathbb{Q}}(1) \subseteq \Phi_{\mathbb{Q}}(d)$), it follows that $E_0(\mathbb{Q})$ does not have a point of order n, so the torsion of E_0 grows from $\mathbb{Q}$ to $K(\sqrt{\delta})$. In particular, there exists a prime $\ell \mid n$ such that $\#E_0(K(\sqrt{\delta}))[\ell^\infty] > \#E_0(\mathbb{Q})[\ell^\infty]$.

If $\#E_0(\mathbb{Q})[\ell] > 1$, then $\ell \leq 7$ and a point $P \in E_0(\mathbb{Q})$ of order ℓ^k for some $k \geq 1$ becomes divisible by ℓ in $E_0(K(\delta))$, i.e. there exists an $P' \in E_0(K(\sqrt{\delta}))$ such that $\ell P' = P$. From [16, Proposition 4.6] we see that $[\mathbb{Q}(P') : \mathbb{Q}]$ has to divide $\ell^2(\ell - 1)$ so the only possibility is that $\mathbb{Q}(P')$ is a quadratic field.

Otherwise, $E_0(\mathbb{Q})[\ell]$ is trivial, and there exists $P' \in E_0(K(\sqrt{\delta}))$ of order ℓ. By [16, Theorem 5.8], we see that $\mathbb{Q}(P')$ has to be divisible by 4 for $\ell \geq 17$ and cannot be of the form $2t$, for any $t > 1$ not divisible by primes ≤ 7, when $\ell \leq 13$. Hence it again follows that $\mathbb{Q}(P')$ is a quadratic field.

Thus $\mathbb{Q}(P') = \mathbb{Q}(\sqrt{\delta_0})$ for some $\delta_0 \in \mathbb{Q}^*$, and the ℓ-power torsion growth occurs over the quadratic field $\mathbb{Q}(\sqrt{\delta_0})$. As $d = [K : \mathbb{Q}]$ is odd, $\mathbb{Q}(\sqrt{\delta_0}) \not\subseteq K$; but $\mathbb{Q}(\sqrt{\delta_0}) = \mathbb{Q}(P') \subseteq K(\sqrt{\delta})$, so it follows that $K(\sqrt{\delta_0}) = K(\sqrt{\delta})$. Hence $\delta\alpha^2 = \delta_0$ for some $\alpha \in K^*$. It follows that $E_0^{\delta_0} \simeq E_0^\delta \simeq E$ over K; in other words, E is a base change of $E_0^{\delta_0}$, which is an elliptic curve defined over $\mathbb{Q}$, giving us a contradiction.

So far we have shown that the cyclic groups in $\Phi_{j\in\mathbb{Q}}(d)$ are all also in $\Phi_{\mathbb{Q}}(d) = \Phi_{\mathbb{Q}}(1)$; in particular, the orders of elements of groups in $\Phi_{j\in\mathbb{Q}}(d)$ are ≤ 12. It remains to check that there are no noncyclic groups in $\Phi_{j\in\mathbb{Q}}(d)$ that are not in $\Phi_{\mathbb{Q}}(d)$. Since a number field of odd degree has no roots of unity apart from ± 1, the only remaining possibilities are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$. For $n \geq 4$ these are already in $\Phi_{\mathbb{Q}}(d)$, while for $n > 6$ they contain elements of order > 12, so cannot occur; we are then left with the cases $n = 5$ and $n = 6$. So suppose $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ with $n = 5$ or 6. Now $E_0(K(\sqrt{\delta}))$ has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$. Let $n' = 5$ or 3, respectively, and P' a point of order n' in $E_0(K(\sqrt{\delta}))$ (where $E_0 \simeq E^\delta$ is defined over $\mathbb{Q}$ as

before). Using the same argument as before, we conclude that $\mathbb{Q}(P')$ is a quadratic field and that E is a base change of an elliptic curve defined over $\mathbb{Q}$, completing the proof. □

Proof of Theorem 1.3. Let E be a $\mathbb{Q}$-curve over a number field K of degree p. If E has CM, the result follows by [9, Theorem 1.4], so suppose from now on that E does not have CM.

By Theorem 2.4 it follows that E is isogenous to E', which is defined over $\mathbb{Q}$. Let $\phi : E' \to E$ be this isogeny (which is defined over $\overline{\mathbb{Q}}$) and define $n := \deg \phi$. We factor $\phi = \phi_2 \circ \phi_1$, where $\deg \phi_1$ is divisible only by primes ≤ 7 and $\deg \phi_2$ is divisible only by primes ≥ 11. We have the diagram of isogenies (over $\overline{\mathbb{Q}}$)

$$E' \xrightarrow{\phi_1} E'' \xrightarrow{\phi_2} E.$$

Let $\ell \leq 7$ be a divisor of d. As the degree of d is, by assumption, coprime to $\#\overline{\rho}_{E',\ell}(G_{\mathbb{Q}})$ for all ≤ 7, we conclude that $K \cap \mathbb{Q}(E'[\ell]) = \mathbb{Q}$ so $\overline{\rho}_{E',\ell}(G_{\mathbb{Q}}) = \overline{\rho}_{E',\ell}(G_K)$, and in particular E' has the same ℓ-isogenies that it had over $\mathbb{Q}$. This implies that ϕ_1 is defined over $\mathbb{Q}$ and hence we have $j(E'') \in \mathbb{Q}$.

Now since E'' and E are isogenous over $\overline{\mathbb{Q}}$, by Lemma A.4, there is a twist of E''^{δ} of E'' which is isogenous over K to E. Since E''^{δ} is isogenous over K to E by an isogeny of degree coprime to $E(K)_{\mathrm{tors}}$ and $E''^{\delta}(K)_{\mathrm{tors}}$, it follows that $E(K)_{\mathrm{tors}} \simeq E''^{\delta}(K)_{\mathrm{tors}}$, and hence $E(K)_{\mathrm{tors}} \in \Phi_{j \in \mathbb{Q}}(p) = \Phi(1)$, with the last equality following from Theorem 4.3.

□

5. A ℚ-curve testing algorithm

In this section we give an algorithm for testing whether a given elliptic curve E, defined over a number field K, is a $\mathbb{Q}$-curve. We assume that we know how to test whether E is CM, and also that we can compute the K-isogeny class of E. In the absence of suitable references, we start with a brief discussion of these two questions. The main algorithm proceeds by applying a series of straightforward tests for necessary conditions satisfied by $\mathbb{Q}$-curves, which in practice quickly allow us to return an answer of "no" for all non-$\mathbb{Q}$-curves, followed by tests for sufficient conditions, allowing us to return the answer "yes" for genuine $\mathbb{Q}$-curves.

The trivial first steps are to return "yes" if $j(E) \in \mathbb{Q}$, and otherwise to replace E by a curve defined over $\mathbb{Q}(j)$ in case $\mathbb{Q}(j)$ has degree strictly less than K.

5.1. **Testing for CM.** We briefly discuss tests for whether a given algebraic number j is a CM j-invariant. First we describe an algebraic method, implemented by the first-named author as the `SageMath` method `j.is_cm_j_invariant()`, which is only guaranteed to work for algebraic numbers of degree h up to 100, for which the complete list of imaginary quadratic discriminants of class number h is known. This is used to prove that a CM j-invariant actually is CM; to prove that a non-CM number is not CM is much simpler.

Suppose we are given an algebraic number j and wish to know whether or not it is a CM j-invariant. A necessary condition is that j is an algebraic integer. Assuming this, the minimal polynomial of j is a monic polynomial $H(X) \in \mathbb{Z}[X]$ of degree h, say, and j is CM if and only if $H(X)$ is one of the finitely many Hilbert Class Polynomials $H_D(X)$ attached to an imaginary quadratic discriminant D of class number h. To establish whether j is CM with a specific discriminant D is easy, since there are good methods available (see [3]) for computing $H_D(X)$ from D, and we only need then test whether $H = H_D$.

If we know the complete list of discriminants D of class number h, where $h = \deg H(X)$, we simply compare $H(X)$ with $H_D(X)$ for each of these. For example, when $h = 1$ this amounts to seeing whether j is one of the 13 known rational CM j-invariants.

The complete list of discriminants of class number h is known for $h \leq 100$. Mark Watkins determined (see [42, Table 4]) the number of fundamental discriminants of each class number $h \leq 100$, together with the largest such discriminant. For example, for $h = 100$, there are 1726 such discriminants, the largest (in absolute value) being 1856563. Using the formula for the class number of a non-maximal order in terms of the class number of the associated maximal order, it is possible to extend this table to give the same quantities over all imaginary quadratic discriminants, including non-fundamental discriminants. This was carried out by Janis Klaise [23]: for example, for $h = 100$ there are 2311 discriminants, the largest still being 1856563 (see [23, p. 19]; note that for 90 class numbers up to 100 the largest discriminant in absolute value is a fundamental discriminant). For $h \leq 10$ the following table gives the number of negative discriminants D of class number h

and the maximum value of $|D|$:

h	1	2	3	4	5	6	7	8	9	10
$\#D$	13	29	25	84	29	101	38	208	55	123
$\max \lvert D\rvert$	163	427	907	1555	2683	4075	5923	7987	10627	13843

See also David Kohel's online database of discriminants and class numbers [26].

Using this precomputed data, it is trivial to test j-invariants of small degree for being CM. The `SageMath` function `cm_j_invariants(K)` uses this method to list all the CM j-invariants in a given number field K, while the method `j.is_cm_j_invariant()` first applies a number of local tests which in practice quickly eliminate non-CM js.

Since the number of CM j-invariants of each degree is finite, for most number fields there are no more CM j-invariants than the 13 already in $\mathbb{Z}$. For example, the 29 quadratic CM j-invariants lie in only 14 different (real) quadratic fields, namely $\mathbb{Q}(\sqrt{d})$ for $d \in \{2, 3, 5, 6, 7, 13, 17, 21, 29, 33, 37, 41, 61, 89\}$.

A different method is used in `Magma` (implemented by Mike Harrison: see [29]). Given a monic integer polynomial $H(X)$ of degree h, floating-point approximations to the real roots z of $H(X)$ are computed, from which one may solve the equations $j(\sqrt{D}) = z$ or $j((1 + \sqrt{D})/2) = z$ to obtain a unique candidate integer value of D, which is then verified by computing $H_D(X)$. An initial test checks that the number of real roots of $H(X)$ is a power of 2 and divides h, since (for a genuine CM j-invariant) this number is the size of the 2-torsion subgroup of the class group. This method works in principle for arbitrary degree h.

5.2. **Computing the K-isogeny class (for non-CM curves).** Given an elliptic curve E defined over a number field K, the problem of computing the complete (finite) set of K-isomorphism classes of elliptic curves E'/K isogenous to E over K can be divided into three steps: first, determine the set of primes ℓ for which $\overline{\rho}_{E,\ell}$ is reducible; then compute all curves ℓ-isogenous to E (over K) for each such ℓ; finally, iterate until each curve encountered is isomorphic to one already in the list. In the case of curves with CM, the set of reducible primes is infinite, and after the first step one must cut down to a finite set of reducible primes sufficient to generate the complete isogeny class; for the sake of brevity, and because we do not need this case for the application to $\mathbb{Q}$-curves, we will now assume that E does not have CM.

5.2.1. *Determining the reducible primes.* The problem of computing the finite set of reducible primes for a non-CM elliptic curve E, has been solved both by Larsen and Vaintrob in [27] and also by Billerey in [4]. Both methods are implemented in `SageMath`, by Larsen and Schembri respectively, with efficiency improvements in both cases by the first-named author. We note here that it is very easy to implement necessary tests for ℓ to be reducible, namely that for all primes $\mathfrak{p}$ of good reduction, $a_{\mathfrak{p}}(E)^2 - 4N(\mathfrak{p})$ must be a square (possibly zero) modulo ℓ. Here, $a_{\mathfrak{p}}(E)$ denotes the trace of Frobenius of the reduction of E at $\mathfrak{p}$. Using this, it is very fast to determine a small set of primes ℓ up to some bound (say 1000) containing all reducible primes (and possibly some others) up to that bound. The harder, and more time-consuming, part is to prove that there are no reducible primes greater than the bound chosen. However, as we will see, in order to prove that an elliptic curve E is a $\mathbb{Q}$-curve, it is sufficient in practice to have a list of curves which are K-isogenous to E via isogenies of degrees supported by a sufficiently large subset of the reducible primes, without needing to know whether or not this is the complete isogeny class.

The `SageMath` command `E.reducible_primes()` will, if E is not CM, return a provably complete list of the reducible primes ℓ for E (using Billerey's algorithm by default), while if E has CM then it returns a finite list of reducible primes such that for every K-isogenous curve E' there is an isogeny $E \to E'$ of degree supported on primes in the list. The command `E.reducible_primes(algorithm='heuristic')` returns the (probably complete) set of reducible primes less than a certain bound, which by default is 1000 (the user can provide a larger bound if needed).

5.2.2. *Computing ℓ-isogenous j-invariants and ℓ-isogenies.* For any fixed prime ℓ we may compute all elliptic curves ℓ-isogenous to E over K using the methods of Tsukazaki's thesis [41], building on earlier work by Vélu, Kohel, and unpublished joint work by Watkins and the first-named author; this is implemented in `SageMath`. Here we do not need to known in advance whether or not ℓ is actually reducible for E, since if it is not then we will simply find no ℓ-isogenous curves.

For the purpose of our $\mathbb{Q}$-curve test, we do not need to know the ℓ-isogenous curves themselves, only their j-invariants, and these may be computed directly as the roots of the modular polynomial $\Phi_\ell(X, j)$ when Φ_ℓ is known. David Kohel's database [26] contains these for $\ell \leq 113$ (available as an optional package in `SageMath`), while `Magma`has them for $\ell \leq 59$ (also computed by David Kohel). On the other hand, we may want to know

the isogenous curves anyway for other reasons, for example if we are compiling a database of elliptic curves such as the LMFDB.

The `SageMath` command `E.isogeny_class(algorithm='heuristic')` returns the partial K-isogeny class of E (where K is the base field of E), using only reducible primes up to 1000.

5.3. **Necessary conditions.** Since most elliptic curves are not $\mathbb{Q}$-curves, it is useful and efficient to have a series of necessary conditions for being a $\mathbb{Q}$-curve which are easy to check, since obviously if any of these fail then we know that the curve is not a $\mathbb{Q}$-curve. Note that we do not assume that the field of definition, K, is Galois over $\mathbb{Q}$. Our tests are local, and are divided into those which involve primes of good and bad reduction respectively. For a prime $\mathfrak{p}$ of good reduction we denote by $E_\mathfrak{p}$ the reduction of E modulo $\mathfrak{p}$ and by $a_\mathfrak{p}$ its trace of Frobenius.

5.3.1. *Local tests at good primes.* If the base field K were Galois and we only needed to test that E was isogenous over K itself to all its conjugates, a necessary condition would be that $a_\mathfrak{p}(E) = a_{\mathfrak{p}'}(E)$ for any two conjugate primes $\mathfrak{p}$, $\mathfrak{p}'$ of K. We replace this with a condition which is valid when K is not necessarily Galois and which detects isogeny over $\overline{\mathbb{Q}}$.

Proposition 5.1. *Let E be a $\mathbb{Q}$-curve defined over the number field K. Let p be a rational prime not dividing the norm of the conductor of E, and let $\mathfrak{p}$, $\mathfrak{p}'$ be primes of K above p. Then E has good reduction at both $\mathfrak{p}$ and $\mathfrak{p}'$, and*

1. *$E_\mathfrak{p}$ and $E_{\mathfrak{p}'}$ are either both ordinary or both supersingular;*
2. *in the ordinary case, the integers $a_\mathfrak{p}(E)^2 - 4N(\mathfrak{p})$ and $a_{\mathfrak{p}'}(E)^2 - 4N(\mathfrak{p}')$ are both negative and have the same square-free part.*

Proof. The condition of being ordinary or supersingular is invariant under base change and under isogeny (over finite fields), and in the ordinary case the endomorphism algebra is an imaginary quadratic field which is also invariant under isogeny and base-change.

Take a finite extension L/K which is Galois, and such that all the isogenies between Galois conjugates of the base-change of E from K to L are defined over L. Let $\mathfrak{q}$ and $\mathfrak{q}'$ be primes of L above $\mathfrak{p}$ and $\mathfrak{p}'$ respectively. Since $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the primes of L above p, the $\mathbb{Q}$-curve condition implies that the reductions $E_\mathfrak{q}$, $E_{\mathfrak{q}'}$ are isogenous. Hence

$$E_\mathfrak{p} \text{ ordinary} \iff E_\mathfrak{q} \text{ ordinary} \iff E_{\mathfrak{q}'} \text{ ordinary} \iff E_{\mathfrak{p}'} \text{ ordinary},$$

giving (1). Assume that we are in the ordinary case. Then in the Hasse bound $|a_\mathfrak{p}(E)| \le 2\sqrt{N(\mathfrak{p})}$ we have strict inequality, so $d_\mathfrak{p} := a_\mathfrak{p}(E)^2 - 4N(\mathfrak{p}) < 0$. The endomorphism ring of $E_\mathfrak{p}$ is an order in the imaginary quadratic field $\mathbb{Q}(\sqrt{d_\mathfrak{p}})$, and that of $E_{\mathfrak{p}'}$ is a (possibly different) order in the same field, giving (2). □

5.3.2. *Local tests at bad primes.* Again, if K were Galois and we only needed to check that E was isogenous over K to its Galois conjugates, the conditions at bad primes could be combined into a single test that the conductor of E was stable under the action of the Galois group. We replace this with a condition which is stable under base-change.

Proposition 5.2. *Let E be a $\mathbb{Q}$-curve defined over the number field K. Let p be a rational prime, and let $\mathfrak{p}$, $\mathfrak{p}'$ be primes of K above p. Then*

$$\mathrm{ord}_\mathfrak{p}(j(E)) < 0 \iff \mathrm{ord}_{\mathfrak{p}'}(j(E)) < 0.$$

Proof. The j-invariant has negative valuation at $\mathfrak{p}$ if and only if the reduction at $\mathfrak{p}$ is potentially multiplicative, and this condition is invariant under base-change. Assume that $\mathrm{ord}_\mathfrak{p}(j(E)) < 0$, and take an extension L/K and primes $\mathfrak{q}$, $\mathfrak{q}'$ as in the proof of Proposition 5.1, with the additional condition that the base-change E_L of E to L has bad multiplicative reduction (not just potentially multiplicative) at $\mathfrak{q}$. Let $g \in \mathrm{Gal}(L/\mathbb{Q})$ be such that $g(\mathfrak{q}) = \mathfrak{q}'$. Since E_L and $g(E_L)$ are isogenous, E_L also has bad multiplicative reduction at $\mathfrak{q}'$, so $\mathrm{ord}_{\mathfrak{q}'}(j(E)) < 0$ and hence also $\mathrm{ord}_\mathfrak{p}(j(E)) < 0$. □

5.4. **Sufficient conditions.** Here we show how to prove that an elliptic curve E/K is a $\mathbb{Q}$-curve, using (possibly incomplete) knowledge of the K-isogeny class of E. Note that we do not have to consider any isogenies defined over extensions of K. If we know that we have the complete K-isogeny class, then this method can also be used to prove that a curve is not a $\mathbb{Q}$-curve, though in practice that would be more easily done using the methods given above.

Suppose that we have computed either the K-isogeny class of our test curve E, or a subset of the isogeny class which is not known to be complete. Consider the finite set of j-invariants of curves in the class. Since

we are assuming that E does not have CM, these j-invariants are distinct: this follows from Lemma A.1. For each, we compute its degree and minimal polynomial.

If any of the j-invariants are rational then E is a $\mathbb{Q}$-curve. In this case the $\mathbb{Q}$-class of $j(E)$ is rational (as defined in Section 2). More generally, E is a $\mathbb{Q}$-curve if the set of j-invariants includes a complete set of Galois conjugates.

If we know that we have the complete K-isogeny class of E, then the previous condition (that the set of j-invariants includes a complete set of Galois conjugates) is both necessary and sufficient. To see this we apply Theorem 2.6: the K-isogeny class contains a central $\mathbb{Q}$-curve together with all its Galois conjugates. Hence, in the case where we have the complete isogeny class, it suffices to examine the j-invariants of 2-power degree, since E is a $\mathbb{Q}$-curve if and only if this set contains a complete set of Galois conjugates, or equivalently if and only if some minimal polynomial of 2-power degree d occurs d times in the collection.

If we do in fact have the complete K-isogeny class, but have not proved that the class is complete, then this test still works in one direction (if the set of j-invariants contains a complete Galois conjugacy class then E is a $\mathbb{Q}$-curve) but we cannot conclude that E is not a $\mathbb{Q}$-curve when the test fails.

5.5. **The algorithm.** We summarise the results of this section by providing pseudocode for our algorithm. We denote the minimal polynomial of an algebraic number j by m_j, the conductor of E by $\mathrm{cond}(E)$ and the norm of an ideal $\mathfrak{a}$ by $N(\mathfrak{a})$.

Algorithm QCurveTest
Input: An elliptic curve E defined over a number field K, and positive integers B_1, B_2.
Output: `True` if E is a $\mathbb{Q}$-curve, else `False`.

(1) If $j(E) \in \mathbb{Q}$ then return `True`.
(2) If $j(E)$ is a CM j-invariant then return `True`.
(3) Set $N = N(\mathrm{cond}(E))$.
(4) For each prime $p \mid N$:
  (a) If $\{\mathrm{ord}_{\mathfrak{p}}(j(E)) : \mathfrak{p} \mid p\}$ contains both negative and non-negative integers then return `False`.
(5) For each prime $p \nmid N$ with $p \le B_1$:
  (a) If $\{E_{\mathfrak{p}} : \mathfrak{p} \mid p\}$ are all ordinary:
    (i) If $\{a_{\mathfrak{p}}(E)^2 - 4N(\mathfrak{p}) : \mathfrak{p} \mid p\}$ do not all have the same squarefree part then return `False`.
  (b) Else if $\{E_{\mathfrak{p}} : \mathfrak{p} \mid p\}$ are not all supersingular then return `False`.
(6) Compute the partial K-isogeny class $\mathcal{C}$ of E, using a bound of B_2 on the reducible primes.
(7) Compute $\mathcal{J} = \{j(E') : E' \in \mathcal{C}\}$, $\mathcal{P} = \{(j', m_{j'}) : j' \in \mathcal{J}\}$.
(8) If $\mathcal{J}$ contains a rational number then return `True`.
(9) Remove from $\mathcal{P}$ any pairs (j', m') with $\deg(m')$ not a power of 2.
(10) For each $(j', m') \in \mathcal{P}$:
  (a) If $\#\{(j'', m'') \in \mathcal{P} : m'' = m'\} = \deg(m')$ then return `True`.
  (b) Remove $\{(j'', m'') \in \mathcal{P} : m'' = m'\}$ from $\mathcal{P}$.
(11) Compute a bound B_2' on the reducible primes for E (using Billerey's algorithm, for example).
(12) If $B_2 \ge B_2'$ return `False`.
(13) Increase B_1 by a factor of 2, replace B_2 by B_2', and go to line (5).

Note that we loop back to line 5 at most once. We only reach line 11 if either E is not a $\mathbb{Q}$-curve but it passes all the necessary tests in lines 4 and 5, or it is a $\mathbb{Q}$-curve but the partial isogeny class we computed in line 6 is too small to contain a complete set of Galois conjugates. On repeating line 6 we will certainly have the complete isogeny class, hence if we reach line 11 a second time we know that E is not a $\mathbb{Q}$-curve; hence the exit at line 12. It would be possible to increase B_2 one or more times first, before replacing it with a rigorous bound, but note that the largest reducible prime for curves in the LMFDB at present (August 2020) is 41 (which occurs for four isogeny classes over $\mathbb{Q}(\sqrt{-1})$, for example the class with label 2.0.4.1-84050.1-b), so we expect that using bounds of 1000 for both B_1 and B_2 it is unlikely that line 11 will be reached at all.

Appendix A. $\mathbb{Q}$-curves and $\mathbb{Q}$-numbers

Here we give a self-contained account of the theory of $\mathbb{Q}$-curves, establishing the results stated in Section 2. Most of the ideas presented here may be found in Elkies' article "On elliptic K-curves" (see [14]); however, we have found it more convenient to present this material in terms of properties of certain algebraic numbers j, viewed as j-invariants of elliptic curves, in order to prove the additional results we need which are not in [14].

We take $\mathbb{Q}$ to be our base field, and denote by $\overline{\mathbb{Q}}$ its algebraic closure, the field of algebraic numbers. Set $G = G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Everything here could also be done with an arbitrary base field K, replacing $\overline{\mathbb{Q}}$ with a separable closure M of K and G by $\mathrm{Gal}(M/K)$. Some minor changes would be needed in case $\mathrm{char}(K) \neq 0$.

See Silverman [40] for standard properties of isogenies used here.

A.1. **Isogenies, degrees and the isogeny graph.**

A.1.1. *Isogenous algebraic numbers.* We define an equivalence relation *isogeny* on $\overline{\mathbb{Q}}$ as follows. Let $j_1, j_2 \in \overline{\mathbb{Q}}$. Then j_1 and j_2 are *isogenous*, denoted $j_1 \sim j_2$, if for each pair E_1, E_2 of elliptic curves over $\overline{\mathbb{Q}}$ with $j(E_i) = j_i$ for $i = 1, 2$, there is an isogeny $\phi : E_1 \to E_2$ defined over $\overline{\mathbb{Q}}$. Clearly this condition does not depend on the choice of the E_i, since different curves with the same j-invariant are isomorphic over $\overline{\mathbb{Q}}$. We call the triple (E_1, E_2, ϕ) consisting of such a pair of curves E_i and the isogeny between them a *realisation* of the isogeny relation $j_1 \sim j_2$.

Isogeny is an equivalence relation: symmetry comes from the existence of dual isogenies. Hence we can partition $\overline{\mathbb{Q}}$ into equivalence classes called *isogeny classes*.

The property of having complex multiplication (CM) is isogeny-invariant; it is even true that $\mathrm{End}(E_1)\otimes\mathbb{Q} \cong \mathrm{End}(E_2) \otimes \mathbb{Q}$ for isogenous curves E_1, E_2, though in general $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$ are different orders in their common field of fractions. Hence it makes sense to define an isogeny class as being CM or non-CM, the set of CM isogeny classes in $\overline{\mathbb{Q}}$ being in bijection with the set of imaginary quadratic fields. We will be mainly concerned with non-CM isogeny classes.

A.1.2. *Degrees of isogenies.* To each pair of isogenous non-CM algebraic numbers j_1, j_2 we assign a positive integer, the *degree* $\deg(j_1, j_2)$ to be the degree of a cyclic isogeny $\phi : E_1 \to E_2$ realizing the relation $j_1 \sim j_2$. This is well-defined by the following lemma.

Lemma A.1. *Let E_1, E_2 be isogenous elliptic curves without CM over $\overline{\mathbb{Q}}$. Then there is a cyclic isogeny $\phi : E_1 \to E_2$, and it is unique up to sign. In particular, the positive integer $d = \deg(\phi)$ is well-defined as the degree of a cyclic isogeny from E_1 to E_2. Every isogeny from E_1 to E_2 has degree dm^2 for some $m \geq 1$, and is cyclic if and only if $m = 1$.*

Proof. Let $\phi_0 : E_1 \to E_2$ be an isogeny. Then $\ker(\phi_0)$ is a finite subgroup of $E_1(\overline{\mathbb{Q}})$. Let $m \geq 1$ be maximal such that $\ker(\phi_0)$ contains $E_1[m]$ (the kernel of the multiplication-by-m map $E_1 \to E_1$). Then $\phi_0 = \phi \circ [m]$ for some cyclic isogeny $\phi : E_1 \to E_2$.

Let $d = \deg(\phi)$, and suppose that $\psi : E_1 \to E_2$ is another cyclic isogeny, of degree d'. Then $\hat{\psi} \circ \phi$ is an endomorphism of E_1 of degree dd'. Since $\mathrm{End}(E_1) \cong \mathbb{Z}$ we have $\hat{\psi} \circ \phi = [\pm n]$ with n a positive integer satisfying $n^2 = \deg(\hat{\psi} \circ \phi) = dd'$. Now $\ker(\phi)$ is cyclic of order d and is a subgroup of $\ker([n]) \cong (\mathbb{Z}/n\mathbb{Z})^2$, so $d \mid n$. Similarly, $d' \mid n$; hence $d = d' = n$ and $\psi = \pm\phi$.

The last part is clear. □

In terms of the modular polynomials $\Phi_d(X, Y) \in \mathbb{Z}[X, Y]$ we have $j_1 \sim j_2$ with $\deg(j_1, j_2) = d$ if and only if $\Phi_d(j_1, j_2) = 0$.

Corollary A.2. *Let $j_1, j_2, j_3 \in \overline{\mathbb{Q}}$ be isogenous. Then*

$$\deg(j_1, j_3) \equiv \deg(j_1, j_2)\deg(j_2, j_3) \pmod{(\mathbb{Q}^*)^2}.$$

Proof. For $1 \leq r \leq 3$ let E_r be an elliptic curve with $j(E_r) = j_r$, and for $1 \leq r < s \leq 3$ let ϕ_{rs} be a cyclic isogeny from E_r to E_s. Then $\phi_{23} \circ \phi_{12}$ and ϕ_{13} are both isogenies from E_1 to E_3, so by Lemma A.1 their degrees are the same up to squares. □

Corollary A.3. *Let $j_1, j_2, j_3 \in \overline{\mathbb{Q}}$ be isogenous with $\deg(j_1, j_2) = \deg(j_1, j_3)$ and $\deg(j_2, j_3)$ square-free. Then $j_2 = j_3$.*

Proof. $\deg(j_2, j_3)$ is a square by Corollary A.2 and is also square-free, hence is 1. □

The next results concern the minimal field of definition of an isogeny realising an isogeny relation. These are certainly well-known: see, for example, Lemma 3.1 in [25].

Lemma A.4. *Let E_1, E_2 be elliptic curves defined over a number field K. If E_1 and E_2 are isogenous over $\overline{\mathbb{Q}}$ then there exists a twist of E_2 which is isogenous to E_1 over K itself.*

Proof. Let $\phi : E_1 \to E_2$ be an isogeny over $\overline{\mathbb{Q}}$. For each $g \in G_K$, ϕ^g is another isogeny $E_1 \to E_2$, hence $\phi^g = \alpha(g) \circ \phi$ with $\alpha(g) \in \mathrm{Aut}(E_2)$. The map $g \mapsto \alpha(g)$ is a cocycle representing an element of $H^1(G, \mathrm{Aut}(E_2)) \cong K^*/(K^*)^n$, where $n = 2$ unless $j(E_2) = 0$ or 1728 in which case $n = 6$ or 4 respectively. Twisting E_2 by α has the desired effect. □

When $j(E_2) \neq 0, 1728$, in this proof we have $\alpha(g) = \pm 1$ with α a character which cuts out a quadratic extension $K(\sqrt{d})$ of K, and the quadratic twist $E_2^{(d)}$ has the desired property.

Corollary A.5. *Let $j_1, j_2 \in \overline{\mathbb{Q}}$ be isogenous. Then there exists an isogeny $\phi : E_1 \to E_2$ realizing the relation $j_1 \sim j_2$, with E_1, E_2 and ϕ all defined over $\mathbb{Q}(j_1, j_2)$.*

Proof. Take any curves E_i defined over $\mathbb{Q}(j_i)$ with $j(E_i) = j_i$ for $i = 1, 2$. By Lemma A.4 with $K = \mathbb{Q}(j_1, j_2)$, after replacing E_2 by a twist if necessary, there is an isogeny $E_1 \to E_2$ defined over K. □

The following easy fact will be used repeatedly.

Lemma A.6. *Let $j_1, j_2 \in \overline{\mathbb{Q}}$. If $j_1 \sim j_2$ then for all $g \in G$ we also have $g(j_1) \sim g(j_2)$, and* $\deg(g(j_1), g(j_2)) = \deg(j_1, j_2)$.

Proof. Applying any Galois automorphism to a cyclic isogeny $E_1 \to E_2$ gives a cyclic isogeny $g(E_1) \to g(E_2)$ of the same degree. □

For an alternate proof, apply g to the equation $\Phi_d(j_1, j_2) = 0$.

A.1.3. *Factorisation of isogenies and Atkin-Lehner involutions.* Every cyclic isogeny can be factored into a composition of isogenies of prime power degree, by repeatedly applying the following well-known fact.

Proposition A.7. *Let E_1 and E_2 be elliptic curves defined over $\overline{\mathbb{Q}}$ and let $\phi : E_1 \to E_2$ be a cyclic isogeny of degree d. For any factorization $d = d_1 d_2$ into positive integers d_1, d_2, there exist an elliptic curve E and isogenies $\phi_1 : E_1 \to E$ and $\phi_2 : E \to E_2$ of degree d_1 and d_2 respectively such that $\phi = \phi_2 \circ \phi_1$.*

E is uniquely determined (up to isomorphism over $\overline{\mathbb{Q}}$) by the ordered pair of factors (d_1, d_2), while ϕ_1 and ϕ_2 are uniquely determined up to replacing (ϕ_1, ϕ_2) by $(\alpha \circ \phi_1, \phi_2 \circ \alpha^{-1})$ for some $\alpha \in \mathrm{Aut}(E)$. In particular, if the curves do not have CM then ϕ_1 and ϕ_2 are uniquely determined up to simultaneous negation.

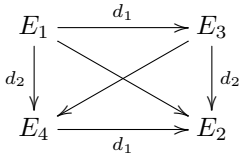
Proof. $\ker(\phi)$ is a cyclic subgroup of $E_1(\overline{\mathbb{Q}})$ of order d and hence has a unique subgroup of order d_1, which determines a cyclic d_1-isogeny $\phi_1 : E_1 \to E$, unique up to post-composition with an automorphism of E. Since $\ker(\phi_1) \subseteq \ker(\phi)$ the original isogeny ϕ factors as $\phi = \phi_2 \circ \phi_1$, through an isogeny $\phi_2 : E \to E_2$ as required. □

In terms of j-invariants, such factorizations can be realized without making additional field extensions, as follows.

Corollary A.8. *Let $j_1, j_2 \in \overline{\mathbb{Q}}$ be isogenous with $d = \deg(j_1, j_2) = d_1 d_2$. Then there exists $j \in \overline{\mathbb{Q}}$ with $j_1 \sim j \sim j_2$ such that $\deg(j_1, j) = d_1$ and $\deg(j, j_2) = d_2$. Moreover, $j \in \mathbb{Q}(j_1, j_2)$.*

Proof. The first part is immediate from the proposition. For the last part, let $K = \mathbb{Q}(j_1, j_2)$ and let $\phi : E_1 \to E_2$ be a cyclic d-isogeny defined over K, as in Corollary A.5. In the notation of the proof of the proposition, $\ker(\phi)$ is defined over K, and so is $\ker(\phi_1)$ since it is the unique subgroup of $\ker(\phi)$ of order d_1. Thus E is also defined over K, and $j = j(E) \in K$. □

Again let $\phi : E_1 \to E_2$ be a cyclic isogeny of degree $d = d_1 d_2$, and now we assume that $\gcd(d_1, d_2) = 1$. Using both this factorization and also $d = d_2 d_1$, we obtain two elliptic curves E_3 and E_4 and a commutative diagram of isogenies as follows:



Here one diagonal is the original isogeny $E_1 \to E_2$, while the other diagonal gives a cyclic isogeny $E_3 \to E_4$ of degree d. As special cases, when $d_1 = 1$ this is the same as ϕ, while when $d_2 = 1$, the new isogeny is the dual $\hat{\phi} : E_2 \to E_1$.

In terms of modular curves, $\phi : E_1 \to E_2$ defines a non-cuspidal point on $X_0(d)$ and the new isogeny $E_3 \to E_4$ is the image of this point under the Atkin-Lehner involution $W_{d_1} : X_0(d) \to X_0(d)$. As d_1 ranges

over all positive divisors of d with $\gcd(d_1, d/d_1) = 1$, these involutions form an elementary abelian 2-group of order 2^r, where r is the number of distinct prime factors of d. In particular, W_1 is the identity map while W_d takes ϕ to its dual.

Applying all such involutions, we obtain a collection of 2^r isogenous curves, with isogeny degrees all such divisors of d. We call this collection of curves and the isogenies between them the *Atkin-Lehner orbit* of the original isogeny $\phi : E_1 \to E_2$.

A.1.4. *The isogeny graph.* We may turn $\overline{\mathbb{Q}}$ into a graph by introducing edges between any isogenous pair (j_1, j_2). Each isogeny class is then a complete graph. More useful is to only include edges of *prime* degree. Since every cyclic isogeny is a composite of isogenies of prime degree, this has the same connected components. The component whose vertex set is the isogeny class of $j \in \overline{\mathbb{Q}}$ is denoted $[j]$.

Fix a prime ℓ. We will construct graphs derived from the isogeny class $[j]$, representing only isogenies of ℓ-power degree. This can be done in two ways, either as a subgraph of the isogeny graph or as a quotient. We briefly describe the subgraph construction, as used by Elkies in [14], before turning to the quotient construction which we use in what follows.

A.1.5. *The ℓ-primary subgraph.* Consider the full subgraph of $[j]$ consisting only of the vertices j' such that $\deg(j, j')$ is a power of ℓ. This is a regular tree, each vertex having degree $\ell + 1$, often called a Bruhat-Tits tree. The graph $[j]$ is the disjoint union of such trees, where two vertices j', j'' lie in the same subgraph if and only if $\deg(j', j'')$ is a power of ℓ. For each j in the isogeny class there is a projection from $[j]$ to the subgraph containing j, mapping each j' to the unique j'' such that $\deg(j, j'')$ is a power of ℓ and $\deg(j'', j')$ is coprime to ℓ.

A.1.6. *The ℓ-primary quotient graph.* Alternatively, we define a new graph, also a regular tree of degree $\ell+1$, which is a *quotient* of $[j]$, and does not depend on a choice of representative j in its isogeny class. We denote this quotient by $[j]_\ell$ and the projection $[j] \to [j]_\ell$ by π_ℓ.

With ℓ fixed, define $j_1 \approx j_2$ to mean that $j_1 \sim j_2$ with $\deg(j_1, j_2)$ *coprime to* ℓ. This is an equivalence relation which refines the relation of isogeny. Denote by $\pi_\ell(j)$ the equivalence class of $j \in \overline{\mathbb{Q}}$ under the new relation; thus the isogeny class $[j]$ is the disjoint union of classes $\pi_\ell(j')$ for $j' \sim j$.

Let $[j]_\ell = \{\pi_\ell(j') \mid j' \in [j]\}$ be the quotient of $[j]$ by $\approx$. Since Galois conjugation preserves isogeny degrees, we have a well-defined induced action of G on $[j]_\ell$, such that $g(\pi_\ell(j)) = \pi_\ell(g(j))$.

For $j_1, j_2 \in [j]$ let $\deg_\ell(j_1, j_2)$ be the ℓ-primary part of $\deg(j_1, j_2)$, and set $\deg_\ell(\pi_\ell(j_1), \pi_\ell(j_2)) = \deg_\ell(j_1, j_2)$. This is well-defined, since if $j_1' \approx j_1$ and $j_2' \approx j_2$ then $\deg_\ell(j_1', j_2') = \deg_\ell(j_1, j_2)$. These degrees between vertices of $[j]_\ell$ are, by definition, powers of ℓ.

The set $[j]_\ell$ inherits a graph structure from $[j]$. Explicitly, there is an edge between $\pi_\ell(j_1)$ and $\pi_\ell(j_2)$ if and only if $\deg_\ell(\pi_\ell(j_1), \pi_\ell(j_2)) = \ell$ (that is, if and only if $\deg(j_1, j_2)$ has ℓ-valuation equal to 1). This graph is a regular tree (every vertex has degree $\ell + 1$), and G acts on $[j]_\ell$ through automorphisms of the tree.

The following result was stated in terms of ℓ-primary subgraphs by Elkies. The version here will play an important role in the construction of the core of an isogeny class of $\mathbb{Q}$-curves.

Proposition A.9 (Chinese Remainder Theorem for isogenies)**.** *Let $j \in \overline{\mathbb{Q}}$.*

1. *Let $j' \in [j]$. Then for almost all primes ℓ we have $\pi_\ell(j') = \pi_\ell(j)$.*
2. *Conversely, for each collection of $j_\ell \in [j]$, one for each prime ℓ, with $\pi_\ell(j_\ell) = \pi_\ell(j)$ for almost all ℓ, there exists a unique $j' \in [j]$ such that $\pi_\ell(j') = \pi_\ell(j_\ell)$ for all ℓ.*

Proof. (1) We have $\pi_\ell(j') = \pi_\ell(j)$ if and only if $\ell \nmid \deg(j, j')$, which is true for almost all ℓ.

(2) Let ℓ_i for $1 \le i \le r$ be the primes for which $\pi_\ell(j_\ell) \ne \pi_\ell(j)$. (If there are none, then $j' = j$ meets the conditions.) To ease notation set $j_i = j_{\ell_i}$ for $1 \le i \le r$. For each i, factor the isogeny $j \to j_i$ as $j \to j_i' \to j_i$ where $\deg(j, j_i') = \deg_\ell(j, j_i) = \ell_i^{e_i}$ (say) is a power of ℓ_i, and $\deg(j_i', j_i)$ is coprime to ℓ_i, so that $\pi_{\ell_i}(j_i') = \pi_{\ell_i}(j_i)$.

Let E be an elliptic curve with $j(E) = j$, and for each i let E_i be a curve with $j(E_i) = j_i'$, and $\phi_i : E \to E_i$ a cyclic isogeny degree $\ell_i^{e_i}$. Define $\phi : E \to E'$ to be an isogeny whose kernel is the sum of the $\ker(\phi_i)$, so that ϕ is cyclic of degree $\prod_i \ell_i^{e_i}$. The isomorphism class of E' depends only on $\ker(\phi)$, since any other isogeny with the same kernel is obtained by composing ϕ with an isomorphism; set $j' = j(E')$. Then for each i we can factor $\phi = \psi_i \circ \phi_i$ with $\deg(\psi_i)$ coprime to ℓ_i, so j' satisfies $\pi_{\ell_i}(j') = \pi_{\ell_i}(j_i') = \pi_{\ell_i}(j_i)$ for $1 \le i \le r$, while $\pi_\ell(j') = \pi_\ell(j)$ for $\ell \ne \ell_1, \dots, \ell_r$ since these primes do not divide $\deg(j, j')$.

For the uniqueness, if also $\pi_\ell(j'') = \pi_\ell(j_\ell)$ for all ℓ, then for all ℓ we have $\pi_\ell(j') = \pi_\ell(j'')$, so $\ell \nmid \deg(j', j'')$; hence $j' = j''$. □

A.2. **$\mathbb{Q}$-curves and $\mathbb{Q}$-numbers.** A $\mathbb{Q}$-*curve* is an elliptic curve E defined over $\overline{\mathbb{Q}}$ such that E is isogenous (over $\overline{\mathbb{Q}}$) to all its Galois conjugates. Since this definition only depends on the $\overline{\mathbb{Q}}$-isomorphism class of E and $\overline{\mathbb{Q}}$ is algebraically closed, it is a property of the algebraic number $j(E)$, so we define $j \in \overline{\mathbb{Q}}$ to be a $\mathbb{Q}$-*number* if any elliptic curve $E/\overline{\mathbb{Q}}$ with $j(E) = j$ is a $\mathbb{Q}$-curve.

As is well-known*, all elliptic curves with CM are $\mathbb{Q}$-curves, so all CM j-invariants are $\mathbb{Q}$-numbers. We will be less interested in these, and will restrict ourselves to non-CM $\mathbb{Q}$-numbers; that is, $\mathbb{Q}$-numbers which are not CM j-invariants.

For $j \in \overline{\mathbb{Q}}$ we denote by $G(j)$ the finite set of Galois conjugates of j. Then the condition for j to be a $\mathbb{Q}$-number is that $G(j) \subseteq [j]$. In fact, if any element of an isogeny class is a $\mathbb{Q}$-number then they all are, so that the class is a union of Galois orbits.

Proposition A.10. *Let $j \in \overline{\mathbb{Q}}$ be a $\mathbb{Q}$-number. Then every $j' \sim j$ is a $\mathbb{Q}$-number.*

Proof. Suppose that $j' \sim j$ where j is a $\mathbb{Q}$-number. Applying $g \in G$ to an isogeny $j \to j'$ shows that $g(j) \sim g(j')$. Since $j \sim g(j)$ by hypothesis, it follows that $g(j') \sim j'$ for all $g \in G$. □

We call an isogeny class consisting of $\mathbb{Q}$-numbers a $\mathbb{Q}$-*class*. By Proposition A.10, the Galois action of G on $\overline{\mathbb{Q}}$ restricts to an action on each $\mathbb{Q}$-class. The simplest $\mathbb{Q}$-classes are isogeny classes containing a rational j, which we call *rational* $\mathbb{Q}$-classes. Any other $\mathbb{Q}$-class, and the $\mathbb{Q}$-numbers in it, are called *strict*. One of our goals is to find the simplest conjugacy class in a general $\mathbb{Q}$-class. In terms of elliptic curves, being isogenous to an elliptic curve with rational j-invariant certainly implies being a $\mathbb{Q}$-curve, by Proposition A.10, but we are interested in studying *strict* $\mathbb{Q}$-curves: $\mathbb{Q}$-curves which are not isogenous to a curve with rational j-invariant.

Let $j \in \overline{\mathbb{Q}}$ be a $\mathbb{Q}$-number. We define† the *degree* of j, or of its conjugacy class, to be the least common multiple of the degrees $\deg(j, g(j))$ for $g \in G$.

Lemma A.11. *Let $\mathcal{Q}$ be a $\mathbb{Q}$-class. For each $g \in G$, the class of the degree $\deg(j, g(j))$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is independent of $j \in \mathcal{Q}$.*

Proof. Let $j_1, j_2 \in \mathcal{Q}$. Since $\deg(j_1, j_2) = \deg(g(j_1), g(j_2))$ by Lemma A.6, it follows from Corollary A.2 that $\deg(j_1, g(j_1)) \equiv \deg(j_2, g(j_2)) \pmod{(\mathbb{Q}^*)^2}$. □

Corollary A.12. *If $\mathcal{Q}$ is a rational $\mathbb{Q}$-class then $\deg(j, g(j))$ is a square for all $j \in \mathcal{Q}$ and $g \in G$.*

The converse to this is also true, and will be proved later (see Proposition A.19 below). Note that it does not follow directly from Lemma A.11 that the square class of the degree is isogeny-invariant, though this will turn out to be true. The key result of Elkies is that every $\mathbb{Q}$-class contains some "central" j whose degree is square-free, this degree being the square-free part of the degree of every element of the class.

Lemma A.11 implies that for any $\mathbb{Q}$-class $\mathcal{Q}$ we have a well-defined map

$$\delta_{\mathcal{Q}} : G \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

given by $\delta_{\mathcal{Q}}(g) = \deg(j, g(j)) \pmod{(\mathbb{Q}^*)^2}$, where $j \in \mathcal{Q}$ is arbitrary.

Corollary A.13. *$\delta_{\mathcal{Q}}$ is a group homomorphism with finite image.*

Proof. For $g, h \in G$ we have

$$\deg(j, gh(j)) \equiv \deg(j, g(j)) \deg(g(j), gh(j)) = \deg(j, g(j)) \deg(j, h(j))$$

by Corollary A.2 and Lemma A.6. Finiteness is immediate since each conjugacy class $G(j)$ is finite. □

Denote the image of $\delta_{\mathcal{Q}}$ by $\delta(\mathcal{Q})$. Being a finite subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, it is an elementary abelian 2-group, isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\rho(\mathcal{Q})}$ for some $\rho(\mathcal{Q}) \geq 0$. The kernel of $\delta_{\mathcal{Q}}$ cuts out a Galois extension $L_{\mathcal{Q}}$ of $\mathbb{Q}$ of degree $2^{\rho(\mathcal{Q})}$ and Galois group isomorphic to $\delta(\mathcal{Q})$, so $L_{\mathcal{Q}}$ is a polyquadratic extension.

Looking only at the ℓ-primary part of the degree, and its exponent modulo 2, we obtain a character $\delta_\ell : G \to \{\pm 1\}$ which is trivial for all but finitely many ℓ, and otherwise cuts out a quadratic extension of $\mathbb{Q}$. Let $r = r(\mathcal{Q}) \geq 0$ be the number of primes ℓ for which δ_ℓ is nontrivial, and let $\ell_1, \ldots, \ell_{r(\mathcal{Q})}$ be these primes. For each ℓ_i, and for every $j \in \mathcal{Q}$, exactly half the degrees $\deg(j, g(j))$ have even ℓ_i-valuation and half odd; while for other primes ℓ, these valuations are all even.

*If $j \in \overline{\mathbb{Q}}$ is CM of degree h, associated to the imaginary quadratic discriminant D with class number h, then the elliptic curves whose j-invariants are the conjugates of j are $\mathbb{C}/\mathfrak{a}$ as $\mathfrak{a}$ runs over a set of proper $\mathcal{O}$-ideal class representatives where $\mathcal{O}$ is the order of discriminant D.

†The degree of j in this sense should not be confused with the degree of j as an algebraic number, *i.e.*, the degree of the field extension $\mathbb{Q}(j)/\mathbb{Q}$. Later we will also refer to the "degree" of a vertex in a graph whose vertices are algebraic numbers j.

Define the *level* $N = N(\mathcal{Q})$ of the $\mathbb{Q}$-class $\mathcal{Q}$ to be the product $\ell_1 \dots \ell_r$. By definition, the level is square-free; it also divides the degree of every $j \in \mathcal{Q}$, since half of the degrees $\deg(j, g(j))$ have odd ℓ_i-valuation and hence in particular are divisible by ℓ_i, so their gcd is divisible by ℓ_i. We will see later that the level is actually *equal* to the square-free part of the degree of every $j \in \mathcal{Q}$, by showing that the degree has odd ℓ-valuation if and only if $\ell \mid N$; at this point we only know the "only if" implication.

Clearly $\ker(\delta_{\mathcal{Q}})$ contains the intersection $\cap_i \ker(\delta_{\ell_i})$, which has index 2^r in G, but in general these subgroups of G are not equal. Hence we have $\rho \leq r$. However when $\rho = 0$ then $\delta_{\mathcal{Q}}$ is trivial, so $r = 0$ also.

If $\mathcal{Q}$ is a rational $\mathbb{Q}$-class, then $\rho(\mathcal{Q}) = r(\mathcal{Q}) = 0$, $N(\mathcal{Q}) = 1$, and $L_{\mathcal{Q}} = \mathbb{Q}$. Again, the converse to this is also true, and will be proved below in Proposition A.19.

When the class $\mathcal{Q}$ is fixed we will simplify notation and write $\rho = \rho(\mathcal{Q})$, $r = r(\mathcal{Q})$, $N = N(\mathcal{Q})$, *etc.*

A.2.1. *Central classes.* In a $\mathbb{Q}$-class $\mathcal{Q}$, an element j and its conjugacy class $G(j)$ are called *central* if their degree is square-free; equivalently, j is central if $\deg(j, g(j))$ is square-free for all $g \in G$. In the next section we will see that every $\mathbb{Q}$-class contains at least one central class. Here we assume the existence of such a class and draw several conclusions about it.

Theorem A.14. *Let $\mathcal{Q}$ be a $\mathbb{Q}$-class. Then for all central classes $C \subset \mathcal{Q}$,*

1. *$C \subseteq \mathbb{Q}(j)$ for all $j \in \mathcal{Q}$;*
2. *$\mathbb{Q}(C) = L_{\mathcal{Q}}$; in particular, $\mathbb{Q}(C)$ depends only on $\mathcal{Q}$;*
3. *the degree of C is $N(\mathcal{Q})$, and moreover the set of degrees between elements of C depends only on $\mathcal{Q}$.*

Proof. (1) Let $g \in G$, $j \in \mathcal{Q}$ and $j_1 \in C$. If $g(j) = j$, then $\deg(j, j_1) = \deg(g(j), g(j_1)) = \deg(j, g(j_1))$. Since $\deg(j_1, g(j_1))$ is square-free, $g(j_1) = j_1$ by Corollary A.3. Hence $\mathbb{Q}(j_1) \subseteq \mathbb{Q}(j)$.

(2) Let $j \in C$, and use j to define the map $\delta_{\mathcal{Q}}$. Now $g \in \ker(\delta_{\mathcal{Q}})$ if and only if $\deg(j, g(j))$ is a square, which is if and only if $j = g(j)$ since $\deg(j, g(j))$ is square-free. Hence the restriction of g to $\mathbb{Q}(C)$ is the identity if and only if $g \in \ker(\delta_{\mathcal{Q}})$, so $\mathbb{Q}(C) = L_{\mathcal{Q}}$ (by definition of $L_{\mathcal{Q}}$).

(3) The fact that all central classes have the same degree follows from Lemma A.11: if j and j' are both central, then the degrees $\deg(j, g(j))$ and $\deg(j', g(j'))$ are square-free numbers which are equivalent modulo squares and hence equal.

Let $N(j)$ be the degree of a central class $C = G(j)$. Using j to define the characters δ_ℓ, we see that δ_ℓ is nontrivial precisely when $\ell \mid N(j)$, so $N(j) = N(\mathcal{Q})$. □

Note that we have not yet proved the existence of any central classes, even when $\rho = 0$.

A.2.2. *Definition of the core.* Let $\mathcal{Q}$ be a $\mathbb{Q}$-class. We define a *core* of $\mathcal{Q}$ to be the Atkin-Lehner orbit of a central class. Thus the existence of a core will follow from the existence of at least one central class C in $\mathcal{Q}$. By Corollary A.8, all j-invariants in the core lie in the polyquadratic field $L_{\mathcal{Q}}$.

From the previous subsection we see that a core consists of 2^r elements, such that for any j in the core the degrees of the isogenies to the other core elements are *all* the divisors of the level $N = N(\mathcal{Q})$. The core is the union of $2^{r-\rho}$ central classes. The isogenies of degree N between elements of the core define a collection of 2^r distinct points on $X_0(N)$, which are closed under the actions of both the Galois group G and the group W of Atkin-Lehner involutions, and hence determine a rational point on the quotient $X_0^*(N) = X_0(N)/W$.

The simplest examples of a strict $\mathbb{Q}$-class are those with $\rho = 1$, where L is a quadratic field. Quadratic $\mathbb{Q}$-curves have been the subject of much study. In this case, a central class consists of a pair of $L/\mathbb{Q}$-conjugate j-invariants linked by a cyclic isogeny of square-free degree $N = \ell_1 \ell_2 \dots \ell_r$. The core consists of the complete Atkin-Lehner orbit of this isogeny, which has 2^r elements, in 2^{r-1} conjugate pairs, the invariants in each pair being linked by a cyclic N-isogeny.

A.3. **Construction of the core.** We now prove that central classes exist for every $\mathbb{Q}$-class. Our proof is similar to that of Elkies in [14], except that we use the quotient trees $\mathcal{Q}_\ell$ instead of subtrees, and we have already established several useful preliminaries. Let $\mathcal{Q}$ be a $\mathbb{Q}$-class. Applying the quotient construction, we obtain a tree $\mathcal{Q}_\ell$ for every prime ℓ. We now associate a finite subtree $T_\ell(j) \subset \mathcal{Q}_\ell$ to every conjugacy class $G(j)$ in $\mathcal{Q}$. Let N_0 be the degree of j. The image of $G(j)$ under π_ℓ is a finite subset of $\mathcal{Q}_\ell$, which is a singleton unless ℓ divides N_0. We define $T_\ell(j)$ to be the finite subtree of $\mathcal{Q}_\ell$ spanned by the conjugate vertices $\pi_\ell(g(j)) \in \mathcal{Q}_\ell$ for $g \in G$. Denote by n the diameter of $T_\ell(j)$; by definition of degree, this is the ℓ-valuation of N_0, being the maximum ℓ-valuation of $\deg(j, g(j))$ for $g \in G$. The leaves (vertices of degree 1) of $T_\ell(j)$ are precisely the vertices $\pi_\ell(g(j)) \in \mathcal{Q}_\ell$, by construction and the transitivity of the action of G on $G(j)$.

We will use a standard fact about finite trees T (see [15]), that they have a unique *centre*, which is either a vertex (when the diameter of T is even) or an edge (when the diameter is odd), such that every maximal

path in the tree passes through the centre. Since automorphisms of T take maximal paths to maximal paths, the centre of T is fixed by all automorphisms. Recall also that in a tree there is a unique path between any two vertices, whose length is defined to be the distance between the vertices. In $T_\ell(j)$ the distance between two leaves $\pi_\ell(j), \pi_\ell(j')$ is d where $\deg_\ell(j, j') = \ell^d$.

In our situation, $T_\ell(j)$ has a central vertex or edge when n is even or odd (respectively), and this centre is fixed by the action of G.

Proposition A.15. *The following are equivalent:*

(1) $\ell \nmid N(\mathcal{Q})$;
(2) *n is even;*
(3) *the distance between any two leaves of $T_\ell(j)$ is even;*
(4) *G has at least one fixed point in $T_\ell(j)$;*
(5) *G has at least one fixed point in $\mathcal{Q}_\ell$;*

Proof. (1) $\Leftrightarrow$ (3): by definition of the level.

(3) $\Rightarrow$ (2): obvious.

(2) $\Rightarrow$ (3), (4): When $n = 2m$ is even, $T_\ell(j)$ has a central point $\pi_\ell(j_0)$, which is fixed by G. Every leaf is at distance m from the centre, so the distances between leaves are all even.

(4) $\Rightarrow$ (5): obvious.

(5) $\Rightarrow$ (2) (by contrapositive): Suppose that $n = 2m + 1$ is odd, and that the central edge of $T_\ell(j)$ is $\pi_\ell(j_1) - \pi_\ell(j_2)$. Every $g \in G$ either fixes both vertices $\pi_\ell(j_1), \pi_\ell(j_2)$, or it interchanges them. Every leaf is at distance m from one of the central vertices and distance $m + 1$ from the other. Since G acts transitively on the leaves and preserves distance, there exists $g_0 \in G$ which does interchange $\pi_\ell(j_1)$ and $\pi_\ell(j_2)$. Moreover, such elements g_0 have no fixed points at all in $\mathcal{Q}_\ell$, since for all such points their distances from these two central vertices differ by 1; in fact, such g_0 interchange the subset of vertices of $\mathcal{Q}_\ell$ which are closer to $\pi_\ell(j_1)$ than to $\pi_\ell(j_2)$ with its complement. □

Corollary A.16. *With the same notation, when $n = 2m + 1$ is odd, the distance between any two leaves of $T_\ell(j)$ is either even and at most $2m$, or is equal to the diameter $2m + 1$.*

Proof. If two leaves are on the same side of the central edge then they are both at distance m from the closest central vertex, and hence the distance between them is even and at most $2m$. If they are on different sides, then the path between them passes through the central edge and has length $2m + 1$. □

Corollary A.17. *For all $j \in \mathcal{Q}$, the square-free part of the degree of j is equal to the level $N(\mathcal{Q})$.*

Proof. This is (1) $\Leftrightarrow$ (2) of the proposition, since n is the ℓ-valuation of the degree of j. □

Hence we have another characterization of the level of a $\mathbb{Q}$-class $\mathcal{Q}$: it is the product of the (finitely many) primes ℓ such that G has no fixed points on $\mathcal{Q}_\ell$, or equivalently the primes ℓ such that for all $j \in \mathcal{Q}$ there exists $g \in G$ such that $\ell \mid \deg(j, g(j))$.

Theorem A.18. *Every $\mathbb{Q}$-class has at least one central conjugacy class and hence a core.*

Before handling the general case, we start with the case of a $\mathcal{Q}$-class of level 1; that is, such that every j has square degree.

Proposition A.19. *Let $\mathcal{Q}$ be a $\mathbb{Q}$-class. Then $N(\mathcal{Q}) = 1$ if and only if $\mathcal{Q}$ is rational.*

Proof. If $\mathcal{Q}$ contains a rational j then $r(\mathcal{Q}) = 0$ and $N(\mathcal{Q}) = 1$. For the converse, suppose that $N(\mathcal{Q}) = 1$; we must show that there exists a rational $j_0 \in \mathcal{Q}$.

Let $j \in \mathcal{Q}$ be arbitrary. Since $N = 1$, for every prime ℓ the tree $T_\ell(j)$ has a central vertex $\pi_\ell(j_\ell)$. For all but finitely many ℓ, $T_\ell(j)$ is a singleton and we may take $j_\ell = j$; in all cases we may choose j_ℓ (in its class with respect to $\approx$) with $\deg(j, j_\ell)$ a power of ℓ. By Proposition A.9, there exists a (unique) $j_0 \in \mathcal{Q}$ such that $\pi_\ell(j_0) = \pi_\ell(j_\ell)$ for all ℓ. We claim that $j_0 \in \mathbb{Q}$.

Let $g \in G$ and let ℓ be any prime. Since $\pi_\ell(j_0) = \pi_\ell(j_\ell)$, it follows that $\deg(j_0, j_\ell)$ and $\deg(g(j_0), g(j_\ell))$ are prime to ℓ. Since g fixes $\pi_\ell(j_\ell)$, also $\deg(j_\ell, g(j_\ell))$ is prime to ℓ. Hence $\deg(j_0, g(j_0))$ is prime to ℓ. As this holds for all primes, $\deg(j_0, g(j_0)) = 1$; that is, $g(j_0) = j_0$. This holds for all $g \in G$, so $j_0 \in \mathbb{Q}$. □

In this minimal case, the core of the class is a singleton consisting of a single rational j-invariant. In general the core is not unique, as any rational number in the class is a core. However, the number of these is finite. To see this, we may combine the fact that over $\mathbb{Q}$ all isogeny classes of elliptic curves are finite with Lemma A.4.

Proof of Theorem A.18. Choose some element j in the $\mathbb{Q}$-class $\mathcal{Q}$. Let $\ell_1, \ldots, \ell_r$ be the prime factors of $N(\mathcal{Q})$, and for each i let the two vertices of the central edge of $T_{\ell_i}(j)$ be $\pi_\ell(j_i^\pm)$. Now, for each choice of signs $s = (s_1, \ldots, s_r) \in \{\pm\}^r$, the Chinese Remainder construction yields $j_s \in \mathcal{Q}$ such that $\pi_{\ell_i}(j_s) = \pi_{\ell_i}(j_i^{s_i})$ for all i, and also $\pi_\ell(j_s) = \pi_\ell(j)$ for $\ell \nmid N(\mathcal{Q})$. Let $C = \{j_s \mid s \in \{\pm\}^r\}$. Since G permutes each pair $\pi_{\ell_i}(j_i^\pm)$, it follows (as in the proof of Proposition A.19) that G acts on C. Explicitly, each $g \in G$ either fixes both $\pi_{\ell_i}(j_i^\pm)$ or swaps them over, so maps j_s to $j_{s'}$ where s' is obtained from s by changing some of the signs. Moreover, $\deg(j_s, g(j_s)) = \prod_i \ell^{\varepsilon_i}$ where $\varepsilon_i = 0$ when $g(\pi_{\ell_i}(j_i^+)) = \pi_{\ell_i}(j_i^+)$ and $\varepsilon_i = 1$ when $g(\pi_{\ell_i}(j_i^+)) = \pi_{\ell_i}(j_i^-)$; in particular, $\deg(j_s, g(j_s))$ is square-free. Hence the conjugacy class $G(j_s)$ is central.

Thus the action of G on C factors faithfully through a homomorphism $G \to (\mathbb{Z}/2\mathbb{Z})^r$, namely $g \mapsto (\varepsilon_1, \ldots, \varepsilon_r)$. The image has order $2^{\rho(\mathcal{Q})}$, and C is the closure of $G(j_s)$ under Atkin-Lehner involutions. □

The following corollary is useful for the $\mathbb{Q}$-curve testing algorithm, since it shows that the isogenies from a $\mathbb{Q}$-curve E defined over a number field K to the central curves in its isogeny class are defined over K itself. It also determines the smallest degree of an isogeny from E to a central $\mathbb{Q}$-curve in terms of the degree of E.

Corollary A.20. *Let K be a number field and let E be a non-CM $\mathbb{Q}$-curve defined over K.*

1. *There exists a central $\mathbb{Q}$-curve E_0 with an isogeny $\phi : E \to E_0$, where both E_0 and ϕ are also defined over K.*
2. *Let N be the degree of E (the least common multiple of the degrees of the isogenies between E and its Galois conjugates); write $N = N_0 M^2$ with N_0 square-free. Then the smallest degree of an isogeny $\phi : E \to E_0$ (as in part 1) is M, and the isogenies from E to the conjugates of E_0 have degree Mn for $n \mid N_0$.*

Proof. (1) Let $j = j(E) \in K$. By Theorem A.14, the core j-invariants are all in K. Taking j_0 to be any of these, we may take E_0 to be an elliptic curve defined over the core field $\mathbb{Q}(j_0)$ (and hence also defined over K), choosing the quadratic twist so that the isogeny $\phi : E \to E_0$ is also defined over $\mathbb{Q}(j, j_0) \subseteq K$ as in Lemma A.4.

(2) Write the degree of j as $N_0 M^2$ as in the statement. We use the notation of the proof of Theorem A.18, so $N_0 = \ell_1 \ldots \ell_r$. The degrees of the isogenies between j and the 2^r central j-invariants have ℓ_i-valuation either m_i or $m_i + 1$, where m_i is the valuation of M and $2m_i + 1$ that of N. Taking the product over all ℓ_i gives the result stated. □

References

[1] K. Arai, *On uniform lower bound of the Galois images associated to elliptic curves.* J. Théorie Nombres Bordeaux **20** (2008), 23–43. 3

[2] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman and J. Vonk, *Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13*, Ann. Math. (2) **189** (2019), 885–944. 3

[3] Juliana Belding, Reinier Bröker, Andreas Enge, Kristin Lauter. *Computing Hilbert Class Polynomials.* ANTS-VIII - Eighth Algorithmic Number Theory Symposium, May 2008, Banff, Canada, 282–295. 5.1

[4] N. Billerey. *Critères d'irréductibilité pour les représentations des courbes elliptiques,* Int. J. Number Theory, **7**, (2011), 1001–1032. 5.2.1

[5] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Ann. Math. (2), **173** (2011), 569–584. 3

[6] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on $X_0^+(p^r)(\mathbb{Q})$,* Ann. Inst. Fourier (Grenoble) **63** (2013), 957–984. 3

[7] 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

[8] A. Bourdon and P. L. Clark, *Torsion points and isogenies on CM elliptic curves*, Proc. London Math. Soc. to appear 3

[9] A. Bourdon, P. L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Trans. Amer. Math. Soc. **369** (2017), 8457–8496. 4

[10] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN **2017** (2017), 4923–4961. 4

[11] J. Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp. to appear. 1

[12] 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. 1

[13] P. Bruin, F. Najman, *Fields of definition of elliptic curves with prescribed torsion,* Acta Arith. **181** (2017), 85–96. 3

[14] N. Elkies, *On elliptic K-curves*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser Basel, 2004, 81–91. 1, A, A.1.4, A.3

[15] C. Jordan, Sur les assemblages des lignes, J. Reine Angew. Math. **70** (1869), 185–190. A.3

[16] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. **323** (2020), 1457–1485. 3, 4, 4

[17] E. González-Jiménez and F. Najman, *An algorithm for determining torsion growth of elliptic curves,* Exp. Math. to appear. `https://arxiv.org/abs/1904.07071` 3

[18] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **108** (2014), 923–934. 4
[19] T. Gužvić, *Torsion of elliptic curves with rational j-invariant defined over number fields of prime degree*, preprint. `https://arxiv.org/abs/1912.04037` 4, 4.2
[20] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields* Astérisque, **228** (1995), 81–98. 4
[21] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. **178** (2009), 485–504. 1
[22] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), 505–586. 1
[23] J. Klaise, *Orders in imaginary quadratic fields of small class number*, University of Warwick Undergraduate Masters thesis, unpublished (2012). 5.1
[24] S. Le Fourn, *Surjectivity of Galois representations associated with quadratic $\mathbb{Q}$-curves,* Math. Ann. **365** (2016), 173–214. 1
[25] S. Le Fourn and F. Najman, *Torsion of $\mathbb{Q}$-curves over quadratic fields,* Math. Res. Letters **27** (2020), 209–225. A.1.2
[26] D. Kohel, *Echidna Databases: Databases for Elliptic Curves and Higher Dimensional Analogues*, available from `https://www.i2m.univ-amu.fr/perso/david.kohel/dbs/index.html` (accessed 11 August 2020). 5.1, 5.2.2
[27] E. Larson and D. Vaintrob, *On the surjectivity of Galois representations associated to elliptic curves over number fields.* Bull. Lond. Math. Soc. **46** (2014), 197–209. 5.2.1
[28] The LMFDB Collaboration, The L-functions and Modular Forms Database, `http://www.lmfdb.org` 1
[29] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 1, 5.1
[30] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1978), 33–186. 1, 4
[31] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. 1, 3, 3
[32] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996) 437–449. 1
[33] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Letters, **23** (2016), 245–272.
[34] 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, 3
[35] O. Propp, *Cartan images and ℓ-torsion points on elliptic curves with rational j-invariant*, Res. Number Theory **4** (2018) 1
[36] A. Reverter and N. Vila, *Images of mod p Galois representations associated to elliptic curves*, Canad. Math. Bull. **44** (2001), 313–322, 4
[37] 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
[38] W. A. Stein et al. *Sage Mathematics Software (Version 9.2)*. The Sage Development Team, 2020. `http://www.sagemath.org`. 1
[39] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331. 3
[40] J . H. Silverman, *The arithmetic of elliptic curves*, Springer GTM 106 (1986). A
[41] K. Tsukazaki, *Explicit isogenies of elliptic curves*, University of Warwick PhD thesis, 2013. `http://wrap.warwick.ac.uk/57568/`. 5.2.2
[42] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907–938. 5.1
[43] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$,* preprint. `http://www.math.cornell.edu/~zywina/papers/PossibleImages/PossibleImages.pdf` 3

Mathematics Institute, University of Warwick, Coventry CV4 7AL, UK
Email address: `j.e.cremona@warwick.ac.uk`

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