

\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 that a \mathbb{Q} -curve without CM may have are those degrees that 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, that 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -conjugates. 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 [22, 23]) 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 [15], and as will be later explained in more detail, \mathbb{Q} -curves in a sense arise most naturally over number fields of degree 2^n . In particular, the first place one looks for \mathbb{Q} -curves that 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 [25] showed that for every strict \mathbb{Q} -curve E over a fixed imaginary quadratic field K , there exists a uniform bound C_K such that for $\ell > C_K$, the mod ℓ representation attached to E is surjective. Bruin and Najman [12] and Box [10] showed that for each N such that the modular curve $X_0(N)$ is hyperelliptic, for all but finitely many explicitly listed exceptional elliptic curves, an elliptic curve over a quadratic field with an N -isogeny is a \mathbb{Q} -curve. Bosman, Bruin, Dujella and Najman [6] 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 [25] 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 [15] concerning \mathbb{Q} -curves and their generalizations. 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, that 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 more generally fields 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

Date: September 14, 2021.

Cremona was supported by the Heilbronn Institute for Mathematical Research.

Najman was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.

an odd degree number field. These results fit into the long-standing program, going back to Levi and Ogg and whose most famous results include Mazur's torsion and isogeny theorems [31, 32], of describing the possible torsion groups and isogeny structures of elliptic curves over number fields. Our results are reminiscent of Merel's uniform boundedness theorem [33], but we will obtain absolute bounds, not depending even on the degree of the number field, on degrees of isogenies of non-CM \mathbb{Q} -curves over odd degree number fields.

In Section 3 we obtain the following results.

Theorem 1.1. *Let E be a \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 $n \leq 37$.*

Clearly, if E is an elliptic curve over \mathbb{Q} and ℓ is any prime, then for a suitable extension K/\mathbb{Q} (generically of degree $\ell + 1$), the base-change of E from \mathbb{Q} to K will acquire an ℓ -isogeny. The point of Theorem 1.1 is that except for the eight primes ℓ listed, K will always have even degree.

We show that even if we include CM curves, 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.

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 .*

We expect that Theorem 1.2 should also hold for even degrees d , once CM curves have been excluded, but new methods would be required to prove such a general uniformity result.

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, which is a generalization of [17, Theorem 7.2. (i)].

Theorem 1.3. *Let p be a prime > 7 , let K be a number field of degree p and E/K a \mathbb{Q} -curve. Then $E(K)_{\text{tors}}$ 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} .*

Note that this result does not hold for $p = 2, 3, 5$. For example, the \mathbb{Q} -curves with LMFDB labels 2.2.17.1-100.1-e2 over $\mathbb{Q}(\sqrt{17})$ and 3.3.49.1-27.1-a2 over the cubic subfield of $\mathbb{Q}(\zeta_7)$ both have torsion order 13, and the \mathbb{Q} -curve with label 5.5.14641.1-121.1-a1 over the quintic subfield of $\mathbb{Q}(\zeta_{11})$ has torsion order 11. We do not know of counterexamples in degree 7, and it is possible that our methods might be extended to include that case.

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 that 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 can 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`[30]. 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 [29]), which (as of August 2020) are defined over fields of degree at most 6, are \mathbb{Q} -curves. Our `SageMath` code is available at [14].

All examples of elliptic curves given in the text are identified with their LMFDB labels and may be found in the LMFDB database [29].

Acknowledgments. We thank Samuel Le Fourn for helpful conversations and suggestions, Andrew Sutherland for the references [11] and [43], Abbey Bourdon for several useful remarks on a previous version of the paper and the referees for their careful reading and helpful suggestions for improving the exposition; we have added many details to several proofs at the referee's request.

2. PROPERTIES OF Q-CURVES

We recall here the definition of a 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 $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A 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 Q-number is an algebraic number j that is the j -invariant of a Q-curve. If j is a Q-number then so are all its Galois conjugates (see Proposition A.10). All CM curves are Q-curves; however, here we will mainly be interested in non-CM 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 that is the degree of a *cyclic* isogeny $E_1 \rightarrow E_2$, where again $j(E_i) = j_i$, denoted $d(j_1, j_2)$ (see Lemma A.1).

A Q-class is an isogeny class $\mathcal{Q} \subset \overline{\mathbb{Q}}$ consisting of Q-numbers. The *isogeny degree* of a Q-number j is the least common multiple of the degrees $d(j, g(j))$ for $g \in G_{\mathbb{Q}}$. A Q-number is *central* if it has square-free isogeny degree, in which case its Galois conjugacy class is called a *central class*. The existence of a central class in every Q-class is established in Theorem A.17, and in Theorem A.13 and Proposition A.18 we prove the other assertions of the following theorem:

Theorem 2.1. *Let \mathcal{Q} be a non-CM Q-class in $\overline{\mathbb{Q}}$. Then \mathcal{Q} contains at least one central conjugacy 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 $\text{Gal}(\mathbb{Q}(C)/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^\rho$;
- (3) the isogeny degree N of one (and hence all) $j \in C$ is a product of r distinct 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 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 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 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 isogeny degree as defined above for a Q-number j .

Proposition 2.2. *Let j be a Q-number in the non-CM 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.13, and $L_{\mathcal{Q}}$ has degree $2^{\rho(\mathcal{Q})}$. □

Proposition 2.3. *For a non-CM 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 Q-class is called *rational* when it satisfies one (and hence all) of the conditions of Proposition 2.3.

Theorem 2.4 (The odd degree theorem). *If the non-CM 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. For example, let p be a prime such that $p \equiv 3 \pmod{4}$ and $p > 163$, let $\mathcal{O} = \mathbb{Z} \left[\frac{1+\sqrt{-p}}{2} \right]$ be the order of discriminant $-p$, and let $j = j((1 + \sqrt{-p})/2)$. Since \mathcal{O} has prime discriminant, its class number h is odd (by genus theory),

and $h > 1$ since $p > 163$. Hence (by standard facts from Class Field Theory), j is an algebraic integer of odd degree $h > 1$. Every element of $\mathbb{Q}(j)$ is the j -invariant of an elliptic curve with CM by an order in $\mathbb{Q}(\sqrt{-p})$, so has degree a multiple of h . Hence $\mathbb{Q}(j) \cap \mathbb{Q} = \emptyset$.

More generally:

Theorem 2.5 (The no-quadratic-subfields theorem). *If the non-CM \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. \square

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. 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. The following theorem is proved in the Appendix in Corollary A.19.

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 $\phi: E \rightarrow E_0$, 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 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. \square

3. ISOGENIES OF \mathbb{Q} -CURVES OVER ODD DEGREE NUMBER FIELDS

Let K be a number field and $G_K = \text{Gal}(\overline{K}/K)$ 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 $K(C)$, or in other words, the smallest number field such that $\text{Gal}(\overline{K(C)}/K(C))$ 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 $E[\ell]$ and define $\overline{\rho}_{E,\ell}: G_K \rightarrow \text{GL}_2(\mathbb{F}_\ell)$ 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 $\left\{ \begin{pmatrix} * & \\ 0 & * \end{pmatrix} \right\}$ of $\text{GL}_2(\mathbb{F}_\ell)$, which has index $\ell + 1$, and let B_1 denote the subgroup $\left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\}$, which is normal of index $\ell - 1$ in B . Then

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

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, $[K(C) : K] = [\overline{\rho}_{E,\ell}(G_K) : B \cap \overline{\rho}_{E,\ell}(G_K)] \leq \ell + 1$. \square

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 , that 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. If $j(E_1), j(E_2) \notin \{0, 1728\}$ then the set of reducible primes is the same for E_1 and E_2 that are isogenous over \bar{K} .*

Proof. First assume that E_1 and E_2 are isogenous over K . By Proposition A.7 we may assume that the given isogeny $\phi: E_1 \rightarrow E_2$ 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 that 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 .

Now suppose that $j(E_1), j(E_2) \notin \{0, 1728\}$ and that E_1 and E_2 are isogenous over \bar{K} . By Lemma A.4 there exists a quadratic twist E'_1 of E_1 such that E'_1 and E_2 are isogenous over K . Since the set of reducible primes is quadratic-twist-invariant it follows by what has already been proved that E_1 and E_2 have the same set of reducible primes. \square

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 let ℓ be an odd 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, unless $j(E) = 2268945/128$, in which case E acquires 7-isogenies over the cubic field generated by a root of $x^3 - 5x - 5$.*

Proof. If $\bar{\rho}_{E,\ell}$ 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, if $\ell \geq 17$ and E does not have an ℓ -isogeny over \mathbb{Q} , by the results of [4, 5, 32, 39] the projective image $\mathbb{P}\bar{\rho}_{E,\ell}(G_K)$ 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 [45, Proposition 1.13], the projective image is either the whole normaliser or an index 3 subgroup, hence has order either $2(\ell + 1)$ or $2(\ell + 1)/3$. Since Borel subgroups of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ have order $\ell(\ell - 1)$, the intersection of the projective image with each Borel subgroup is cyclic of order dividing $\gcd(\ell + 1, \ell - 1) = 2$, and hence 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 [17, Table 2] (where all the non-surjective possibilities are listed), and we can see that if E does not have a 13-isogeny and $\bar{\rho}_{E,13}$ 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 $\bar{\rho}_{E,\ell}(G_K)$ are known and from [17, 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 results hold when we replace the base field \mathbb{Q} by a field K (of characteristic not ℓ), provided that $\sqrt{5} \notin K$ when $\ell = 5$. For all $\ell \geq 3$, 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. We claim that the discriminant of f modulo squares is $\ell^* = \pm\ell$, the sign being taken so that $\ell^* \equiv 1 \pmod{4}$.

Granted the truth of the claim, our assumption that E has no ℓ -isogenies defined over K means that 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 .

Now let $\ell = 7$. If f has irreducible factors of odd degree and no rational roots, it must factor as $f = gh_1h_2$ where g has degree 2 and h_1, h_2 both have degree 3. (As we saw in the case $\ell = 5$, if there is an irreducible factor of degree 3 then its splitting field contains all the roots of f , so f cannot also have an irreducible factor of degree 5.) Both h_1 and h_2 have the same splitting field, which contains that of g , so f has Galois group isomorphic to S_3 , and, since $\mathrm{disc}(f) = -7$ (modulo squares) by our claim, all three factors have discriminant -7 (modulo squares). Now the nontrivial elements of the Galois group of f either have order 2 and act on each set of conjugate roots via a transposition, fixing one root of each of the cubic factors; or have order 3, acting as 3-cycles on the cubic roots and fixing both quadratic roots. Hence every element of the Galois group of f fixes at least one root of f , so E admits 7-isogenies modulo p for almost all primes p , the situation described by Sutherland in detail in [42]. By [42, Section 3], this is only possible when $j(E) = 2268945/128$.

The polynomial $\Phi_7(X, 2268945/128)$ has two irreducible factors of degree 3 whose roots each generate a cubic field isomorphic to $\mathbb{Q}[x]/(x^3 - 5x - 5)$, and a quadratic factor which splits over $\mathbb{Q}(\sqrt{-7})$.

It remains to prove the claim. The faithful action of $\mathrm{PGL}(2, \mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$ determines (after fixing a labelling of the points on the projective line) an injective group homomorphism $\pi: \mathrm{PGL}(2, \mathbb{F}_\ell) \rightarrow S_{\ell+1}$, the symmetric group on $\ell + 1$ letters. Identifying the roots of f with $\mathbb{P}^1(\mathbb{F}_\ell)$, we see that the composite $\pi \circ \bar{\rho}_{E, \ell}: G_K \rightarrow S_{\ell+1}$ gives the permutation action of G_K on the roots of f . The image of π is not contained in the alternating group $A_{\ell+1}$, since if a generates \mathbb{F}_ℓ^* then $\pi \left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \right)$ is an $\ell - 1$ -cycle, which is odd.

Hence the preimage under π of $A_{\ell+1}$ has index 2 in $\mathrm{PGL}(2, \mathbb{F}_\ell)$, and must therefore be $\mathrm{PSL}(2, \mathbb{F}_\ell)$, as this is the unique such subgroup: for $\ell \geq 5$ this follows from the simplicity of $\mathrm{PSL}(2, \mathbb{F}_\ell)$, while for $\ell = 3$ the map π is an isomorphism. Hence, for all extensions L/K , the image $\bar{\rho}_{E, \ell}(G_L)$ is contained in $\mathrm{PSL}(2, \mathbb{F}_\ell)$ if and only if $\pi(\bar{\rho}_{E, \ell}(G_L)) \subseteq A_{\ell+1}$, which is if and only if $\mathrm{disc}(f)$ is a square in L by standard Galois theory.

On the other hand, for $g \in G_K$ we have $\bar{\rho}_{E, \ell}(g) \in \mathrm{PSL}(2, \mathbb{F}_\ell)$ if and only if $\det \rho_{E, \ell}(g) \in (\mathbb{F}_\ell^*)^2$. Since the determinant of $\rho_{E, \ell}$ is the ℓ 'th cyclotomic character, this holds if and only if $g(\sqrt{\ell^*}) = \sqrt{\ell^*}$. Thus $\mathrm{disc}(f)$ is a square in L if and only if $\sqrt{\ell^*} \in L$, and so $K(\sqrt{\ell^*}) = K(\sqrt{\mathrm{disc}(f)})$ as claimed. \square

Corollary 3.4. *Let E be an elliptic curve without CM defined over a number field K 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 $j(E_0) = j$. The same holds for $\ell = 7$, unless $j = 2268945/128$ and K contains a root of $x^3 - 5x - 5$.*

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. \square

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 196.a1. Equivalently, the image of the mod 2 representation attached 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 $d = 3$.

As an example of the exceptional case when $\ell = 7$, the elliptic curve 2450.i1 has j -invariant $2268945/128$, and 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 $\mathbb{Q}(\sqrt{-7})$.

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]. When $d = 1$, the set of set of prime degrees of isogenies of non-CM elliptic curves defined over \mathbb{Q} is

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

by [32].

We can now prove Theorem 1.1 a), that the only primes ℓ that are reducible for a non-CM \mathbb{Q} -curve defined over a number field of odd degree are those that are in $J_{\mathbb{Q}}(1)$.

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 in $J_{\mathbb{Q}}(1)$. \square

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, as there exist composite isogeny degrees between \mathbb{Q} -curves that appear over odd degree number fields but not over \mathbb{Q} .

In the proof of the next Proposition, and also later (Proposition 4.1), we will need some elementary properties of the *affine linear group* $\mathrm{AGL}_1(\mathbb{F}_\ell)$, which we identify with a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$:

$$\mathrm{AGL}_1(\mathbb{F}_\ell) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_\ell^*, b \in \mathbb{F}_\ell \right\}.$$

Lemma 3.5. *The group $\mathrm{AGL}_1(\mathbb{F}_\ell)$ has the following properties:*

- (1) *It acts transitively on \mathbb{F}_ℓ via $x \mapsto ax + b$.*
- (2) *It has order $\ell(\ell - 1)$, and is the semidirect product of the additive group \mathbb{F}_ℓ and the multiplicative group \mathbb{F}_ℓ^* , fitting in the short exact sequence*

$$0 \longrightarrow \mathbb{F}_\ell \longrightarrow \mathrm{AGL}_1(\mathbb{F}_\ell) \longrightarrow \mathbb{F}_\ell^* \longrightarrow 1,$$

the inner maps being $b \mapsto \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mapsto a$.

- (3) *For every subgroup $H \leq \mathrm{AGL}_1(\mathbb{F}_\ell)$, one of two cases occurs: either H has order divisible by ℓ , acts transitively on \mathbb{F}_ℓ and has a subgroup of index ℓ ; or is cyclic of order dividing $\ell - 1$, acts on \mathbb{F}_ℓ with orbits of size dividing $\ell - 1$, with at least one fixed point.*

Proof. Elementary. In (3) if H is nontrivial and cyclic of order dividing $\ell - 1$ and generated by $g = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$, then $a \neq 1$ and $b/(1 - a)$ is a fixed point of the action of g (and hence H). \square

Proposition 3.6. *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 $\rho_{E,\ell} : G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the ℓ -adic representation attached to E/K . 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

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

Note that, as $n \geq 2$, G_n has index ℓ in G_{n-1} . Write $\rho = \rho_{E,\ell}$ and $H_m = \rho(G_K) \cap G_m$ for $m = n, n - 1$. Since $\ker \rho \subseteq G_{K(C)}$ (a Galois automorphism which fixes all ℓ -power torsion points fixes all the points of C and hence certainly fixes $K(C)$), we have

$$[K(C) : K(\ell C)] = [G_{K(\ell C)} : G_{K(C)}] = [\rho(G_{K(\ell C)}) : \rho(G_{K(C)})] = [\rho(G_K) \cap G_{n-1} : \rho(G_K) \cap G_n] = [H_{n-1} : H_n].$$

We must show that this index is either ℓ or a divisor of $\ell - 1$.

The map $\pi : G_{n-1} \rightarrow \mathrm{AGL}_1(\mathbb{F}_\ell)$ defined by $\begin{pmatrix} a & b \\ \ell^{n-1} c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{d}/\bar{a} & \bar{c}/\bar{a} \\ 0 & 1 \end{pmatrix}$ is a surjective group homomorphism, so that G_{n-1} acts transitively on \mathbb{F}_ℓ via $\begin{pmatrix} a & b \\ \ell^{n-1} c & d \end{pmatrix} : x \mapsto (\bar{d}x + \bar{c})/\bar{a}$. Under this action, the stabiliser of 0 is G_n . (Here the bar denotes reduction modulo ℓ , and a is a unit in \mathbb{Z}_ℓ since $n \geq 2$). Hence the index of $H_n = G_n \cap H_{n-1}$ in H_{n-1} is the size of the orbit of 0 under H_{n-1} . By Lemma 3.5(3) the orbit size is either ℓ or is a divisor of $\ell - 1$, as required. \square

We will need a result about degrees of fields of definition of isogenies that is, in certain instances, more precise than Proposition 3.6. Before stating and proving it, we introduce a definition.

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

Proposition 3.7. *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 $E(\bar{K})$ of order ℓ^n , we have $[K(C) : K(\ell C)] = \ell$.*

Proof. In the notation of the proof of Proposition 3.6, the image of H_{n-1} in the affine group contains elements of order ℓ , and hence acts transitively. \square

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 $G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell) \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell/\ell^n \mathbb{Z}_\ell)$.

Remark. The result of Proposition 3.6 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 $\Gamma_0(\ell^2) \cap \Gamma_1(\ell) \bmod \ell^2$. 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 11.a3.

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 3.8. *Let d be an odd 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 $\phi: E \rightarrow E'$ 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. By Theorem 2.7 we conclude that E is isogenous to an elliptic curve E' with $j(E') \in \mathbb{Q}$. By Corollary 3.4, there exists an elliptic curve E''/\mathbb{Q} with $j(E'') = j(E')$ such that the degrees of isogenies of E' and E'' are the same.

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 over K 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 3.6. \square

Proof of Theorem 1.1 b). This follows directly from Proposition 3.8. \square

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 [7, 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 E' with CM by the ring of integers of the CM field of E ; as E' certainly satisfies the conditions of [7, Theorem 5.3. b)] its possible degrees of ℓ -power isogenies are bounded so it follows that the degrees of the possible ℓ -power isogenies on E over K are also bounded.

Suppose now that E does not have CM. By Theorem 2.7 we know E is isogenous to an elliptic curve E' with $j(E') \in \mathbb{Q}$. By Corollary 3.4, there exists an elliptic curve E'' with $j(E'') = j(E')$ such that the degrees of isogenies of E' and E'' are the same. We will bound the possible degree of an isogeny of E'' from which a bound on the possible degree of an isogeny of E immediately follows.

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 K of degree d . 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 3.7, we can conclude that if E'' has an isogeny of degree ℓ^k for $k > B_{\ell}$, then d is divisible by $\ell^{k-B_{\ell}}$. It follows that $\nu_{\ell}(N) \leq \nu_{\ell}(d) + B_{\ell}$. \square

Remark. If one knows all the B_{ℓ} in the proof of the previous theorem, then C_d can be effectively computed. Using the notation above, if E''/\mathbb{Q} has an ℓ -power isogeny of degree at most ℓ^a over a number field K of odd degree, then it follows that E has an ℓ -power isogeny of degree at most ℓ^{2a} over K , coming from the possible isogeny diagram

$$E \xleftarrow{\ell^a} E'' \xrightarrow{\ell^a} E^{\sigma}.$$

For elliptic curves without CM, we get the bound:

$$C_d^{\text{nonCM}} := \prod_{\ell \in J(\mathbb{Q})} \ell^{2(\nu_{\ell}(d) + B_{\ell})}.$$

For elliptic curves with CM, one can produce a bound C_d^{CM} using the results of [7]. Finally, set

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

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 [18, 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 [21, 19, 20]) 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 [31], we have that

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

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_0 with $j(E_0) \in \mathbb{Q}$. There exists a quadratic twist E' of E_0 such that E' is defined over \mathbb{Q} . Since $E(K)$ has a point of order ℓ , by Proposition 3.2, E_0 has an ℓ -isogeny over K , and since having an ℓ -isogeny is a quadratic-twist-invariant property, it follows that 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. Let K_0 be the field of definition of an isogeny between E and E' ; it is either K or a quadratic extension of K .

By [17, Tables 1 and 2] we see that $E'(K_0)$ cannot have a point of order ℓ over a number field of degree $2d$ where d is not divisible by any prime ≤ 7 . Then the fact that $E(K_0)$ has a point of order ℓ , together with [36, Proposition 1.4], implies that, up to conjugation, we have

$$H = \bar{\rho}_{E', \ell}(G_{K_0}) = \begin{pmatrix} \chi_{\ell}(G_{K_0}) & * \\ 0 & 1 \end{pmatrix},$$

with $*$ nonzero, so H is a subgroup of $\text{AGL}_1(\mathbb{F}_{\ell})$. Observe that $x \in \mathbb{F}_{\ell}$ is a fixed point of H with respect to its action on \mathbb{F}_{ℓ} if and only if $\begin{pmatrix} x \\ 1 \end{pmatrix} \in \mathbb{F}_{\ell}^2$ (viewed as an element of $E'[\ell]$) is a fixed point with regard to the action of H on $E'[\ell]$. Since $E'(K_0)$ has no points of order ℓ , it follows that H has to act without fixed points on $E'[\ell] \setminus \{0\}$, so H acts without fixed points on \mathbb{F}_{ℓ} . By Lemma 3.5 (3) we conclude that H has a subgroup S of index ℓ .

It then follows from Galois theory that the fixed field K' of S is of degree ℓ over K_0 and such that $\bar{\rho}_{E', \ell}(G_{K'}) = S$. By the same argument as before we conclude that the action of $\bar{\rho}_{E', \ell}(G_{K'})$ (and hence $G_{K'}$) on $E'[\ell]$ has a fixed point so E' has a point of order ℓ over K' .

But then E' has a point of order ℓ over K' , of degree ℓd or $2\ell d$, where d is not divisible by any prime ≤ 7 , again contradicting [17, Tables 1 and 2]. \square

Recall the following result of Gužvić.

Theorem 4.2 ([20, 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 [17, 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 [9, 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 [17, Proposition 4.6] we see that $[\mathbb{Q}(P') : \mathbb{Q}]$ has to divide $\ell^2(\ell - 1)$. Since $[K : \mathbb{Q}] = d$, it follows that $[\mathbb{Q}(P') : \mathbb{Q}]$ divides $2d$. Hence $[\mathbb{Q}(P') : \mathbb{Q}]$ divides $\gcd(\ell^2(\ell - 1), 2d)$ and since d is not divisible by any prime ≤ 7 , we conclude that $[\mathbb{Q}(P') : \mathbb{Q}]$ divides 2. It follows that 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 [17, Theorem 5.8], we see that $[\mathbb{Q}(P') : \mathbb{Q}]$ has to be divisible by 4 for $\ell \geq 17$. For $\ell \leq 13$, we see that $[\mathbb{Q}(P') : \mathbb{Q}]$ is never of the form $2t$, with $t > 1$ divisible by primes ≥ 7 . Hence it again follows that $\mathbb{Q}(P')$ is a quadratic field.

Thus $\mathbb{Q}(P') = \mathbb{Q}(\sqrt{\delta_0})$ for some $\delta_0 \in K^*$, 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 subgroups of groups in $\Phi_{j \in \mathbb{Q}}(d)$ are all also subgroups of groups 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 $1 \leq n \leq 4$ 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. \square

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 [8, 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 a curve E' defined over \mathbb{Q} . Let $\phi : E' \rightarrow E$ 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 \mathbb{Q})

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

Let $\ell \leq 7$ be a divisor of n . As the degree of K is, by assumption, coprime to $\#\bar{\rho}_{E', \ell}(G_{\mathbb{Q}})$ (which is a divisor of $\ell(\ell - 1)^2(\ell + 1)$ since $\bar{\rho}_{E', \ell}(G_{\mathbb{Q}})$ is a subgroup of $\text{GL}_2(\mathbb{F}_\ell)$) for all $\ell \leq 7$, we conclude that $K \cap \mathbb{Q}(E'[\ell]) = \mathbb{Q}$ so $\bar{\rho}_{E', \ell}(G_{\mathbb{Q}}) = \bar{\rho}_{E', \ell}(G_K)$, 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'' that is isogenous over K to E . Since E''^δ is isogenous over K to E by an isogeny of degree coprime to $E(K)_{\text{tors}}$ and $E''^\delta(K)_{\text{tors}}$, it follows that $E(K)_{\text{tors}} \simeq E''^\delta(K)_{\text{tors}}$, and hence $E(K)_{\text{tors}} \in \Phi_{j \in \mathbb{Q}}(p) = \Phi(1)$, with the last equality following from Theorem 4.3. \square

5. A \mathbb{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, or equivalently, whether a given algebraic number j is a \mathbb{Q} -number. We assume that we know how to test whether E is CM, and also that we can compute the K -isogeny class of E —though, as we

will see, only a weak form of the latter is needed. We start with a brief discussion of these two questions. The main algorithm then 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. Both `SageMath` and `Magma` have functions for testing whether an algebraic number is a CM j -invariant. We therefore say no more about such tests here, except to remark that for each degree h there are only finitely many CM j -invariants of degree h , and complete lists of these have been computed for all $h \leq 100$, so that for small degrees the tests just amounts to checking that j is an algebraic integer whose minimal polynomial is in a precomputed list. For example, the total number for $h \leq 10$ is 705. See [44] for a list of all fundamental negative discriminants with class number $h \leq 100$, and for the extension including non-fundamental discriminants, see [24]; given a discriminant $D < 0$, the Hilbert Class Polynomial $H_D(X)$ is the minimal polynomial of the associated j -invariants.

5.2. Computing the K -isogenous j -invariants (for non-CM curves). Given a non-CM elliptic curve E defined over a number field K , the problem of computing the complete (finite) set of K -isomorphism classes of elliptic curves isogenous to E over K can be divided into three steps: first, determine the finite set of reducible primes ℓ ; next, 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. This procedure is implemented in `SageMath`, though not yet in `Magma` (except over \mathbb{Q}). For our purposes, it suffices to use a simpler (and faster) procedure that outputs a list of isogenous j -invariants that is not necessarily complete, which we describe briefly here.

5.2.1. Determining the reducible primes. The difficult problem of computing the complete finite set of reducible primes for a non-CM elliptic curve E , has been solved both by Larson and Vaintrob in [27] and also by Billerey in [3]; both methods are implemented in `SageMath` (see [28]). For our application to \mathbb{Q} -curve testing, however, it will suffice to only implement a simple necessary test for reducibility. If ℓ is reducible, then for all primes \mathfrak{p} of good reduction, the integer $a_{\mathfrak{p}}(E)^2 - 4N(\mathfrak{p})$ must be a square (possibly zero) modulo ℓ , since it is the discriminant of the characteristic polynomial of $\bar{\rho}_{E,\ell}(\text{Frob } \mathfrak{p})$, whose eigenvalues lie in \mathbb{F}_{ℓ} . (Here, $a_{\mathfrak{p}}(E)$ denotes the trace of Frobenius of the reduction of E at \mathfrak{p} , whose reduction modulo ℓ is the trace of $\bar{\rho}_{E,\ell}(\text{Frob } \mathfrak{p})$, while $\det \bar{\rho}_{E,\ell}(\text{Frob } \mathfrak{p}) \equiv N(\mathfrak{p}) \pmod{\ell}$.) Computing these integers for all \mathfrak{p} with norm less than some bound, we can discard any primes ℓ modulo which any of the integers is a quadratic non-residue. Using this, it is very fast to determine a small set of primes ℓ up to some bound 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, but this is not needed for the \mathbb{Q} -curve test.

The `SageMath` command `E.reducible_primes()` will, if E is not CM, return a provably complete list of the reducible primes ℓ for E , while `E.reducible_primes(algorithm='heuristic', max_l=B)` returns the set of reducible primes less than B .

5.2.2. Computing ℓ -isogenous j -invariants. For any fixed prime ℓ we may compute the j -invariants of elliptic curves ℓ -isogenous to E over K by finding the roots in K of $\Phi_{\ell}(X, j(E))$. Using the methods of [11] it is practical to compute $\Phi_{\ell}(X, Y)$ for primes $\ell < 5000$, and a precomputed database for $\ell \leq 300$ is available at [43]. By comparison, the largest reducible prime for any non-CM elliptic curve in the LMFDB database is currently (September 2020) $\ell = 41$, which occurs for four isogeny classes over $\mathbb{Q}(\sqrt{-1})$, for example the class with label 2.0.4.1-84050.1-b.

Iterating this process, we can compute, starting from any $j \in K$, a possibly complete list of isogenous $j' \in K$ linked to j by isogenies of degrees supported on primes $\ell \leq B$ for some bound B . This list is either known to be complete, if for B we take a rigorous bound such as provided by Billerey’s algorithm, or not, and the \mathbb{Q} -curve testing algorithm will take this into account.

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 that are easy to check, since obviously if any of these fail then we know that the curve is not a \mathbb{Q} -curve. 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 that is valid when K is not necessarily Galois and that 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 $d_{\mathfrak{p}} = a_{\mathfrak{p}}(E)^2 - 4N(\mathfrak{p})$ and $d_{\mathfrak{p}'} = a_{\mathfrak{p}'}(E)^2 - 4N(\mathfrak{p}')$ 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). In the ordinary case, the endomorphism algebra is an imaginary quadratic field K , which is also invariant under isogeny (since the endomorphism rings of all isogenous curves are orders in K) and under base-change (since for ordinary curves all endomorphisms are already defined over the base field).

Take a finite extension L/K that 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 $\text{Gal}(L/\mathbb{Q})$ 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 $|a_{\mathfrak{p}}(E)| \leq 2\sqrt{N(\mathfrak{p})}$ 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). \square

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 is Galois invariant. We replace this with a condition that 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*

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

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 $\text{ord}_{\mathfrak{p}}(j(E)) < 0$, 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 $g \in \text{Gal}(L/\mathbb{Q})$ 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 $\text{ord}_{\mathfrak{q}'}(j(E)) < 0$ and hence also $\text{ord}_{\mathfrak{p}'}(j(E)) < 0$. \square

5.4. Sufficient conditions. Here we show how to prove that a non-CM elliptic curve E/K is a \mathbb{Q} -curve, using possibly incomplete knowledge of the finite set \mathcal{J} of j -invariants isogenous to $j(E)$ over K . It is not necessary 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 is more easily done using the methods given above.

Note that since E does not have CM, the j -invariants of the curves in the K -isogeny class of E are distinct; this follows from Lemma A.1.

Using the method of Section 5.2, we compute a subset $\mathcal{J}_0 \subseteq \mathcal{J}$, which may be a proper subset. If any elements of \mathcal{J}_0 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).

Otherwise, first suppose that we know that $\mathcal{J}_0 = \mathcal{J}$. Then we are able to apply Theorem 2.6, testing the condition that E is a \mathbb{Q} -curve if and only if \mathcal{J} includes a complete set of Galois conjugates. To this end, we compute the degree and minimal polynomial of each $j \in \mathcal{J}$, and see whether any of these polynomials occurs with multiplicity equal to its degree. 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.

On the other hand, suppose that we do not know whether $\mathcal{J}_0 = \mathcal{J}$, having used a non-rigorous bound in determining the reducible primes by the method of Section 5.2. We may still test whether \mathcal{J}_0 contains a

complete conjugacy class, and if this is the case then E is certainly a \mathbb{Q} -curve. However, if in this case we do not see a complete conjugacy class in \mathcal{J}_0 , then we cannot conclude that E is not a \mathbb{Q} -curve, since \mathcal{J}_0 may be a proper subset of \mathcal{J} . If this occurs, then we can apply more of the necessary tests of Section 5.3 to try to prove that E is not a \mathbb{Q} -curve, or compute a rigorous bound on the reducible primes in order to establish that we do in fact have $\mathcal{J}_0 = \mathcal{J}$.

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 $\text{cond}(E)$ 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 $N = N(\text{cond}(E))$.
- (4) For each prime $p \mid N$:
 - (a) If $\{\text{ord}_p(j(E)) : p \mid p\}$ contains both negative and non-negative integers then return False.
- (5) For each prime $p \nmid N$ with $p \leq B_1$:
 - (a) If $\{E_p : p \mid p\}$ are all ordinary:
 - (i) If $\{a_p(E)^2 - 4N(p) : p \mid p\}$ do not all have the same squarefree part then return False.
 - (b) Else if $\{E_p : p \mid p\}$ 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 $B_2 \geq B'_2$ 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 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.

Our SageMath code implementing this algorithm is available at [14]. The function `is_Q_curve()` takes an elliptic curve over an arbitrary number field as input, and optionally returns, as well as a True/False value, a “certificate” enabling a simple verification of the correctness of the output. For \mathbb{Q} -curves E , the certificate consists of either a CM discriminant if E has CM, or otherwise a quadruple (r, ρ, N, H) where r , ρ , and N are the quantities defined above, and $H \in \mathbb{Z}[X]$ is an irreducible monic polynomial in $\mathbb{Z}[X]$ of degree 2^ρ whose roots are all j -invariants of elliptic curves isogenous to E over its field of definition.

APPENDIX A. Q-CURVES AND 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 [15]); 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 that are not in [15].

We take \mathbb{Q} to be our base field, and denote by $\overline{\mathbb{Q}}$ its algebraic closure, the field of algebraic numbers. Set $G = G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. 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 $\text{Gal}(M/K)$. Some minor changes would be needed in case $\text{char}(K) \neq 0$.

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 $\phi: E_1 \rightarrow E_2$ 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 *realization* 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 $\text{End}(E_1) \otimes \mathbb{Q} \cong \text{End}(E_2) \otimes \mathbb{Q}$ for isogenous curves E_1, E_2 , though in general $\text{End}(E_1)$ and $\text{End}(E_2)$ 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 $\phi: E_1 \rightarrow E_2$ 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 $\phi: E_1 \rightarrow E_2$, 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 $\phi_0: E_1 \rightarrow E_2$ 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 $E_1 \rightarrow E_1$). Then $\phi_0 = \phi \circ [m]$ for some cyclic isogeny $\phi: E_1 \rightarrow E_2$.

Let $d = \deg(\phi)$, and suppose that $\psi: E_1 \rightarrow E_2$ is another cyclic isogeny, of degree d' . Then $\hat{\psi} \circ \phi$ is an endomorphism of E_1 of degree dd' . Since $\text{End}(E_1) \cong \mathbb{Z}$ 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. \square

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 and not CM. 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. \square

Corollary A.3. *Let $j_1, j_2, j_3 \in \overline{\mathbb{Q}}$ be isogenous, not CM, 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. \square

The next results concern the minimal field of definition of an isogeny realizing an isogeny relation. These are certainly well-known: see, for example, Lemma 3.1 in [26].

Lemma A.4. *Let E_1, E_2 be non-CM 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 that is isogenous to E_1 over K itself.*

Proof. Let $\phi: E_1 \rightarrow E_2$ be an isogeny over $\overline{\mathbb{Q}}$. For each $g \in G_K$, ϕ^g is another isogeny $E_1 \rightarrow E_2$ of the same degree as ϕ , hence, by Lemma A.1, we have $\phi^g = \alpha(g) \circ \phi$ with $\alpha(g) = \pm 1$. The map $g \mapsto \alpha(g)$ is a homomorphism, hence there exists $d \in K^*$ such that $\alpha(g) = g(\sqrt{d})/\sqrt{d}$. Then the quadratic twist of E_2 by d is isogenous to E_1 over K . \square

Corollary A.5. *Let $j_1, j_2 \in \overline{\mathbb{Q}}$ be isogenous and not CM. Then there exists an isogeny $\phi: E_1 \rightarrow E_2$ 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 $E_1 \rightarrow E_2$ defined over K . \square

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 $E_1 \rightarrow E_2$ gives a cyclic isogeny $g(E_1) \rightarrow g(E_2)$ of the same degree. \square

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

A.1.3. Factorization of isogenies and Atkin–Lehner involutions. Every cyclic isogeny can be factored into a composition of isogenies of prime 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 $\phi: E_1 \rightarrow E_2$ 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 $\phi_1: E_1 \rightarrow E$ and $\phi_2: E \rightarrow E_2$ of degrees 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 $\alpha \in \text{Aut}(E)$. In particular, if the curves do not have CM then ϕ_1 and ϕ_2 are uniquely determined up to simultaneous negation.

Proof. Since $\ker(\phi)$ is a cyclic subgroup of $E_1(\overline{\mathbb{Q}})$ of order d , it has a unique subgroup of order d_1 ; this determines a cyclic d_1 -isogeny $\phi_1: E_1 \rightarrow E$, 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 $\phi_2: E \rightarrow E_2$ as required. \square

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 and not CM, 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 $\phi: E_1 \rightarrow E_2$ 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 $j = j(E) \in K$. \square

Again let $\phi: E_1 \rightarrow E_2$ 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:

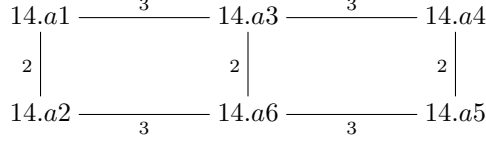
$$\begin{array}{ccc} E_1 & \xrightarrow{d_1} & E_3 \\ d_2 \downarrow & \swarrow & \downarrow d_2 \\ E_4 & \xrightarrow{d_1} & E_2 \end{array}$$

Here one diagonal is the original isogeny $E_1 \rightarrow E_2$, while the other diagonal gives a cyclic isogeny $E_3 \rightarrow E_4$ 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 $\phi: E_2 \rightarrow E_1$.

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

For example, the isogeny class of elliptic curves over \mathbb{Q} with LMFDB label 14.a consists of six curves labelled 14.a1-14.a6, linked by isogenies of degrees dividing 18.



There is an 18-isogeny from 14.a1 to 14.a5; applying W_9 gives the 18-isogeny from 14.a4 to 14.a2, while applying W_2 gives the dual 18-isogeny from 14.a2 to 14.a4. Thus the Atkin–Lehner orbit consists of four of the six curves in the class. The other two curves, 14.a3 and 14.a6, are 3-isogenous to these (and 2-isogenous to each other) and may be obtained via the construction in Proposition A.7. If we start with the 6-isogeny from 14.a1 to 14.a6, then applying W_2 takes it to the 6-isogeny from 14.a2 to 14.a3.

A.1.4. The isogeny graph. We may turn $\overline{\mathbb{Q}}$ into a graph by introducing edges between isogenous pairs (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 and a non-CM $j \in \overline{\mathbb{Q}}$. 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 [15], before turning to the quotient construction that 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 $[j] \rightarrow [j]_\ell$ 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 that 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 $j \in \overline{\mathbb{Q}}$ be non-CM.*

- (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 $1 \leq i \leq r$ be the primes for which $\pi_\ell(j_\ell) \neq \pi_\ell(j)$. (If there are none, then $j' = j$ meets the conditions.) To ease notation set $j_i = j_{\ell_i}$ for $1 \leq i \leq r$. For each i , factor the isogeny $j \rightarrow j_i$ as $j \rightarrow j'_i \rightarrow j_i$ 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 $\phi_i: E \rightarrow E_i$ a cyclic isogeny degree $\ell_i^{e_i}$. Define $\phi: E \rightarrow E'$ 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 $1 \leq i \leq r$, while $\pi_{\ell}(j') = \pi_{\ell}(j)$ for $\ell \neq \ell_1, \dots, \ell_r$ since these primes do not divide $\deg(j, j')$.

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

A.2. Q-curves and Q-numbers. A Q-curve is an elliptic curve E defined over $\overline{\mathbb{Q}}$ such that E is isogenous (over \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 Q-number if any elliptic curve $E/\overline{\mathbb{Q}}$ with $j(E) = j$ is a Q-curve.

As is well-known*, all elliptic curves with CM are Q-curves, so all CM j -invariants are Q-numbers. We will be less interested in these, and will restrict ourselves to non-CM Q-numbers; that is, Q-numbers that 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 Q-number is that $G(j) \subseteq [j]$. In fact, if any element of an isogeny class is a 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 Q-number. Then every $j' \sim j$ is a Q-number.*

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

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

For example, $j = -43136\sqrt{2} + 60992$ is a strict Q-number, being the j -invariant of the elliptic curve with LMFDB label 2.2.8.1-4096.1-a1 which is 2-isogenous to its Galois conjugate 2.2.8.1-4096.1-a2. (It will follow from the results of this Appendix that there can be no rational number isogenous to this j .) By contrast, $j = -36872164\sqrt{2} + 52151080$ is a non-strict Q-number: it is the j -invariant of 2.2.8.1-128.1-a2, but its isogeny class consists of four curves including 2.2.8.1-128.1-a1 which has $j = 128$.

Let $j \in \overline{\mathbb{Q}}$ be a Q-number. We define[†] the *isogeny degree* of j to be the least common multiple of the degrees $\deg(j, g(j))$ for $g \in G$. This is clearly the same for Galois conjugate Q-numbers, so we may also refer to the isogeny degree of a conjugacy class $G(j)$ of Q-numbers.

Definition 3. For each Q-class \mathcal{Q} , define

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

by

$$\delta_{\mathcal{Q}}(g) = \deg(j, g(j)) \pmod{(\mathbb{Q}^*)^2},$$

where $j \in \mathcal{Q}$ is arbitrary.

Lemma A.11. *For each Q-class \mathcal{Q} , $\delta_{\mathcal{Q}}$ is a well-defined group homomorphism with finite image.*

Proof. We first show that $\delta_{\mathcal{Q}}$ is well-defined, not depending on the choice of $j \in \mathcal{Q}$. 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 $\deg(j_1, g(j_1)) \equiv \deg(j_2, g(j_2)) \pmod{(\mathbb{Q}^*)^2}$.

Next, for $g, h \in G$ we have

$$\deg(j, gh(j)) \equiv \deg(j, g(j)) \deg(g(j), gh(j)) = \deg(j, g(j)) \deg(j, h(j)) \pmod{(\mathbb{Q}^*)^2}$$

by Corollary A.2 and Lemma A.6, so $\delta_{\mathcal{Q}}$ is a group homomorphism. Finiteness is immediate since the conjugacy class $G(j)$ is finite. \square

*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 ; these are all isogenous to \mathbb{C}/\mathcal{O} (see Chapter 2 of [41]).

[†]The isogeny 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 $\mathbb{Q}(j)/\mathbb{Q}$.

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.18 below). Note that it does not follow directly from Lemma A.11 that the square class of the isogeny 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 isogeny degree is square-free, this degree being the square-free part of the isogeny degree of every element of the class.

Definition 4. For a \mathbb{Q} -class \mathcal{Q} , let $L_{\mathcal{Q}}$ be the fixed field of $\ker(\delta_{\mathcal{Q}})$.

Since the image of $\delta_{\mathcal{Q}}$ is a finite subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, it is an elementary abelian 2-group, so $L_{\mathcal{Q}}$ is a finite polyquadratic extension of \mathbb{Q} . Its Galois group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\rho(\mathcal{Q})}$ for some $\rho(\mathcal{Q}) \geq 0$.

Looking only at the ℓ -primary part of the isogeny degree, and its exponent modulo 2, we obtain a character $\delta_{\ell}: G \rightarrow \{\pm 1\}$ that 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 $\ell_1, \dots, \ell_r(\mathcal{Q})$ be these primes. For each ℓ_i , and for every $j \in \mathcal{Q}$, exactly half the isogeny degrees $\deg(j, g(j))$ have even ℓ_i -valuation and half odd; while for other primes ℓ , these valuations are all even.

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 isogeny degree of every $j \in \mathcal{Q}$, since half of the isogeny 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 isogeny degree of every $j \in \mathcal{Q}$, by showing that the isogeny 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.18.

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 isogeny 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.13. *Let \mathcal{Q} be a \mathbb{Q} -class. Then for all central classes $C \subset \mathcal{Q}$,*

- (1) $C \subseteq \cap_{j \in \mathcal{Q}} \mathbb{Q}(j)$;
- (2) $\mathbb{Q}(C) = L_{\mathcal{Q}}$; in particular, $\mathbb{Q}(C)$ depends only on \mathcal{Q} ;
- (3) the isogeny degree of C is $N(\mathcal{Q})$, and 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 $\delta_{\mathcal{Q}}$ (see Definition 3 and Lemma A.11). 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 isogeny degree follows from Lemma A.11, for if j and j' are both central, then the degrees $\deg(j, g(j))$ and $\deg(j', g(j'))$ are square-free numbers that are equivalent modulo squares, and hence equal.

Let N be the isogeny 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 $\ell \mid N$, so $N = N(\mathcal{Q})$, independent of the choice of C . \square

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 Theorem A.13 and 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 $L_{\mathbb{Q}}$ 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 $L_{\mathbb{Q}}/\mathbb{Q}$ -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.

For example, let $j = (-30862080\sqrt{13} - 111275008)\sqrt{2} - 43645440\sqrt{13} - 157366464$, which is the j -invariant of the \mathbb{Q} -curve E with LMFDB label 4.4.10816.1-1.1-a1. Its isogeny class 4.4.10816.1-1.1-a (over the bi-quadratic field $K = \mathbb{Q}(\sqrt{2}, \sqrt{13})$) consists of the four Galois conjugates of E , linked by isogenies of all degrees dividing the level, which is 15. Here we have $\rho = r = 2$ and $L_{\mathbb{Q}} = K$.

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 [15], except that we use the quotient trees \mathcal{Q}_{ℓ} 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}_{ℓ} 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 isogeny degree of j . The image of $G(j)$ under π_{ℓ} is a finite subset of \mathcal{Q}_{ℓ} , which is a singleton unless ℓ divides N_0 . We define $T_{\ell}(j)$ to be the finite subtree of \mathcal{Q}_{ℓ} spanned by the conjugate vertices $\pi_{\ell}(g(j)) \in \mathcal{Q}_{\ell}$ for $g \in G$. Denote by $n(\ell, j)$ the diameter of $T_{\ell}(j)$; by definition of isogeny 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 valency 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 [16]), that they have a unique *centre*, that 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 defines 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 its diameter $n(\ell, j)$ is even or odd (respectively), and this centre is fixed by the action of G .

Proposition A.14. *The following are equivalent:*

- (1) $\ell \nmid N(\mathcal{Q})$;
- (2) $n(\ell, j)$ 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}_{ℓ} ;

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

(3) \Rightarrow (2): obvious.

(2) \Rightarrow (3), (4): When $n(\ell, j) = 2m$ is even, $T_{\ell}(j)$ has a central point $\pi_{\ell}(j_0)$, 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 $n(\ell, j) = 2m + 1$ 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 $g_0 \in G$ that 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}_{ℓ} , 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}_{ℓ} that are closer to $\pi_{\ell}(j_1)$ than to $\pi_{\ell}(j_2)$ with its complement. \square

Corollary A.15. *With the same notation, when $n(\ell, j) = 2m + 1$ 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 $2m + 1$. \square

Corollary A.16. *For all $j \in \mathcal{Q}$, the square-free part of the isogeny degree of j is equal to the level $N(\mathcal{Q})$.*

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

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}_ℓ , or equivalently the primes ℓ such that for all $j \in \mathcal{Q}$ there exists $g \in G$ such that $\text{ord}_\ell \deg(j, g(j))$ is odd.

Theorem A.17. *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 isogeny degree.

Proposition A.18. *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 $j_0 \in \mathbb{Q}$. \square

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.17. Choose some element j in the \mathbb{Q} -class \mathcal{Q} . Let ℓ_1, \dots, ℓ_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 $\pi_{\ell_i}(j_i^\pm)$. Now, for each choice of signs $s = (s_1, \dots, s_r) \in \{\pm\}^r$, 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.18) 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, $\deg(j_s, g(j_s)) = \prod_i \ell_i^{\varepsilon_i}$ 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 $G \rightarrow (\mathbb{Z}/2\mathbb{Z})^r$, namely $g \mapsto (\varepsilon_1, \dots, \varepsilon_r)$. The image has order $2^{\rho(\mathcal{Q})}$, and C is the closure of $G(j_s)$ under Atkin–Lehner involutions. \square

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 a \mathbb{Q} -curve E to a central \mathbb{Q} -curve in terms of the isogeny degree of E (that is, the least common multiple of the degrees of the isogenies between E and its Galois conjugates).

Corollary A.19. *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 $\phi: E \rightarrow E_0$, where both E_0 and ϕ are also defined over K .*
- (2) *Let N be the isogeny degree of E , and write $N = N_0 M^2$ with N_0 square-free. Then the smallest degree of an isogeny $\phi: E \rightarrow E_0$ (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.13, 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 $\phi: E \rightarrow E_0$ is also defined over $\mathbb{Q}(j, j_0) \subseteq K$ as in Lemma A.4.

(2) Write the isogeny degree of j as $N_0 M^2$ as in the statement. We use the notation of the proof of Theorem A.17, so $N_0 = \ell_1 \dots \ell_r$. 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. \square

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] N. Billerey, *Critères d’irréductibilité pour les représentations des courbes elliptiques*, Int. J. Number Theory, **7**, (2011), 1001–1032. 5.2.1
- [4] Y. Bilu and P. Parent, *Serre’s uniformity problem in the split Cartan case*, Ann. Math. (2), **173** (2011), 569–584. 3
- [5] 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
- [6] 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
- [7] A. Bourdon and P. L. Clark, *Torsion points and isogenies on CM elliptic curves*, J. London Math. Soc. **102** (2020), 580–622. 3
- [8] 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
- [9] 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
- [10] J. Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp. **90**, 321–343 (2021). 1
- [11] R. Bröker, K. Lauter, and A. V. Sutherland, *Modular polynomials via isogeny volcanoes*, Mathematics of Computation **81**, no. 278 (2012), 1201–1231. 1, 5.2.2
- [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] J. E. Cremona, *SageMath code at <https://github.com/JohnCremona/ecnf-data/blob/master/sage/Qcurves.py>*. 1, 5.5
- [15] 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
- [16] C. Jordan, *Sur les assemblages des lignes*, J. Reine Angew. Math. **70** (1869), 185–190. A.3
- [17] E. González-Jiménez and F. Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comp. **323** (2020), 1457–1485. 1, 3, 4, 4
- [18] 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
- [19] E. González-Jiménez and J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Mat. RACSAM **108** (2014), 923–934. 4
- [20] T. Gužvić, *Torsion of elliptic curves with rational j -invariant defined over number fields of prime degree*, Proc. Am. Math. Soc. **149** (2021), 3261–3275. 4, 4.2
- [21] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields* Astérisque, **228** (1995), 81–98. 4
- [22] C. Khare and J.-P. Wintenberger, *Serre’s modularity conjecture (I)*, Invent. Math. **178** (2009), 485–504. 1
- [23] C. Khare and J.-P. Wintenberger, *Serre’s modularity conjecture (II)*, Invent. Math. **178** (2009), 505–586. 1
- [24] J. Klaise, *Orders in imaginary quadratic fields of small class number*, University of Warwick Undergraduate Masters thesis, unpublished (2012). 5.1
- [25] S. Le Fourn, *Surjectivity of Galois representations associated with quadratic \mathbb{Q} -curves*, Math. Ann. **365** (2016), 173–214. 1
- [26] S. Le Fourn and F. Najman, *Torsion of \mathbb{Q} -curves over quadratic fields*, Math. Res. Letters **27** (2020), 209–225. A.1.2
- [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] SageMath reference manual for *Galois representations for elliptic curves over number fields*. (code by E. Larson and J. E. Cremona), https://doc.sagemath.org/html/en/reference/arithmetic_curves/sage/schemes/elliptic_curves/gal_reps_number_field.html 5.2.1
- [29] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, <http://www.lmfdb.org> 1
- [30] 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
- [31] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1978), 33–186. 1, 4
- [32] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162. 1, 3, 3
- [33] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996) 437–449. 1
- [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] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, GTM 151 (1994). *

- [42] A. V. Sutherland, *A local-global principle for rational isogenies of prime degree*, Journal de Théorie des nombres de Bordeaux **24** (2012), 475–485. 3
- [43] A. V. Sutherland, *Modular polynomial database*, <https://math.mit.edu/~drew/ClassicalModPolys.html>. 1, 5.2.2
- [44] M. Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907–938. 5.1
- [45] 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`