ISOGENIES OF NON-CM ELLIPTIC CURVES WITH RATIONAL j-INVARIANTS OVER NUMBER FIELDS

FILIP NAJMAN

ABSTRACT. We unconditionally determine $I_{\mathbb{Q}}(d)$, the set of possible prime degrees of cyclic K-isogneies of elliptic curves with $\mathbb{Q}$-rational j-invariants and without complex multiplication over number fields K of degree $\leq d$, for $d \leq 7$, and give an upper bound for $I_{\mathbb{Q}}(d)$ for $d > 7$. Assuming Serre's uniformity conjecture, we determine $I_{\mathbb{Q}}(d)$ exactly for all positive integers d.

1. Introduction

Let E/K be an elliptic curve over a number field. If there exists a K-rational cyclic isogeny $\phi : E \to E'$ of degree n, this implies that $\ker \phi$ is a $\mathrm{Gal}(\overline{K}/K)$-invariant cyclic group of order n and we will say that E/K has an *n-isogeny*.

When talking about possible isogeny degrees of elliptic curves over number fields, it makes sense to restrict to only elliptic curves without complex multiplication (CM). This is because an elliptic curve E with complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field L will have p-isogenies for infinitely many primes p over any number field containing L. We will restrict to elliptic curves without CM in the whole paper, without further mention.

Understanding the possible torsion groups and possible degrees of a cyclic isogeny is one of the basic problems in the study of elliptic curves over number fields. After the possible torsion groups [12] and prime degrees of isogenies [13] of elliptic curves over $\mathbb{Q}$ were determined by Mazur, Kenku [6, 7, 8, 9] soon completed the classification of possible degrees (not just of prime order) of isogenies of elliptic curves over $\mathbb{Q}$.

From then, there has been much progress in understanding the possible torsion groups of elliptic curves over number fields: primes that can divide the order of the torsion of an elliptic curves over number fields of degree d were determined by Kamienny [5] for $d = 2$, Parent [15, 16] for $d = 3$ and bounds for the size of such primes for general d were determined by Merel [14].

Unfortunately, there has been much less progress in understanding possible degrees of isogenies. A full list of primes p such that p divides n for some n-isogeny of an elliptic curve over a number field of degree $d > 1$ is not known, even when one restricts to elliptic curves defined over a single number field $K \neq \mathbb{Q}$. We should mention that, for a fixed number field K, Larson and Vaintrob [10] recently proved that such a list of possible degrees is finite, assuming the Generalized Riemann Hypothesis.

In this paper, we give a list of primes $I_{\mathbb{Q}}(d)$ that divide n for some n-isogeny of an elliptic curve with $\mathbb{Q}$-rational j-invariant without CM over a number field of degree $\leq d$. This can be considered to be an analogue of a similar result of Lozano-Robledo [11] for the torsion, and in fact we will use similar methods as in that paper.

2010 *Mathematics Subject Classification.* 11G05.

We should note that when studying p-isogenies one can look at the set of elliptic curves with rational j-invariant instead of the set of elliptic curves with coefficients from $\mathbb{Q}$. The latter set has density 0 in the former over any number field $\neq \mathbb{Q}$ and using any sensible ordering. We can study just the j-invariants because a p-isogeny is a quadratic–twist-invariant property, while having p-torsion is not (except when $p = 2$). In other words the set of elliptic curves with a p-isogeny is a coarse moduli space, while the set of elliptic curves with p-torsion (for $p > 3$) is a fine moduli space.

By the aforementioned result of Mazur [13] we know that

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

Note that by definition $I_{\mathbb{Q}}(1) \subseteq I_{\mathbb{Q}}(d)$ for all $d \geq 1$.

We prove the following result.

Theorem 1.1. *$I_{\mathbb{Q}}(d) = I_{\mathbb{Q}}(1)$ for all $d \leq 7$.*

We also give an unconditional upper bound on $I_{\mathbb{Q}}(d)$ for all positive integers d in Theorem 3.4.

In Section 4, we describe $I_{\mathbb{Q}}(d)$ for all positive integers d, under the assumption that Serre's uniformity conjecture (see Conjecture 2.3) is true.

2. Preliminaries: Galois representations

Studying both the torsion and isogenies of elliptic curves can be viewed as a more general problem of studying their Galois representations. Let $E[n] = \{P \in E(\overline{\mathbb{Q}}) | nP = 0\}$ denote the n-th division group of E over $\overline{\mathbb{Q}}$ and let $\mathbb{Q}(E[n])$, the field obtained by adjoining the coordinates of all points in $E[n]$, be the n-th division field of E. The Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ and gives rise to a homomorphism

$$\rho_{E,n} : G_{\mathbb{Q}} \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

called a *mod n Galois representation*. The composition of the determinant map and ρ_n is the *cyclotomic character* χ_n. For a number field K, $E(K)[n]$ denotes the set of K-rational points in $E[n]$.

Let p be a prime and ϵ a fixed quadratic non-residue of $\mathbb{F}_p$. Following [11], we define

$$\mathcal{C}_{ns} = \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p, (a, b) \not\equiv (0, 0) \pmod{p} \right\}$$

to denote the non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$. Futhermore, we define

$$M(a, b) := \left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p, (a, b) \not\equiv (0, 0) \pmod{p} \right\},$$

$$N(c, d) := \left\{ \begin{pmatrix} c & \epsilon d \\ -d & -c \end{pmatrix} : c, d \in \mathbb{F}_p, (c, d) \not\equiv (0, 0) \pmod{p} \right\}$$

and

$$\mathcal{C}_{ns}^{+} = \{M(a, b), N(c, d), a, b, c, d \in \mathbb{F}_p, (a, b), (c, d) \not\equiv (0, 0) \pmod{p}\}$$

be the normalizer of the non-Split Cartan subgroup.

Let $E/\mathbb{Q}$ be an elliptic curve and $p \geq 5$ a prime, and let K be an extension of $\mathbb{Q}_p$ of the least possible degree such that E has good or multiplicative reduction over K. Let e be the ramification index of K over $\mathbb{Q}_p$; it is well known that $e \leq 6$ [17].

Theorem 2.1 ([1, 2, 13, 17])**.** *Let $p \notin I_{\mathbb{Q}}(1)$ be a prime and e be the ramification index of $K/\mathbb{Q}_p$, as defined above. Then the image G of $\rho_{E,p}(G_{\mathbb{Q}})$ is either*

1. *Contained in the normalizer of a non-split Cartan subgroup: then G contains the e-the power of a non-split Cartan subgroup, or*
2. *Surjective, i.e. $G = \mathrm{GL}_2(\mathbb{F}_p)$.*

In fact, Zywina [19] recently proved an even more precise result of what the image of $\rho_{E,p}$ looks like if $p \notin I_{\mathbb{Q}}(1)$.

Proposition 2.2 ([19], Proposition 1.13.)**.** *Suppose $E/\mathbb{Q}$, $p \notin I_{\mathbb{Q}}(1)$ and $\rho_{E,p}$ is not surjective. Then*

1. *If $p \equiv 1 \pmod 3$, then $\rho_{E,p}(G_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ to $\mathcal{C}_{ns}^+$.*
2. *If $p \equiv 2 \pmod 3$, then $\rho_{E,p}(G_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ to either $\mathcal{C}_{ns}^+$ or $(\mathcal{C}_{ns}^+)^3$.*

Serre's Open image theorem [17] implies that for an elliptic curve $E/\mathbb{Q}$ without CM, for all but finitely many primes p, $\rho_{E,p}$ is surjective.

We should note that there does not exist one known elliptic curve $E/\mathbb{Q}$ such that for a prime $p \notin I_{\mathbb{Q}}(1)$, the representation $\rho_{E,p}$ is not surjective. Sutherland [18] has recently checked this for all elliptic curves [3] (over 2 million of them) with conductor up to 350000 and all elliptic curves in the Stein-Watkins database (more than 140 million curves).

These observations gives rise to Serre's Uniformity conjecture states that there should exist a bound B, not depending on the elliptic curve E, such that $\rho_{E,p}$ is surjective for all $p > B$ and for all elliptic curves over $\mathbb{Q}$. Here we state the following version of this conjecture.

Conjecture 2.3 (Serre's uniformity conjecture, see [19], Conjecture 1.12.)**.** *For $E/\mathbb{Q}$, $p \notin I_{\mathbb{Q}}(1)$, the representation $\rho_{E,p}$ is surjective.*

3. Degree of the field of definition of a p-isogeny

To prove Theorem 1.1, we will need to find the minimal degree of definition of a p-isogeny of an elliptic curve with $\mathbb{Q}$-rational j-invariant. By Theorem 2.1 and Proposition 2.2, we need to consider 2 cases: either $\rho_{E,p}$ is surjective or its image is surjective or is contained in a normalizer of non-split Cartan subgroup.

Let $P \in E[p]$ be a point of degree p and $C = \langle P \rangle$ be the subgroup generated by P. For a number field K, 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 p-isogeny ϕ with kernel C is defined over K, or in other words, the smallest number field such that $\mathrm{Gal}(\overline{K(C)}/K(C))$ acts on C.

3.1. Full image.

Proposition 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime such that $\rho_{E,p}$ is surjective, and C of $E[p]$ of order p. Then $[\mathbb{Q}(C) : \mathbb{Q}] = p + 1$.*

Proof. Let $\{P, R\}$ be the basis of $E[P]$. The field of definition of $\mathbb{Q}(C)$ is then the fixed field of the subgroup

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in \mathbb{F}_p^{\times}, b \in \mathbb{F}_p \right\}.$$

We have $|\mathrm{GL}_2(\mathbb{F}_p)| = p(p-1)^2(p+1)$ and $|H| = p(p-1)^2$, so we conclude that

$$[\mathbb{Q}(\langle P \rangle) : \mathbb{Q}] = |\mathrm{GL}_2(\mathbb{F}_p)/H| = p + 1.$$

□

3.2. **Normalizer of non-split Cartan.** A result that we will need is the following easy lemma.

Lemma 3.2. *Let E/K be an elliptic curve over a number field and $P \in E[p]$. Let $C = \langle P \rangle$. Then $[K(P) : K(C)]$ divides $p - 1$.*

Proof. By definition E has a p-isogeny over $K(C)$. Then the same proof as [4, Lemma 7], taking $K(P)$ instead of $\mathbb{Q}$ as the base field (which does not make a difference in the proof) proves the claim. □

Now we can prove our result.

Proposition 3.3. *Let $E/\mathbb{Q}$ be an elliptic curve and p a prime such that the image of $\rho_{E,p}$ is contained in the normalizer of the non-split Cartan subgroup and let $\langle P \rangle = C \subseteq E[p]$ a cyclic subgroup of order p. Then*

1. *If $p \equiv 2 \pmod 3$, then $[\mathbb{Q}(C) : \mathbb{Q}] \geq p + 1$.*
2. *If $p \equiv 2 \pmod 3$, then $[\mathbb{Q}(C) : \mathbb{Q}] \geq (p + 1)/3$.*
3. *If E does not have additive reduction at p, then $[\mathbb{Q}(C) : \mathbb{Q}] \geq p + 1$.*

Proof. For an elliptic curve $E/\mathbb{Q}$ such that the image of $\rho_{E,p}$ is contained in the normalizer of the non-split Cartan subgroup, by the proof of [11, Theorem 7.3] the field of smallest degree $\mathbb{Q}(P)$ over which a point P of order p is defined is $\geq \frac{p^2-1}{a}$, where a is the smallest integer such that $\rho_{E,p}(G_{\mathbb{Q}})$ contains an a-th power of $\mathcal{C}_{ns}$[1].

On the other hand, by Lemma 3.2, we have $[\mathbb{Q}(P) : \mathbb{Q}(C)] \leq p - 1$. Together this implies that for any $P \in E[p]$,

$$[\mathbb{Q}(C) : \mathbb{Q}] \geq \frac{\frac{p^2-1}{a}}{p-1} \geq \frac{p+1}{a}.$$

By Proposition 2.2,

$$a = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 3, \\ 1 \text{ or } 3 & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

from which (1) and (2) follow.

Part (3) follows from part (1) of Theorem 2.1, since by assumption we have $e = 1$ and hence $\rho_{E,p}(G_{\mathbb{Q}})$ contains $\mathcal{C}_{ns}$. □

3.3. **Proof of Theorem 1.1.** Let $p \notin I_{\mathbb{Q}}(1)$ and $d(p)$ be the minimal field of definition of a p-isogeny of an elliptic curve with rational j-invariant.

By Propositions 3.1 and 3.3, we have that $d(p) \geq p + 1$ if $p \equiv 1 \pmod 3$ and $d(p) \geq (p + 1)/3$ if $p \equiv 2 \pmod 3$. Since for $p \notin I_{\mathbb{Q}}(1)$, we have $p \geq 19$ for $p \equiv 1 \pmod 3$ and $p \geq 23$ for $p \equiv 2 \pmod 3$, it follows that $d(p) \geq 8$ for all $p \notin I_{\mathbb{Q}}(1)$, proving the Theorem. □

Note that we have in the proof above in fact proved an unconditional upper bound for $I_{\mathbb{Q}}(d)$, for all integers d.

[1] In the statment of [11, Theorem 7.3], it says that $[\mathbb{Q}(P) : \mathbb{Q}] \geq \frac{p-1}{e}$, where e is as defined in Section 2, since this guarantees that $\rho_{E,p}(G_{\mathbb{Q}})$ contains C_{ns}^e. But from the proof we see that it is true that $[\mathbb{Q}(P) : \mathbb{Q}] \geq \frac{p^2-1}{a}$, where a (which may be smaller than e) is the smallest integer such that $\rho_{E,p}(G_{\mathbb{Q}})$ contains C_{ns}^a.

Theorem 3.4. *For all positive integers d,*

$$I_{\mathbb{Q}}(d) \subseteq I_{\mathbb{Q}}(1) \cup \{p \text{ prime} : p \leq d-1,\ p \equiv 1 \pmod 3\} \cup \{p \text{ prime} : p \leq 3d-1,\ p \equiv 2 \pmod 3\}.$$

4. Results assuming Serre's uniformity conjecture

If we assume Conjecture 2.3, we can prove stronger results.

Theorem 4.1. *Suppose Conjecture 2.3 is true. Then for all positiver integers d,*

$$I_{\mathbb{Q}}(d) = I_{\mathbb{Q}}(1) \cup \{p \text{ prime} : p \leq d-1\}.$$

In particular $I_{\mathbb{Q}}(d) = I_{\mathbb{Q}}(1)$ for $d \leq 19$.

Proof. Let $p \notin I_{\mathbb{Q}}(1)$ and $d(p)$ be the minimal field of definition of a p-isogeny of an elliptic curve with rational j-invariant. Then by assumption $\rho_{E,p}$ is surjective and by Proposition 3.1, $d(p) = p+1$. □

References

[1] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Ann. Math. (2), **173** (2011), 569–584. 2.1

[2] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on $X_0 + (p^r)(\mathbb{Q})$,* Ann. Inst. Fourier (Grenoble) **63** (2013), 957–984. 2.1

[3] J. Cremona, *Elliptic curve data*, online database `https://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html` 2

[4] E. Gonzalez-Jimenez, F. Najman, J. M. Tornero, *Torsion of rational elliptic curves over cubic fields,* Rocky Mountain J. Math, to appear. 3.2

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

[6] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. 1

[7] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. 1

[8] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244. 1

[9] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) 23 (1981), 415–427. 1

[10] E. Larson and D. Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*, J. Inst. Math. Jussieu **13** (2014), 517–559. 1

[11] Á. Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), 279–305. 1, 2, 3.2, 1

[12] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186. 1

[13] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), pp. 129–162. 1, 2.1

[14] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449. 1

[15] P. Parent. *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–16. 1

[16] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres de Bordeaux **15** (2003), 831–838. 1

[17] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331. 2, 2.1, 2

[18] A. Sutherland, *Computing images of Galois representations attached to elliptic curves*, preprint. `http://arxiv.org/abs/1504.07618` 2

[19] 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` 2, 2.2, 2.3

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: fnajman@math.hr

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
E-mail address: fnajman@mit.edu