ISOLATED POINTS ON $X_1(\ell^n)$ WITH RATIONAL j-INVARIANT

ÖZLEM EJDER

Abstract. Let ℓ be a prime and let $n \geq 1$. In this note we show that if there is a non-cuspidal, non-CM isolated point x with a rational j-invariant on the modular curve $X_1(\ell^n)$, then $\ell = 37$ and the j-invariant of x is either $7 \cdot 11^3$ or $-7.137^3 \cdot 2083^3$. The reverse implication holds for the first j-invariant but it is currently unknown whether or not it holds for the second.

1. Introduction

Let C be a curve over a field k. Frey [Fre94] observed that Faltings's theorem implies that if C has infinitely many degree d points, then either there is a function $C \to \mathbb{P}^1$ of degree d or that the image of the map $\phi_d : C^{(d)} \to \mathrm{Jac}(C)$ is a union of translates of a positive rank subabelian variety. We call a closed point on a curve C isolated if it is neither a member of a family parametrized by $\mathbb{P}^1$ or by a positive rank subabelian variety of the Jacobian of C. See the next page for a more precise definition. Motivated by the classification of torsion subgroups of elliptic curves over various number fields, we study the isolated points on $X_1(n)$. In [BEL$^+$19, Corollary 1.7], it is proven that there are only finitely many rational j-invariants giving rise to isolated points assuming Serre's uniformity conjecture (originally a question of Serre [Ser72], formalized as a conjecture by Zywina [Zyw, Conj 1.12] and Sutherland [Sut16, Conj 1.1]).

Conjecture 1.1 (Uniformity conjecture)**.** *For all non-CM elliptic curves $E/\mathbb{Q}$, the mod-ℓ Galois representation of E is surjective for all $\ell > 37$.*

In this short note, we prove unconditionally that there are finitely many isolated rational j-invariants on $X_1(\ell^n)$ for any prime $\ell > 7$.

Theorem 1.2. *Let ℓ be a prime greater than 7 and let n be a positive integer. If $X_1(\ell^n)$ has a non-CM, non-cuspidal isolated point with a rational j-invariant, then $\ell = 37$ and the j-invariant is either $7 \cdot 11^3$ or $-7 \cdot 137^3 \cdot 2083^3$.*

Remark 1.3. The first j-invariant $7 \cdot 11^3$ gives rise to an isolated point on $X_1(37)$ by [BEL$^+$19, Proposition 8.4]. However, we currently do not know whether the second j-invariant $-7 \cdot 137^3 \cdot 2083^3$ gives rise to an isolated point on $X_1(37)$ or not. We also note that the case $\ell = 2$ was studied in [BEL$^+$19, Theorem 8.5] (for sporadic points) and it is an open problem to determine the isolated rational j-invariants on $X_1(\ell^n)$ for $\ell = 3, 5, 7$ and $n \geq 2$.

Another unconditional result related to this problem is given in [BGRW20] for isolated points of odd degree with rational j-invariant on $X_1(n)$. Also see [Smi20, Theorem 2.3] for a result on sporadic points on $X_1(\ell^n)$ corresponding to elliptic curves with supersingular reduction at ℓ.

2. Background and Notation

By curve we mean a projective nonsingular 1-dimensional scheme over a field. For a curve C over a number field k, we use $\mathrm{gon}_k(C)$ to denote the k-gonality of C, which is the minimum degree of a dominant morphism $C \to \mathbb{P}^1_k$. If x is a closed point of C, we denote the residue field of x by $\mathbf{k}(x)$ and define the degree of x to be the degree of the residue field $\mathbf{k}(x)$ over k.

If E is an elliptic curve defined over a number field k and $P \in E(k)$, then $k(P)$ denotes the field extension of k generated by the $x-$ and $y-$coordinates of P.

We use E to denote an elliptic curve, i.e., a curve of genus 1 with a specified rational point O. Throughout we will consider only elliptic curves defined over number fields. We say that an elliptic curve E over a field k has complex multiplication, or CM, if the geometric endomorphism ring is strictly larger than $\mathbb{Z}$.

2.1. **Galois Representations.** Let k be a number field. Throughout, we denote the absolute Galois group of k by G_k. We use ℓ to denote an odd prime number. Let E/k be an elliptic curve defined over the number field k. Fixing a basis for the ℓ-adic Tate module of E, we obtain the representation given by

$$\rho_{E,\ell^\infty} : G_k \to \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where $\mathbb{Z}_\ell$ denotes the ring of ℓ-adic integers. Similarly for any $n \geq 1$, we also have

$$\rho_{E,\ell^n} : G_k \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}),$$

which describes the action of G_k on the ℓ^n-torsion subgroup $E[\ell^n]$ of $E(\bar{k})$. We note that $\rho_{E,\ell^n} = \pi_n \circ \rho_{E,\ell^\infty}$ where π_n is the natural projection map $\mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

We denote the image of ρ_{E,ℓ^n} (resp., ρ_{E,ℓ^∞}) as G_{E,ℓ^n} (resp., G_{E,ℓ^∞}).

2.2. **Modular Curve $X_1(n)$.** For a positive integer n, let

$$\Gamma_1(n) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{n},\ a \equiv d \equiv 1 \pmod{n} \right\}.$$

The group $\Gamma_1(n)$ acts on the upper half plane $\mathbb{H}$ via linear fractional transformations, and the points of the Riemann surface $Y_1(n) := \mathbb{H}/\Gamma_1(n)$ correspond to equivalence classes of pairs $[(E, P)]$, where E is an elliptic curve over $\mathbb{C}$ and $P \in E$ is a point of order n. Here two pairs (E, P) and (E', P') are equivalent if there exists an isomorphism $\varphi\colon E \to E'$ such that $\varphi(P) = P'$. By adjoining a finite number of cusps to $Y_1(n)$, we obtain the smooth projective curve $X_1(n)$. In fact, we may view $X_1(n)$ as an algebraic curve defined over $\mathbb{Q}$.

Lemma 2.1. [BEL+19, Lemma 2.1] *Let E be a non-CM elliptic curve defined over the number field $k = \mathbb{Q}(j(E))$, let $P \in E$ be a point of order n, and let $x = [(E, P)] \in X_1(n)$. Then*

$$\deg(x) = c_x[k(P) : k],$$

where $c_x = 1/2$ if $2P \neq O$ and there exists $\sigma \in \mathrm{Gal}_k$ such that $\sigma(P) = -P$ and $c_x = 1$ otherwise.

Proposition 2.2. [BEL+19, Proposition 2.2] *For positive integers $n \geq m$ and a prime ℓ, there is a natural $\mathbb{Q}$-rational map $\pi\colon X_1(\ell^n) \to X_1(\ell^m)$ with*

$$\deg(\pi) = \ell^{2(n-m)}$$

2.3. **Isolated Points.** Let C/k be a curve with a point $P \in C(k)$. For $d \in \mathbb{N}$, let C^d denote the direct product of d copies of C. We denote the d-th symmetric product of C by $C^{(d)}$, i.e., the quotient of C^d by the symmetric group S_d. We have a natural map $\phi_d\colon C^{(d)} \to \mathrm{Jac}(C)$ given by $(P_1, \ldots, P_d) \mapsto [P_1 + \ldots P_d - dP]$. We say that a point x on C is isolated [BEL+19, Definition 4.1] if

- ($\mathbb{P}^1$-isolated) there is no $x' \in C^{(d)}$ such that $\phi_d(x) = \phi_d(x')$ and
- (AV-isolated) there is no positive rank subabelian variety A of $\mathrm{Jac}(C)(k)$ such that $\phi_d(x) + A \subset \mathrm{im}(\phi_d)$.

The first condition is due to the fact that if such a point exists, then there has to be a rational map $f\colon C \to \mathbb{P}^1$ of degree d such that x is in $f^{-1}(\mathbb{P}^1(k))$. If this is the case, we say x is a member of a family parametrized by $\mathbb{P}^1$. Similarly, if there is such an abelian variety, we say x is parametrized by a positive rank subabelian variety of $\mathrm{Jac}(C)$. We note here that if $\mathrm{Jac}(C)(\mathbb{Q})$ is of rank zero and the degree of a point x on C is less than the gonality, then x is isolated.

Lemma 2.3. *Let C/k be a curve of genus $g > 0$. Let x be a point on C of degree d. If x is an isolated point, then $d \leq g$.*

Proof. Assume that $d > g$. Let x be a point of degree d on C. Then $D = \sum_i x_i$, where x_i are Galois conjugates of x, is a degree d divisor. By the Riemann-Roch theorem, $\ell(D) \geq d - g + 1 \geq 2$ and hence there is a non-constant function $f : C \to \mathbb{P}^1$ defined over k whose poles are at most at x_i's. Since f is defined over k, if x_j is a pole of f, then x_i is a pole of f for all i. We deduce that f has degree d which implies that x is not $\mathbb{P}^1$-isolated, hence it is not isolated. □

Theorem 2.4. [BEL+19, Theorem 4.3] *Let $f : C \to D$ be a finite map of curves and let $x \in C$ be an isolated point. If $\deg(x) = \deg(f(x))\dot{\deg}(f)$, then $f(x)$ is an isolated point of D.*

Remark 2.5. Let $\pi : X_1(\ell^n) \to X_1(\ell^m)$ for integers $n > m$. Let $x := [(E, P)]$ be a point on $X_1(\ell^n)$. If $G_{E,\ell^n} = \pi^{-1}(G_{E,\ell^m})$, then the assumption of Theorem 2.4 holds by [BEL+19, Corollary 5.3]. This holds in particular when $\ell > 3$ and ρ_ℓ is surjective.

We call a point $j \in X_1(1) \simeq \mathbb{P}^1$ an isolated j-invariant if it is the image of an isolated point on $X_1(n)$, for some positive integer n.

2.4. **Some Subgroups of** $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$**.** The nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is the subgroup

$$C_{ns}(\ell) = \left\{ \begin{bmatrix} a & \epsilon b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z}/\ell\mathbb{Z}, (a,b) \not\equiv (0,0) \pmod{\ell} \right\}$$

where ϵ is a non-quadratic residue modulo ℓ. We denote the normalizer of $C_{ns}(\ell)$ by $C_{ns}^+(\ell)$ respectively. The group $C_{ns}(\ell)$ has order $\ell^2 - 1$ and $C_{ns}^+(\ell)$ has order $2(\ell^2 - 1)$.

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $\ell \geq 5$ be a prime. Let K be an extension of $\mathbb{Q}_\ell$, of the least possible degree such that E/K has good or multiplicative reduction. Let e be the ramification index of $K/\mathbb{Q}_\ell$. Let D denote the semi-Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ given by

$$D = \left\{ \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z}/\ell\mathbb{Z}^* \right\}.$$

Here e is $1, 2, 3, 4$ or 6. Let $f = \gcd(\ell - 1, e)$, then $f < 5$ or $f = 6$.

Theorem 2.6. [Ser72] *If E/K has potential good ordinary or multiplicative reduction at p, then $G_{E,\ell}$ contains a subgroup that is conjugate to D^f.*

Proof. See [LR13, Theorem 3.1]. □

Let $E/\mathbb{Q}$ be a non-CM elliptic curve. Then $G_{E,\ell}$ is either $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or it is contained in one of the maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$: the normalizer of Cartan subgroups, Borel subgroups and the exceptional subgroups. Mazur [Maz78] showed that if it is contained in a Borel subgroup, then ℓ is in $\{2, 3, 5, 7, 11, 17, 37\}$. Moreover, if ℓ is 17 or 37, then $j(E)$ is in

$$\{-17 \cdot 373^3/2^{17}, -17^2 \cdot 101^3/2, -7 \cdot 11^3, -7 \cdot 137^3 \cdot 2083^3\}.$$

See [Zyw]. In the case of the normalizer of a split Cartan subgroup, by [BP11] and [BPR13], we know that $\ell \leq 7$ or $\ell = 13$. Recent progress on finding rational points on curves [BDM+19] showed that ℓ cannot be 13. Similarly, Serre himself showed that if the group $G_{E,\ell}$ is contained in an exceptional subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, then ℓ must be less than or equal to 13. Hence if $\ell \geq 17$ and $\rho_{E,\ell}$ is not surjective, then it is either contained in the normalizer of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or the j-invariant is in the list $\{-17 \cdot 373^3/2^{17}, -17^2 \cdot 101^3/2, -7 \cdot 11^3, -7 \cdot 137^3 \cdot 2083^3\}$.

In the Borel case, we know that G_{E,ℓ^∞} is as large as possible given the group $G_{E,\ell}$ for $\ell \leq 7$. Although Greenberg proves a similar result also for $\ell = 5$, we only need to use the case $\ell > 5$ in this article.

Theorem 2.7. [Gre12], [Gre14] *Assume that $\ell > 5$. Assume that $E/\mathbb{Q}$ is a non-CM curve with an ℓ-isogeny. Then the image of ρ_{E,ℓ^∞} contains a Sylow pro-ℓ subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.*

3. Classifying isolated Points on Prime Power Level

Let E be an elliptic curve over $\mathbb{Q}$. Then [Lem19, Proposition 2.2] implies that if $\ell \geq 5$ and $G_{E,\ell}$ is contained in $C_{ns}^+(\ell)$, then E has potential good reduction at ℓ. We show that E, in fact, has potential good supersingular reduction at ℓ when $\ell > 7$.

Proposition 3.1. *Assume that $\ell > 7$ and $\ell \neq 13$. Let E be an elliptic curve defined over $\mathbb{Q}$. If $G_{E,\ell}$ is conjugate to a subgroup of $C_{ns}^+(\ell)$, then E has potential supersingular reduction at ℓ.*

Proof. Let $\ell > 7$. Fixing a basis for $E[\ell]$, we may assume that $G_{E,\ell}$ is contained in $C_{ns}^+(\ell)$. Assume for contradiction that E has potential good ordinary or multiplicative reduction at ℓ. By Theorem 2.6, $G_{E,\ell}$ contains a subgroup H that is conjugate to D^f, the f'th power of a semi-Cartan subgroup.

We first consider the composition of the inclusion map $H \hookrightarrow C_{ns}^+(\ell)$ and the quotient map $C_{ns}^+(\ell) \to C_{ns}^+(\ell)/C_{ns}(\ell)$. We observe that the kernel of this composition is $H \cap C_{ns}(\ell)$ and hence we have an injective map

$$H/H \cap C_{ns}(\ell) \hookrightarrow C_{ns}^+(\ell)/C_{ns}(\ell).$$

Since the order of $C_{ns}^+(\ell)/C_{ns}(\ell)$ is two, the index of the subgroup $H \cap C_{ns}(\ell)$ in H is at most 2. We also note that the order of H (and also the order of $H \cap C_{ns}(\ell)$) divides $\ell - 1$. The group $C_{ns}(\ell)$ is isomorphic to $\mathbb{F}_{\ell^2}^*$ by the map

$$\begin{bmatrix} a & b\epsilon \\ b & a \end{bmatrix} \mapsto a + \epsilon b,$$

where ϵ is a non-quadratic residue modulo ℓ and hence it is cyclic. The unique subgroup of $C_{ns}(\ell)$ of order equal to $|H \cap C_{ns}(\ell)|$ is isomorphic to a subgroup of $\mathbb{F}_\ell^*$, i.e., it is isomorphic to a subgroup of the group of diagonal matrices.

A matrix in D^f has two eigenvalues: 1 and a. However a diagonal matrix has one eigenvalue with multiplicity two. Hence $H \cap C_{ns}(\ell) = \{(1)\}$ and H has at most two elements. For $\ell > 13$, the order of H which equals $(\ell - 1)/f$ is strictly greater than 2 since $f \leq 6$. This proves that E has potential supersingular reduction at ℓ for $\ell > 7$ and $\ell \neq 13$. ☐

Proposition 3.2. *Let $\ell > 7$ and $\ell \neq 13$. Let E be an elliptic curve defined over $\mathbb{Q}$ such that the image of $\rho_{E,\ell}$ is conjugate to a subgroup of $C_{ns}^+(\ell)$. If R is a point of order ℓ^n on E, then the degree of $\mathbb{Q}(R)$ over $\mathbb{Q}([\ell]R)$ equals ℓ^2.*

Proof. By Proposition 3.1, the elliptic curve E has potential supersingular reduction at ℓ. Let R be a point of exact order ℓ^n on E. By [LR16, Theorem 1.2(2)] the degree of the extension $\mathbb{Q}(R)$ over $\mathbb{Q}([\ell]R)$ is divisible by ℓ^2. Since the degree $[\mathbb{Q}(R) : \mathbb{Q}([\ell]R)]$ can be at most ℓ^2, we are done. ☐

Lemma 3.3. *Let $\ell > 7$ and $\ell \neq 13$. Let $x = [(E, P)]$ be a point on $X_1(\ell^n)$ such that $G_{E,\ell}$ is conjugate to a subgroup of $C_{ns}^+(\ell)$. Then $\deg(x) = \deg(\pi(x))\deg(\pi)$ where $\pi : X_1(\ell^n) \to X_1(\ell^m)$ for any $n > m$.*

Proof. This follows from Lemma 2.1, Proposition 2.2 and Proposition 3.2. ☐

Remark 3.4. If $\ell = 13$, then there are no non-CM elliptic curves with Galois representation contained in $C_{ns}^+(\ell)$ ([BDM+19]). Hence the conclusion of Proposition 3.1, Proposition 3.2 and Lemma 3.3 holds for $\ell > 7$ and for all non-CM elliptic curves defined over $\mathbb{Q}$.

3.1. **Proof of Theorem 1.2.** Let $x = [(E, P)]$ be a non-CM, non-cuspidal isolated point on $X_1(\ell^n)$ with a rational j-invariant. We may assume that E is defined over $\mathbb{Q}$. For $\ell > 7$ and $\ell \neq 13$, $\rho_{E,\ell}$ is either surjective, contained in a Borel subgroup, or the normalizer of a non-split Cartan subgroup. When $\ell = 13$, it can also be contained in an exceptional subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ by the classification given in [Zyw]. We will first show that when $\ell > 7$, x induces an isolated point on $X_1(\ell)$. Then we will rule out the existence of an isolated point on $X_1(\ell)$.

Assume $\ell > 7$. If $G_{E,\ell}$ is contained in a Borel subgroup, then by Theorem 2.7, the ℓ-adic representation of E is as large as possible given the mod ℓ representation. Using Remark 2.5 and Theorem 2.4 we conclude that if the image of $\rho_{E,\ell}$ is $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or it is contained in a Borel subgroup, then x maps to an isolated point on $X_1(\ell)$.

We assume now that $G_{E,\ell}$ is contained in the normalizer of a non-split Cartan subgroup. In this case, we do not know that the ℓ-adic representation is determined by the mod ℓ image. However, by Lemma 3.3 and Theorem 2.4, we are able to conclude that the image of x on $X_1(\ell)$ is isolated.

Assume that mod ℓ representation $G_{E,\ell}$ is exceptional. By the classification of the images of $\rho_{E,\ell}$ given in [Zyw], we may assume $\ell = 13$. Moreover by the results of [BDM+19], we know the (finitely many) j-invariants giving rise to these points. Recent work [RSZB] of Rouse, Sutherland and Zureick-Brown shows that ℓ-adic representation of E in this case is as large as possible given the mod ℓ representation. By Remark 2.5, x induces an isolated point on $X_1(\ell)$.

We may now assume that x is an isolated point on $X_1(\ell)$ with a rational j-invariant. The rest of the proof is similar to the proof of [BEL+19, Proposition 8.4]. The genus of $X_1(\ell)$ is less than $(\ell^2 - 1)/24$ for prime ℓ. If the image of $\rho_{E,\ell}$ is contained in the normalizer of a nonsplit Cartan subgroup, then the degree of x is at least $(\ell^2 - 1)/12$ by [LR13, Theorem 7.3]. By Lemma 2.3, x is not isolated. Assume $G_{E,\ell}$ is contained in a Borel subgroup. Then $\ell = 11, 17$ or 37. Assume $\ell = 11$. Since $X_1(11)$ has genus one, x cannot be isolated by Lemma 2.3. Assume $\ell = 17$. Then the degree of x is either 4 or 8. By [DMK18, Proposition 6], there are no $\mathbb{P}^1$-isolated points of degree 4. Since the Jacobian of $X_1(17)$ has only finitely many rational points, it follows that there are no isolated points of degree 4 on $X_1(17)$. Since the genus is 5, a degree 8 point cannot be isolated by Lemma 2.3. On the other hand, there are two rational j-invariants giving rise to an elliptic curve with a rational 37-isogeny. They are given by $7 \cdot 11^3$ and $-7 \cdot 137^3 \cdot 2083^3$. The first one is isolated by ([BEL+19, Proposition 8.4]).

Let $\ell = 13$. We have covered all cases except the exceptional subgroup. There are three such rational j-invariants. We compute using Magma that the degree of these points on $X_1(13)$ are greater than 3, since the genus is 2, we are done. □

Acknowledgements. The author is grateful to Abbey Bourdon, Filip Najman, Alvaro Lozano-Robledo and the anonymous referee for their comments on the earlier drafts of this paper. The author is supported by the project Marie Skłodowska-Curie actions and TUBITAK.

References

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk, *Explicit Chabauty-Kim for the split Cartan modular curve of level 13*, Ann. of Math. (2) **189** (2019), no. 3, 885–944. MR3961086

[BEL+19] Abbey Bourdon, Özlem Ejder, Yuan Liu, Frances Odumodu, and Bianca Viray, *On the level of modular curves that give rise to isolated j-invariants*, Adv. Math. **357** (2019), 106824, 33. MR4016915

[BGRW20] Abbey Bourdon, David R. Gill, Jeremy Rouse, and Lori D. Watson, *Odd degree isolated points on $X_1(N)$ with rational j-invariant*, arXiv e-prints (June 2020), arXiv:2006.14966, available at `2006.14966`.

[BP11] Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. (2) **173** (2011), no. 1, 569–584. MR2753610

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984. MR3137477

[DMK18] Maarten Derickx, Barry Mazur, and Sheldon Kamienny, *Rational families of 17-torsion points of elliptic curves over number fields*, Contemporary Mathematics (2018), 81–104.

[Elk06] Noam D. Elkies, *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*, arXiv Mathematics e-prints (December 2006), math/0612734, available at `math/0612734`.

[Fre94] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83. MR1264340

[Gre12] Ralph Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), no. 5, 1167–1196. MR2975233

[Gre14] R. Greenberg, *On elliptic curves with an isogeny of degree* 7, Amer. J. Math. **136** (2014), no. 1, 77–109. MR3163354

[Lem19] Pedro Lemos, *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*, Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146. MR3885140

[LR13] Álvaro Lozano-Robledo, *On the field of definition of p-torsion points on elliptic curves over the rationals*, Math. Ann. **357** (2013), no. 1, 279–305. MR3084348

[LR16] Álvaro Lozano-Robledo, *Ramification in the division fields of elliptic curves with potential supersingular reduction*, Res. Number Theory **2** (2016), Art. 8, 25. MR3501021

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR482230

[RSZB] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of galois for elliptic curves over $\mathbb{Q}$*, preprint, arXiv:2106.11141.

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR387283

[Smi20] Hanson Smith, *Ramification in division fields and sporadic points on modular curves*, 2020.

[Sut16] Andrew V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79. MR3482279

[Zyw] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over q*, preprint, arXiv:1508.07660.

Boğaziçi University, Department of Mathematics, Istanbul, Turkey
Email address: `ozlem.ejder@boun.edu.tr`
URL: `https://sites.google.com/site/ozheidi/Home`