UNIFORM BOUNDS ON THE IMAGE OF ARBOREAL GALOIS REPRESENTATIONS ATTACHED TO NON-CM ELLIPTIC CURVES

MICHAEL CERCHIA AND JEREMY ROUSE

Abstract. Let $\ell$ be a prime number and let $F$ be a number field and $E/F$ a non-CM elliptic curve with a point $\alpha \in E(F)$ of infinite order. Attached to the pair $(E, \alpha)$ is the $\ell$-adic arboreal Galois representation $\omega_{E,\alpha,\ell} : \text{Gal}(\overline{F}/F) \to \mathbb{Z}_\ell^2 \rtimes \text{GL}_2(\mathbb{Z}_\ell)$ describing the action of $\text{Gal}(\overline{F}/F)$ on points $\beta_n$ so that $\ell^n \beta_n = \alpha$. We give an explicit bound on the index of the image of $\omega_{E,\alpha,\ell}$ depending on how $\ell$-divisible the point $\alpha$ is, and the image of the ordinary $\ell$-adic Galois representation. The image of $\omega_{E,\alpha,\ell}$ is connected with the density of primes $p$ for which $\alpha \in E(F_p)$ has order coprime to $\ell$.

1. Introduction and Statement of Results

Let $F$ be a number field, $E/F$ an elliptic curve, and $\alpha \in E(F)$ a point of infinite order. For each prime $p$ of $F$ of good reduction for $E$, $E(F_p)$ is a finite abelian group and so $\alpha \in E(F_p)$ has finite order. It is natural to ask how often $\alpha$ has odd order or even order (or more generally how often the order of $\alpha$ is coprime to any fixed prime $\ell$). It seems reasonable to guess that $\alpha$ has odd order “half” the time. However, in [7], Rafe Jones and the second author determined that for $E : y^2 + y = x^3 - x$ and $\alpha = (0, 0)$, the density of primes $p$ for which $\alpha \in E(F_p)$ has odd order is $\frac{11}{21}$.

It is elementary to see that $\alpha \in E(F_p)$ has order coprime to $\ell$ if and only for all $n \geq 1$ there is some $\beta_n \in E(F_p)$ so that $\ell^n \beta_n = \alpha$. This connects the order of $\alpha \in E(F_p)$ with Galois-theoretic properties of the preimages $\beta_n$ of $\alpha$ under multiplication by powers of $\ell$. These are governed by the arboreal Galois representation $\omega_{E,\alpha,\ell}$. To define this, we need some notation.

Let $E[\ell^n]$ denote the set of points of order dividing $\ell^n$ on $E$ and define $\rho_{E,\ell^n} : \text{Gal}(E[\ell^n]/F) \to \text{Aut}(E[\ell^n]) \cong \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ be the usual mod $\ell^n$ Galois representation. Let $T_n = F(E[\ell^n])$ and $T_\infty = \bigcup_{n=1}^{\infty} F(E[\ell^n])$.

2010 Mathematics Subject Classification. Primary 11F80; Secondary 11G05, 12G05.
The representations \(\rho_{E,\ell^n}\) are compatible, and if we let \(T_\ell(E) = \lim E[\ell^n]\) be the \(\ell\)-adic Tate module of \(E\), we get a representation \(\rho_{E,\ell,\infty} : \text{Gal}(T_\ell(E)/F) \to \text{Aut}(T_\ell(E)) \cong \text{GL}_2(\mathbb{Z}_\ell)\). Serre [13] has proven that if \(E/F\) does not have complex multiplication, the image of \(\rho_{E,\ell,\infty}\) is a finite index subgroup of \(\text{GL}_2(\mathbb{Z}_\ell)\). Given an \(\alpha \in E(F)\), fix a sequence of points \(\beta_1, \beta_2, \ldots\) so that \(\ell \beta_1 = \alpha\) and \(\ell \beta_n = \beta_{n-1}\) for \(n \geq 1\). Let \(K_n = F[\ell^n, \beta_n]\). For each \(\sigma \in \text{Gal}(K_n/F)\), \(\sigma(\beta_n)\) is also a preimage of \(\alpha\) under multiplication by \(\ell^n\) and so \(\sigma(\beta_n) - \beta_n \in E(\ell^n)\). Define \(\omega_{E,\ell,\infty} : \text{Gal}(K_n/F) \to E[\ell^n] \times \text{Aut}(E[\ell^n])\) by \(\omega_{E,\ell,\infty}(\sigma) = (\sigma(\beta_n) - \beta_n, \sigma|_{E[\ell^n]})\). These representations are again compatible and if we let \(K_\infty = \bigcup_{n=1}^{\infty} K_n\), they give rise to \(\omega_{E,\ell,\infty} : \text{Gal}(K_\infty/F) \to T_\ell(E) \times \text{Aut}(T_\ell(E)) \cong \mathbb{Z}_\ell^2 \times \text{GL}_2(\mathbb{Z}_\ell)\). Theorem 3.2 of [7] shows that the density of primes \(p\) for which \(\alpha \in E(\mathbb{F}_p)\) has order coprime to \(\ell\) only depends on the image of \(\omega_{E,\ell,\infty}\), and Theorem 5.5 of [7] shows that, in the case that \(\omega_{E,\ell,\infty}\) is surjective, the density of primes for which \(\alpha\) has order coprime to \(\ell\) is \(\frac{\ell^{3}\ell^{3}+\ell^{3}+1}{\ell^{3}-\ell^{2} + \ell + 1}\).

The goal of the present paper is to prove uniformity results about the image of \(\omega_{E,\ell,\infty}\). In [10] (see Definition 4.1) the authors declare a point \(\alpha \in E(F)\) to be strongly \(\ell\)-indivisible if \(\alpha + T \notin E(F)\) for any torsion point \(T \in E(F)\) of \(\ell\)-power order. This is a natural primivity condition to impose. Without this condition, the index of the image of \(\omega\) in \(\mathbb{Z}_\ell^2 \times \text{GL}_2(\mathbb{Z}_\ell)\) can be arbitrarily large, and the corresponding density can be made very large (by taking \(\alpha = \ell^k\gamma\) for some large \(k\) and \(\gamma \in E(F)\)) or very small (by taking \(\alpha = \ell^k\gamma + T\) for \(\gamma \in E(F)\) and \(T \in E[\ell](F)\)). Moreover, if \(\alpha + T = \ell\gamma\) for \(\gamma \in E(F)\) one can read off the representation \(\omega_{E,\ell,\infty}\) from that of \(\omega_{E,\gamma,\ell,\infty}\).

In [8], the authors show that if \(E = \mathbb{Q}\), \(\ell = 2\), \(\rho_{E,2,\infty}\) is surjective, and \(\alpha\) is strongly 2-indivisible, then \(\omega_{E,\alpha,2,\infty}\) is either surjective (in which case the density of primes \(p\) for which \(\alpha\) has odd order is 11/21), or the image of \(\omega_{E,\alpha,2,\infty}\) has index 4 in \(\mathbb{Z}_2^2 \times \text{GL}_2(\mathbb{Z}_2)\), and the odd order density is 179/336. This latter case arises when \(\mathbb{Q}(\beta_1) \subset \mathbb{Q}(E[4])\).

In [9], it is shown that if the image of \(\rho_{E,2,\infty} = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, d \in \mathbb{Z}_2^\times, b \in \mathbb{Z}_2 \right\}\), and \(\alpha\) is strongly 2-indivisible, then there are 63 possibilities for the image of \(\omega_{E,\alpha,2,\infty}\) up to conjugacy in \(\mathbb{Z}_2^2 \times \text{GL}_2(\mathbb{Z}_2)\) and the odd order density can vary between 1/14 and 89/168.

The main result of the present paper is the following.

**Theorem 1.** Suppose that \(F\) is a number field, \(\ell\) is a prime, \(E/F\) is a non-CM elliptic curve with \(\text{im} \rho_{E,\ell,\infty} = G\), and let \(d\) be the largest positive integer for which \(\alpha = \ell^d\gamma + T\) for some \(\gamma \in E(F)\) and some \(F\)-rational \(\ell\)-power torsion point \(T\). Then, the index of \(\text{im} \omega_{E,\alpha,\ell,\infty}\) in \(\mathbb{Z}_\ell^2 \times \text{GL}_2(\mathbb{Z}_\ell)\) is at most \(\ell^{2d+2r+s} \cdot |\text{GL}_2(\mathbb{Z}_\ell) : G|\), where \(r\) is the smallest positive integer so that \(G\) contains a matrix \(\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}\) with \(\text{ord}_\ell(x-1) = r\),
and $s$ is the largest positive integer such that there is a degree $\ell^s$ cyclic isogeny $E \to E'$ defined over $F$.

**Remark.** The paper \[10\], by Lombardo and Tronto which was finished at nearly the same time as this present paper, contains a similar result to the one above. In particular, Theorem 4.15 gives a bound on the index of the image of $\omega_{E,\alpha,\ell}\mid_{\text{Gal}(K_\infty/T_\infty)}$ in $\mathbb{Z}_\ell^2$ in terms of the parameter $n_\ell$ (the smallest positive integer so that the image of $\rho_{E,\ell}\mid_{\text{Gal}(K_\infty/T_\infty)}$ contains all matrices $\equiv I \pmod{\ell^{n_\ell}}$). The bound given in Theorem 4.15 is $2d + 4n_\ell$, while the bound we give is $\leq 2d + 3n_\ell$.

**Remark.** Indeed, the bound in Theorem 1 is sharp in many instances. For example, if $E : y^2 = x^3 - 343x + 2401$ and $\alpha = (0, -49)$, then $\alpha$ is strongly $2$-indivisible (and so $d = 0$). The image $G$ of $\rho_{E,2}\mid_{\text{Gal}(K_\infty/T_\infty)}$ is an index 4 subgroup of $\text{GL}_2(\mathbb{Z}_\ell)$ and corresponds to the modular curve $X_{2\alpha}$ of \[12\]. The curve $E$ has no cyclic isogenies defined over $\mathbb{Q}$ and so $s = 0$, while $G$ contains $5I$ but does not contain $mI$ for any $m \equiv 3 \pmod{4}$. Thus, $r = 2$. One can explicitly compute that if $\beta_2$ is a point such that $4\beta_2 = \alpha$, then $\beta_2 \in E(\mathbb{Q}(E[8]))$ and this implies that the image of $\omega_{E,\alpha,2}\mid_{\text{Gal}(K_\infty/T_\infty)}$ has index 64 in $\mathbb{Z}_\ell^2 \rtimes \text{GL}_2(\mathbb{Z}_\ell)$. We have that $64 = 2^{2d+2r+s} \cdot |\text{GL}_2(\mathbb{Z}_\ell) : G|$.

The parameters $r$ and $s$ in the theorem above depend only on the structure of $T_\ell(E)$ as a Galois module, and hence only on $G$. We can strengthen the above result using known results about the image of $\rho_{E,\ell}\mid_{\text{Gal}(K_\infty/T_\infty)}$.

**Theorem.** If $m$ is a fixed positive integer, then as $E$ ranges over all non-CM elliptic curves $E/F$, where $[F : \mathbb{Q}] = m$, there is an absolute bound on the index of the image of $\rho_{E,\ell}\mid_{\text{Gal}(K_\infty/T_\infty)}$ in $\text{GL}_2(\mathbb{Z}_\ell)$.

A complete proof of this theorem can be found in \[5\] (see Theorem 2.3(a)), relying on work of Serre \[13\], Abramovich \[1\], and Frey \[6\]. A more general statement is the main theorem of \[4\].

The above result immediately yields the following corollary.

**Corollary 2.** Fix a positive integer $m$ and a prime $\ell$. Then there is a constant $C(m, \ell)$ with the following property. For all number fields $F$ with $[F : \mathbb{Q}] = m$ and for all pairs of curves and points $E/F$ and $\alpha \in E(F)$ which are strongly $\ell$-indivisible, the image of $\omega_{E,\alpha,\ell}\mid_{\text{Gal}(K_\infty/T_\infty)}$ in $\mathbb{Z}_\ell^2 \rtimes \text{GL}_2(\mathbb{Z}_\ell)$ has index $\leq C(m, \ell)$.

We prove Theorem \[11\] by showing that the fields $F(\beta_n)$ and $T_n = F(E[\ell^n])$ are “approximately disjoint”. The failure of disjointness of these fields is related to the exponent of the cohomology group $H^1(T_n/F, E[\ell^n])$. The order of this cohomology group can be shown to be uniformly bounded (as a function of $m$ and $n$) in terms of the image of $\rho_{E,\ell}\mid_{\text{Gal}(K_\infty/T_\infty)}$. 
Acknowledgements. This work represents the master’s thesis of the first author completed at Wake Forest University in the spring of 2019.

2. Background

Let $G$ be a topological group and let $M$ be a right topological $G$-module. Define as usual the group $H^1(G, M)$ of continuous 1-cocycles $\xi : G \to M$ modulo 1-coboundaries. We will use the following Lemma of Sah (see [8] for a proof).

Lemma 3. If $\alpha \in Z(G)$, then the endomorphism $(\alpha - 1)$ of $H^1(G, M)$ is the zero map.

3. Proof of Theorem 1

Let $F$ be a number field, $E/F$ an elliptic curve and $\alpha \in E(F)$ be a non-torsion point. Let $d$ be the smallest positive integer so that $\alpha = \ell^d \gamma + T$ for some $\gamma \in E(F)$ and $T$ an $F$-rational $\ell$-power torsion point. Define a sequence of points $\beta_1, \beta_2, \ldots$ so that $\ell \beta_1 = \alpha$ and $\ell \beta_n = \beta_{n-1}$. As in Section 1 define $T_n = F(E[\ell^n])$, $T_\infty = \bigcup_{n=1}^{\infty} T_n$, $K_n = F(E[\ell^n], \beta_n)$ and $K_\infty = \bigcup_{n=1}^{\infty} K_n$ and $\omega_{E,\alpha,\ell^n} : \text{Gal}(K_\infty/F) \to \mathbb{Z}_\ell^2 \times GL_2(\mathbb{Z}_\ell)$. Define $\kappa_{E,\alpha,\ell^n} : \text{Gal}(K_\infty/T_\infty) \to T_\ell(E)$ to be the first coordinate of $\omega_{E,\alpha,\ell^n}$, namely $\kappa(\sigma) = (\sigma(\beta_1) - \beta_1, \sigma(\beta_2) - \beta_2, \ldots) \in \lim_i E[\ell^i] = T_\ell(E)$. In [2], Bertrand shows that the image of $\kappa$ has finite index in $T_\ell(E)$ using similar cohomological arguments to those of Ribet in [11].

Proof of Theorem 1: We fix $G = \text{im } \rho_{E,\ell^n} \subseteq GL_2(\mathbb{Z}_\ell)$ and let $r$ and $s$ be as defined in the statement of Theorem 1. We show that if $m > r + d$ then $\beta_m \notin E(T_\infty)$. Suppose to the contrary that $\beta_m \in E(T_\infty)$ and define $\xi : \text{Gal}(T_\infty/F) \to E[\ell^m]$ by $\xi(\sigma) = \sigma(\beta_m) - \beta_m$. This is a 1-cocycle and gives rise to an element of $H^1(T_\infty/F, E[\ell^m])$. If $g = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \in G$ with $\text{ord}_\ell(x - 1) = r$, then $g - I$ kills every element of $H^1(T_\infty/F, E[\ell^m])$. This is the same as multiplication by $x - 1$. Since $H^1(T_\infty/F, E[\ell^m])$ is an $\ell$-group, it follows that $\ell \xi$ is a 1-coboundary. Thus, there is some $T \in E[\ell^m]$ so that $\ell \sigma(\beta_m) - \ell \beta_m = \sigma(T) - T$ for all $\sigma \in \text{Gal}(T_\infty/F)$. This implies that $Q = \ell^r \beta_m - T \in E(F)$, which leads to a contradiction because $\alpha = \ell^{m-r}Q + \ell^{m-r}T$, and $\alpha \in E(F)$ and $Q \in E(F)$ implies that $\ell^{m-r}T \in E(F)$ is an $\ell$-power torsion point.

It follows that there is some $\sigma \in \text{Gal}(K_\infty/T_\infty)$ so that $\sigma(\beta_{r+d+1}) \neq \beta_{r+d+1}$. Consider $\vec{\sigma} = \kappa(\sigma) = (\sigma(\beta_1) - \beta_1, \sigma(\beta_2) - \beta_2, \ldots) \in T_\ell(E) \cong \mathbb{Z}_\ell^2$.
as a row vector. The reduction of \( \vec{v} \) in \((\mathbb{Z}/\ell^{r+d+1}\mathbb{Z})^2\) is nonzero and therefore, the minimal \( \ell \)-adic valuation of the coordinates is at most \( r + d \). Write \( \vec{v} = \ell^t \vec{p} \), where \( \vec{p} \) is a primitive vector (one where not both entries are \( \equiv 0 \) (mod \( \ell \))). Since the image of \( \kappa \subseteq \mathbb{Z}_\ell^2 \) has a natural action of \( \mathcal{G} = \text{im } \rho_{E,\ell^\infty} \) on it, the image of \( \alpha \) contains \( \ell^t \vec{p}g \) for all \( g \in G \). Let \( S \subseteq \mathbb{Z}_\ell^2 \) be the smallest subgroup containing \( \vec{p}g \) for all \( g \in G \). Since \( G \) is open in \( \text{GL}_2(\mathbb{Z}_\ell) \), there is a positive integer \( k \) so that \( G \) contains all \( g \equiv I \) (mod \( \ell^k \)). A straightforward calculation shows that for any \( \vec{q} \equiv \vec{p} \) (mod \( \ell^k \)) there exists some \( g \equiv I \) (mod \( \ell^k \)) so that \( gp = \vec{q} \). It follows that \( S \) contains all vectors \( \equiv \vec{0} \) (mod \( \ell^k \)). Define \( \overline{S} = \{ \vec{v} \text{ mod } \ell^k : \vec{v} \in S \} \) and identify \( \overline{S} \) with a subgroup of \( E[\ell^k] \). Then \( \overline{S} \) contains a primitive vector and is stable under the action of \( \text{Gal}(\mathbb{T}_\infty/F) \). From Proposition III.4.12 and Remark III.4.13.2 of [15] it follows that there is an \( F \)-rational cyclic isogeny \( \phi : E \to E' \) for some elliptic curve \( E'/F \) whose kernel is \( \overline{S} \). We have then that
\[
|Z_\ell^2 : S| = |(\mathbb{Z}/\ell^k\mathbb{Z})^2 : \overline{S}|
\]
is less than or equal to the maximum degree of an \( \ell \)-power isogeny \( \phi : E \to E' \) defined over \( F \), namely \( \ell^a \). Since the image of \( \alpha \) contains \( \ell^{r+d} : S \), it follows that the index of the image of \( \alpha \) is \( \leq \ell^{2d+2r+s} \) and moreover that the image of \( \alpha \) contains all \( \vec{v} \equiv 0 \) (mod \( \ell^{d+r+s} \)).

Next, we show that the image of \( \omega_{E,\alpha,\ell^\infty} \) has finite index in \( \mathbb{Z}_\ell^2 \times \text{GL}_2(\mathbb{Z}_\ell) \). Let \( n \) be the number of elements in the set \( \{ \vec{g} \text{ mod } \ell^{d+r+s} : (\vec{g}, g) \in \text{im } \omega \text{ for some } g \in \text{GL}_2(\mathbb{Z}_\ell) \} \), and let \( \vec{g}_1, \ldots, \vec{g}_n \) be elements in \( \mathbb{Z}_\ell^2 \) that reduce mod \( \ell^{d+r+s} \) to the elements of that set. For any \( (\vec{g}, g) \in \text{im } \omega \), there is some \( \vec{g}_i \) so that \( \vec{g} \equiv \vec{g}_i \) (mod \( \ell^{d+r+s} \)). We then get that \( (\vec{g}_i, g) = (\vec{g}, g) * (\vec{g}_i - \vec{g}, I) \) is in the image of \( \omega_{E,\alpha,\ell^\infty} \).

Let \( H = \{ g \in \text{GL}_2(\mathbb{Z}_\ell) : (\vec{0}, g) \in \text{im } \omega \} \). We will prove that \( H \) is a finite index subgroup of \( \text{GL}_2(\mathbb{Z}_\ell) \). Define \( m = \max\{k, d + r + s\} \) and let \( \Gamma(\ell^m) = \{ g \in \text{GL}_2(\mathbb{Z}_\ell) : g \equiv I \text{ (mod } \ell^m) \} \). In particular, we will show that if \( g_1 \equiv g_2 \) (mod \( \ell^m \)) and \( (\vec{g}_i, g_1) \) and \( (\vec{g}_i, g_2) \) are both in the image of \( \omega \), then \( g_1 \) and \( g_2 \) are in the same left coset of \( H \cap \Gamma(\ell^m) \). Letting \( \vec{x} = -\vec{g}_i(-g_1^{-1}g_2 + I) \) we have that \( \vec{x} \equiv 0 \) (mod \( \ell^m \)) and hence \( (\vec{x}, I) \in \text{im } \omega \). Therefore
\[
(\vec{g}_i, g_1)^{-1} * (\vec{g}_i, g_2) * (\vec{x}, I) = (\vec{g}_i(-g_1^{-1}g_2 + I), g_1^{-1}g_2)*(-\vec{g}_i(-g_1^{-1}g_2 + I)) = (\vec{0}, g_1^{-1}g_2) \in \text{im } \omega
\]
and thus \( g_1^{-1}g_2 \in H \cap \Gamma(\ell^m) \). Since every \( g \in \Gamma(\ell^m) \) has the property that \( (\vec{g}_i, g) \in \text{im } \omega \) for some \( i \), it follows that \( |\Gamma(\ell^m) : H \cap \Gamma(\ell^m)| \leq n \) and so \( |\text{GL}_2(\mathbb{Z}_\ell) : H| \leq |\text{GL}_2(\mathbb{Z}_\ell) : H \cap \Gamma(\ell^m)| \leq |\text{GL}_2(\mathbb{Z}_\ell) \cap \Gamma(\ell^m)| \leq n \cdot |\text{GL}_2(\mathbb{Z}/\ell^m\mathbb{Z})| \) is finite. Since \( \Gamma(\ell^m) \) is a topologically finitely generated pro-\( \ell \) group, a theorem of Serre (see Section 4.2 of [14]) shows that \( H \cap \Gamma(\ell^m) \) is open in \( \Gamma(\ell^m) \) and hence in \( \text{GL}_2(\mathbb{Z}_\ell) \). It follows that there is some integer \( v \geq m \) so that every \( g \equiv I \) (mod \( \ell^v \)) is contained in \( H \). Finally, if \( \vec{x} \equiv 0 \) (mod \( \ell^v \)) and \( g \equiv I \) (mod \( \ell^v \)) then \( (\vec{x}, I) \) and \( (\vec{0}, g) \) are both in the
image of $\omega$ and so the image of $\omega$ contains $(\vec{0}, h) \ast (\vec{x}, I) = (\vec{x}, h)$ and hence all $(\vec{x}, h)$ with $\vec{x} \equiv 0 \pmod{\ell^v}$ and $h \equiv I \pmod{\ell^v}$. This implies that the image of $\omega$ is the full preimage in $\mathbb{Z}_\ell^2 \rtimes \text{GL}_2(\mathbb{Z}_\ell)$ of the image of $\omega_{E, \alpha, \ell^v}$. The map $\kappa_v : \text{Gal}(\mathbb{K}_v/\mathbb{T}_v) \to E[\ell^v]$ given by $\kappa_v(\sigma) = \sigma(\beta_v) - \beta_v$ has an image that contains the mod $\ell^v$ reduction of the image of $\kappa$, and $\text{Gal}(\mathbb{T}_v/F)$ has index $|\text{GL}_2(\mathbb{Z}_\ell) : G|$ inside $\text{GL}_2(\mathbb{Z}/\ell^v\mathbb{Z})$. It follows from this that

$$|\mathbb{Z}_\ell^2 \rtimes \text{GL}_2(\mathbb{Z}_\ell) : \text{im} \omega| \leq \ell^{2d+2r+s}|\text{GL}_2(\mathbb{Z}_\ell) : G|,$$

as desired. □

References

[1] Dan Abramovich. A linear lower bound on the gonality of modular curves. *Internat. Math. Res. Notices*, (20):1005–1011, 1996.

[2] D. Bertrand. Galois representations and transcendental numbers. In *New advances in transcendence theory (Durham, 1986)*, pages 37–55. Cambridge Univ. Press, Cambridge, 1988.

[3] Alexi Block Gorman, Tyler Genao, Heesu Hwang, Noam Kantor, Sarah Parsons, and Jeremy Rouse. The density of primes dividing a particular non-linear recurrence sequence. *Acta Arith.*, 175(1):71–100, 2016.

[4] Anna Cadoret and Akio Tamagawa. A uniform open image theorem for $\ell$-adic representations, II. *Duke Math. J.*, 162(12):2301–2344, 2013.

[5] Pete L. Clark and Paul Pollack. Pursuing polynomial bounds on torsion. *Israel J. Math.*, 227(2):889–909, 2018.

[6] Gerhard Frey. Curves with infinitely many points of fixed degree. *Israel J. Math.*, 85(1-3):79–83, 1994.

[7] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[8] Serge Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[9] Ke Liang and Jeremy Rouse. Density of $\ell$-adic order reductions for elliptic curves with a rational point of order 2. *Int. J. Number Theory*, 15(8):1547–1563, 2019.

[10] Davide Lombardo and Sebastiano Tronto. Explicit Kummer theory for elliptic curves, 2019.

[11] Kenneth A. Ribet. Kummer theory on extensions of abelian varieties by tori. *Duke Math. J.*, 46(4):745–761, 1979.

[12] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.