Arithmetic statistics for the fine Selmer group in Iwasawa theory

Anwesh Ray\textsuperscript{1*} and R. Sujatha\textsuperscript{2}

Abstract
We study arithmetic statistics for Iwasawa invariants for fine Selmer groups associated to elliptic curves.

Keywords: Arithmetic statistics, Iwasawa theory, Fine Selmer groups, Elliptic curves, Local torsion, Euler characteristic

Mathematics Subject Classification: 11G05, 11R23 (primary); 11R45 (secondary)

1 Introduction
Iwasawa studied growth questions of class groups in certain infinite towers of number fields. These initial developments led to deep questions, many of which are still unresolved. Given a number field $F$ and a prime number $p$, let $F_{\text{cycl}}$ denote the cyclotomic $\mathbb{Z}_p$-extension of $F$. Letting $F_n \subset F_{\text{cycl}}$ be such that $[F_n : F] = p^n$, denote by $\text{Cl}_p(F_n)$ the $p$-Sylow subgroup of the class group of $F_n$. Iwasawa showed that for $n \gg 0$,

$$\# \text{Cl}_p(F_n) = p^{\mu n + \lambda n + \nu}$$

where $\mu, \lambda, \nu \in \mathbb{Z}_{\geq 0}$ and $\nu \in \mathbb{Z}$. Let $K(F_{\text{cycl}}) \subset \bar{K}$ be the maximal abelian pro-$p$ extension of $F_{\text{cycl}}$ in which all primes of $F_{\text{cycl}}$ are unramified. The classical $\mu = 0$ conjecture of Iwasawa states that $X(F_{\text{cycl}}) := \text{Gal}(K(F_{\text{cycl}})/F_{\text{cycl}})$ is finitely generated as a $\mathbb{Z}_p$-module. Equivalently, the invariant $\mu$ in (1.1) is equal to 0. The $\mu = 0$ conjecture was proved by Ferrero and Washington [9] for all abelian number fields $F/\mathbb{Q}$.

Mazur initiated the Iwasawa theory of elliptic curves and abelian varieties in [22]. Let $E$ be an elliptic curve and $p$ an odd prime number at which $E$ has good ordinary reduction. The main object of study is the $p$-primary Selmer group over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Greenberg conjectured that when the residual representation on the $p$-torsion subgroup of $E$ is irreducible, the Iwasawa $\mu$-invariant of this Selmer group must vanish, see [11, Conjecture 1.11]. This means that the Pontryagin dual of the Selmer group over $\mathbb{Q}_{\text{cycl}}$ is a finitely generated $\mathbb{Z}_p$-module. The rank of the dual Selmer group as a $\mathbb{Z}_p$-module is the $\lambda$-invariant, and is of significant interest. It was proven by Kato [16] and Rohrlich [27] that the rank of $E(\mathbb{Q}_{\text{cycl}})$ is bounded as $n \to \infty$. In fact, rank $E(\mathbb{Q}_{\text{cycl}})$ is always bounded above by the $\lambda$-invariant. When the residual representation is reducible, there are examples and explicit criteria under which the $\mu$-invariant is positive, see [28, sections 3 and 7].
Let $E_{/\mathbb{Q}}$ be an elliptic curve with good reduction at an odd prime $p$ (either ordinary or supersingular). The fine Selmer group was systematically studied by Coates and the second named author in [4]. This is the subgroup $R_{p}\sim (E/\mathbb{Q}_{\text{cyc}})$ of the $p$-primary Selmer group over $\mathbb{Q}_{\text{cyc}}$ consisting of all cohomology classes that are trivial when localized at the primes above $p$ and the primes at which $E$ has bad reduction (cf. Definitions 2.1 and 2.2). The fine Selmer group is closely related to class group extensions studied by Iwasawa. Conjecture A in [4] predicts that the $\mu$-invariant of the fine Selmer group is always zero. Let $F = \mathbb{Q}(E[p])$ be the extension of $\mathbb{Q}$ which is cut out by the residual representation on $E[p]$. In other words, it is the Galois extension of $\mathbb{Q}$ fixed by the kernel of the residual representation. By Serre’s Open image theorem [30, section 4, Theorem 3], if $E$ is a non-CM elliptic curve, $\text{Gal}(F/\mathbb{Q})$ is isomorphic to $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for all but finitely many primes $p$. Thus, the extension $F/\mathbb{Q}$ is in most cases non-abelian and in fact, non-solvable; and Iwasawa’s $\mu = 0$ conjecture is wide open for such extensions. It follows from results of Coates and the second named author that Iwasawa’s $\mu = 0$ conjecture for $\text{Gal}(K(\mathbb{F}_{\text{cyc}})/\mathbb{F}_{\text{cyc}})$ is closely related to the $\mu = 0$ conjecture for the fine Selmer group. In greater detail, the $\mu$-invariant vanishes for the fine Selmer group over $\mathbb{F}_{\text{cyc}}$ vanishes if and only if the classical Iwasawa $\mu$-invariant for $X(\mathbb{F}_{\text{cyc}})$ vanishes (cf. Theorem 2.3).

The arithmetic statistics of elliptic curves is concerned with the study of the average behaviour of certain interesting arithmetic invariants associated with elliptic curves. One such invariant is the rank of the Mordell–Weil group. A conjecture of Katz and Sarnak [19] supported with heuristics from random matrix theory predicts that when ordered by height (or conductor or discriminant), 50% of all elliptic curves have rank 0 and the other 50% have rank 1. Certain unconditional results on rank distribution have been proven by Bhargava and Shankar [2] who study the average cardinality of certain Selmer groups over $\mathbb{Q}$. This provides ample motivation to study the average behavior of Iwasawa invariants of elliptic curves associated to Selmer groups over $\mathbb{Q}_{\text{cyc}}$. The main difficulty is that the methods of Bhargava and Shankar can only be applied to $n$ Selmer groups over $\mathbb{Q}$ and for numbers $n \leq 5$. Therefore, an altogether different method is required to study Selmer groups over the cyclotomic $\mathbb{Z}_p$-extension. Arithmetic statistics for the Iwasawa theory of elliptic curves was initiated by Kundu and the first named author in [17]. In the present article, we study similar questions for the fine Selmer group. In greater detail, we study the following questions:

1. Fix a prime number $p$. What can be said about the proportion of elliptic curves $E_{/\mathbb{Q}}$ with good reduction at $p$ for which the $p$-primary fine Selmer group over $\mathbb{Q}_{\text{cyc}}$ is infinite (i.e., either $\mu > 0$ or $\lambda > 0$)? Here, the elliptic curves are ordered according to their naive height (cf. Sect. 4 for further details).

2. Given an elliptic curve $E_{/\mathbb{Q}}$ and a fixed positive number $Y > 0$, what can be said about the number of primes $p \leq Y$ at which $E$ has good reduction and the fine Selmer group of $E$ over $\mathbb{Q}_{\text{cyc}}$ is infinite.

In Sect. 4, we study the first question and prove explicit results. From a statistical point of view it makes sense to only consider elliptic curves of rank $\leq 1$ (since the elliptic curves of rank $> 1$ are expected to constitute a set of density 0). Let $p$ be a prime $\geq 5$. Consider the set $\mathcal{B}_p$ (resp. $\mathcal{D}_p$) consisting of elliptic curves $E_{/\mathbb{Q}}$ that have Mordell–Weil rank 0 (resp. 1), good reduction at $p$, and for which the $p$-primary fine Selmer group $R_{p}\sim (E/\mathbb{Q}_{\text{cyc}})$ is infinite. Theorem 4.7 gives a precise upper bound for the upper natural density of $\mathcal{B}_p$ in
terms of $p$. In greater detail, let $\delta(\mathfrak{B}_p)$ denote the upper density of $\mathfrak{B}_p$ (see Definition 4.1 for a precise definition). Let $f, g$ and $h$ be functions defined on the set of primes $p$, taking positive real values. Then, we say that $f(p) \leq g(p) + O(h(p))$ if $f(p) \leq g(p) + ch(p)$ for some constant $c \geq 0$. We view the association $p \mapsto \delta(\mathfrak{B}_p)$ as a function on the set of prime numbers $p$. We show that

$$\delta(\mathfrak{B}_p) \leq \frac{2\zeta(10)}{p} + O\left(\frac{\log p (\log \log p)^2}{p^{1/2}}\right).$$

A similar bound is also obtained for the function $p \mapsto \delta(\mathfrak{Q}_p)$, see Theorem 4.9. The bounds we obtain for $\delta(\mathfrak{B}_p)$ and $\delta(\mathfrak{Q}_p)$ are conditional. For all primes $p$ for which our bounds are valid, it is assumed that $\mathbb{III}(E/\mathbb{Q})[p^\infty]$ is finite. Furthermore, we assume a conjecture of Delaunay on the density of elliptic curves $E/\mathbb{Q}$ for which $\mathbb{III}(E/\mathbb{Q})[p^\infty] \neq 0$. We refer to Conjecture 4.4 for a precise statement. One also considers the set $\mathfrak{g}_p$ of all elliptic curves $E/\mathbb{Q}$ with Mordell–Weil rank 0 and good ordinary reduction at $p$, such that the entire Selmer group $\text{Sel}_p(E/\mathbb{Q}_{\text{cycl}})$ is infinite. The bound obtained for $\delta(\mathfrak{g}_p)$ in [17, section 4] is of the form

$$\delta(\mathfrak{g}_p) = O\left(\frac{\log p (\log \log p)^2}{p^{1/2}}\right)$$

(see Theorem 4.5 for the refined statement). The results show that that given a prime $p$ the fine Selmer group $\mathcal{R}_p^{\infty}(E/\mathbb{Q}_{\text{cycl}})$ of most elliptic curves is finite. Furthermore, we give an explicit upper bound for the proportion of elliptic curves for which $\mathcal{R}_p^{\infty}(E/\mathbb{Q}_{\text{cycl}})$ may be infinite and this proportion becomes smaller as $p$ gets larger. In fact, the quantity decreases at the rate of $O(1/p)$. On the other hand, for elliptic curves of rank 0, the Selmer group $\text{Sel}_p^{\infty}(E/\mathbb{Q}_{\text{cycl}})$ shows similar behavior on average. However, as $p$ gets larger, the upper bound decreases at a much slower rate.

In Sect. 5, we study a variant of the second question. Let $E$ be an elliptic curve with Mordell–Weil rank zero. According to Corollary 2.10, the set of primes $p$ at which $\mathcal{R}_p^{\infty}(E/\mathbb{Q}_{\text{cycl}})$ is infinite is contained in the set of primes $\Pi_{lt,E} \cup \mathfrak{S}$. Here, $\Pi_{lt,E}$ is the set of primes $p$ at which $E(\mathbb{Q}_p)[p] \neq 0$. Such primes are referred to as the set of local torsion primes. On the other hand, $\mathfrak{S}$ is an explicit finite set of primes (see loc. cit. for details). Given a positive number $Y > 0$, we denote by $\Pi_{lt,E}(Y)$ the set of local torsion primes $p$ that are $\leq Y$. We prove results about the expected size of $\#\Pi_{lt,E}(Y)$ when $Y$ is fixed and $E$ ranges over all elliptic curves. This gives us some insight into the number of primes $\leq Y$ at which the fine Selmer group may be infinite. We use a version of the Large Sieve inequality due to Huxley, see Theorem 5.2. Fix $Y > 0$ (for example $Y = 100$), let $P(Y) := \sum_{p \leq Y} \frac{\#\mathfrak{S}_p}{p^3}$ be the quantity defined in the discussion following the proof of

Theorem 5.3. Here, the fraction $\frac{\#\mathfrak{S}_p}{p^3}$ represents the proportion of elliptic curves $E$ over $\mathbb{Z}_p$ such that $E(\mathbb{Q}_p)[p] \neq 0$. We refer to Definition 3.7 for the precise definition of the set $\mathfrak{S}_p$. The main result of Sect. 5, Theorem 5.4, shows that $P(Y)$ is a good estimate for $\#\Pi_{lt,E}(Y)$. More precisely, it is shown that there is an absolute constant $c > 0$ such that for any number $\beta > 0$, the proportion of all elliptic curves $E/\mathbb{Q}$ for which

$$|\#\Pi_{lt,E}(Y) - P(Y)| < \beta \sqrt{P(Y)}$$

is $\geq (1 - \frac{c}{\beta^2})$. Thus, the average size of $\#\Pi_{lt,E}(Y)$ is close to $P(Y)$ for an explicit positive density set of elliptic curves. For instance, setting $\beta = 10\sqrt{\mathcal{E}}$, we find that $\geq 99\%$ of elliptic
curves satisfy the above inequality (1.2). These results shed light on the distribution of primes outside of which the fine Selmer group is finite, when the elliptic curve $E$ in question has Mordell–Weil rank zero.

2 Iwasawa theory of the fine Selmer group

Let $E$ be an elliptic curve defined over $\mathbb{Q}$ and $p$ an odd prime at which $E$ has good reduction. Fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and a finite set of primes $S$ containing $\{p, \infty\}$ outside of which $E$ has good reduction. Let $\mathbb{Q}_S$ be the maximal extension of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ in which all primes $\ell \not\in S$ are unramified. Denote by $E[p^n]$ the $p^n$-torsion subgroup of $E(\mathbb{Q})$, and set $E[p^\infty]$ to be the the union of all $p$-primary torsion groups $E[p^n]$. Given a field $L \subset \mathbb{Q}_S$, set $H^1(\mathbb{Q}_S/L, \cdot) := H^1(\text{Gal}(\mathbb{Q}_S/L, \cdot))$. For a number field $L$ and a prime $\ell \in S$, set $K_\ell(\cdot/L)$ to be the direct sum $\bigoplus_{\nu|\ell} H^1(L_{\nu}, \cdot)$. Here, $\nu$ ranges over the primes of $L$ above $\ell$.

**Definition 2.1** Let $L$ be a number field. The fine Selmer group $R_{p^n}(E/L)$ is defined to be the kernel of the restriction map

$$\ker \left\{ H^1(\mathbb{Q}_S/L, E[p^\infty]) \longrightarrow \bigoplus_{\ell \in S} K_\ell(\text{E}[p^\infty]/L) \right\}.$$ 

We study the fine Selmer group from an Iwasawa theoretic point of view. This involves passing up an infinite tower of number fields. Let $\mathbb{Q}(\mu_{p^n})$ be the field generated by $\mathbb{Q}$ and the $p$-power roots of unity $\mu_{p^n} \subset \bar{\mathbb{Q}}$. For $n \in \mathbb{Z}_{\geq 1}$, let $\mathbb{Q}_n \subset \mathbb{Q}(\mu_{p^n})$ be the extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\mu_{p^n})$ such that $[\mathbb{Q}_n : \mathbb{Q}] = p^n$. The cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ is the union $\mathbb{Q}_{cyc} := \bigcup_{n \geq 1} \mathbb{Q}_n$, with Galois group $\Gamma := \text{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q})$. Fix a topological generator $\gamma \in \Gamma$. This gives rise to an isomorphism $\mathbb{Z}_p \overset{\sim}{\longrightarrow} \Gamma$, sending $a \in \mathbb{Z}_p$ to $\gamma^a$. The Iwasawa algebra is the completed group algebra $\Lambda := \lim_{\leftarrow n} \mathbb{Z}_p[\text{Gal}(\mathbb{Q}_n/\mathbb{Q})]$. Fix an isomorphism of $\Lambda$ with the formal power series ring $\mathbb{Z}_p[[T]]$, where $T$ is the formal variable in place of $(\gamma - 1) \in \Lambda$.

**Definition 2.2** The fine Selmer group over $\mathbb{Q}_{cyc}$ is taken to be the direct limit

$$R_{p^n}(E/\mathbb{Q}_{cyc}) := \lim_{\rightarrow n} R_{p^n}(E/\mathbb{Q}_n)$$

and is a cofinitely generated module over $\Lambda$.

In other words, the Pontryagin dual

$$R_{p^n}(E/\mathbb{Q}_{cyc})^\vee := \text{Hom}_{cts}(R_{p^n}(E/\mathbb{Q}_{cyc}), \mathbb{Q}_p/\mathbb{Z}_p)$$

is finitely generated over $\Lambda$. We refer to [3] for the definition of the $p$-primary Selmer group over $\mathbb{Q}_{cyc}$, which we denote by $\text{Sel}_{p^n}(E/\mathbb{Q}_{cyc})$. Note that the fine Selmer group is a subgroup of $\text{Sel}_{p^n}(E/\mathbb{Q}_{cyc})$. It follows from a deep result of Kato [16] that $\text{Sel}_{p^n}(E/\mathbb{Q}_{cyc})^\vee$ is torsion over $\Lambda$. In particular it follows that $R_{p^n}(E/\mathbb{Q}_{cyc})^\vee$ is torsion over $\Lambda$.

Let $M$ be a cofinitely generated and cotorsion $\Lambda$-module. We introduce the Iwasawa invariants associated to the Pontryagin dual $M^\vee := \text{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. Associated with $M^\vee$ are its Iwasawa invariants. By the Structure Theorem for finitely generated and torsion $\Lambda$-modules [31, Theorem 13.12], $M^\vee$ is pseudo-isomorphic to a finite direct sum of cyclic $\Lambda$-modules. In other words, there is a map of $\Lambda$-modules...
Let $E$ be an elliptic curve and $p$ an odd prime number. Let $F$ be the number field given by $\mathbb{Q}(E[p])$, i.e., the field which is fixed by the kernel of the mod-$p$ representation on $E[p]$. Let $\mu_p(F_{\text{cyc}}/F)$ be the classical Iwasawa $\mu$-invariant associated with the maximal abelian pro-$p$ extension of $F_{\text{cyc}}$ which is unramified at all primes. The classical $\mu = 0$ conjecture of Iwasawa predicts that $\mu_p(K_{\text{cyc}}/K) = 0$ for any number field $K$. The following result due to Coates and the second named author establishes a relationship between the vanishing of the classical $\mu$-invariant and the $\mu$-invariant of the fine Selmer group of $E$ over $F$.

**Theorem 2.3** Let $E$ be an elliptic curve and $p$ an odd prime number. Let $F$ be the number field given by $\mathbb{Q}(E[p])$. Then, the following are equivalent

1. $\mathcal{R}_p^{\infty}(E/F_{\text{cyc}})\vee$ is a torsion $\Lambda$-module with $\mu^{\text{fn}}_p(E/F_{\text{cyc}}) = 0$,
2. $\mu_p(F_{\text{cyc}}/F) = 0$.

**Proof** The statement follows directly from from [4, Theorem 3.4].

One should note that the above result in fact provides us with a criterion for the classical $\mu = 0$ conjecture to hold for number field extensions $F = \mathbb{Q}(E[p])$, which need not be abelian or even solvable. However, instead of studying the vanishing of $\mu^{\text{fn}}_p(E/F_{\text{cyc}})$, we shall study conditions for the vanishing of $\mu^{\text{fn}}_p(E/Q_{\text{cyc}})$. Conjecture A of [4] asserts that $\mu^{\text{fn}}_p(E/Q_{\text{cyc}}) = 0$ for all elliptic curves $E/Q$. The above result shows that it is a special case of the $\mu = 0$ conjecture for number fields.

Now consider for a moment the special case when the residual representation

$$\hat{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\bar{\mathbb{F}}_p)$$

on $E[p]$ is reducible, i.e., $\hat{\rho} = \begin{pmatrix} \varphi_1 & * \\ 0 & \varphi_2 \end{pmatrix}$, for globally defined characters

$$\varphi_i : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \mathbb{F}_p^\times.$$
Proposition 2.4 Let $E_{/\mathbb{Q}}$ be an elliptic curve and $p$ an odd prime such that $\bar{p}$ is reducible, then, $\mu_{p}^{\text{fn}}(E_{\mathbb{Q}_{\text{cyc}}}) = 0$.

Proof Let $\mathbb{Q}(\varphi_{i})$ be the field fixed by the kernel of $\varphi_{i}$ and set $L$ to be the composite of $\mathbb{Q}(\varphi_{1})$ and $\mathbb{Q}(\varphi_{2})$. Note that $\mathbb{Q}(E[p^{\infty}])/L$ is pro-$p$ and since $L$ an abelian number field, by the Theorem of Ferrero and Washington [9], the Iwasawa $\mu = 0$ conjecture holds for $L_{\text{cyc}}/L$. It follows from [4, Corollary 3.5] that in fact, $\mu_{p}^{\text{fn}}(E/L_{\text{cyc}}) = 0$, and it is easy to see that this implies that $\mu_{p}^{\text{fn}}(E_{/\mathbb{Q}_{\text{cyc}}}) = 0$. \hfill $\square$

In contrast, the $\mu$-invariant of the Selmer group $\text{Sel}_{p^{\infty}}(E_{/\mathbb{Q}_{\text{cyc}}})$ is known to be positive in some cases when $\bar{p}$ is reducible. From a statistical point of view, the case of interest is that when $\bar{p}$ is surjective, in particular, irreducible. It follows from Serre’s Open image representation theorem that when $E_{/\mathbb{Q}}$ is an elliptic curve without complex multiplication, the residual Galoisrepresentation is irreducibleforall odd primes $p$. A Serre curve is an elliptic curve whose adelic Galois representation has index-2 in $\text{GL}_{2}(\mathbb{Z})$, see [15] for a more precise definition. Serre curves are of interest since they are the elliptic curves for which the adelic Galois image is as large as possible. It is not hard to see that given a Serre curve, the mod-$p$ Galois representation is irreducible for all odd primes $p$. Jones proves in loc. cit. that 100% of elliptic curves ordered according to height are Serre curves.

Let $f(T)$ be the characteristic element of the fine Selmer group $R_{p^{\infty}}(E_{/\mathbb{Q}_{\text{cyc}}})$, and write $f(T) = a_{r}T^{r} + a_{r+1}T^{r+1} + \ldots$, where $a_{r} \in \mathbb{Z}_{p}$ is non-zero. Here, the number $r$ is called the order of vanishing of $f(T)$ at $T = 0$ and $a_{r}$ is called the leading term. The class of $a_{r}$ modulo $\mathbb{Z}_{p}$ does not depend on the choice of topological generator $\gamma \in \Gamma$. Let $\mathcal{M}(E_{/\mathbb{Q}})$ be the subgroup of elements of $R_{p^{\infty}}(E_{/\mathbb{Q}})$ that lie in the image of the Kummer map

$$E(\mathbb{Q}) \otimes \mathbb{Q}_{p}/\mathbb{Z}_{p} \to H^{1}(\mathbb{Q}_{S}/\mathbb{Q}, E[p^{\infty}]),$$

and the fine Tate-Shafarevich group $\mathcal{X}E_{p^{\infty}}(E_{/\mathbb{Q}})$ is the cokernel of

$$\mathcal{M}(E_{/\mathbb{Q}}) \to R_{p^{\infty}}(E_{/\mathbb{Q}}).$$

Then, $\mathcal{X}E_{p^{\infty}}(E_{/\mathbb{Q}})$ is naturally identified with a subgroup of $\text{III}(E/K)[p^{\infty}]$. In our applications, we would like to understand when $\mathcal{X}E_{p^{\infty}}(E_{/\mathbb{Q}})$ is non-zero. The following result shows that the fine Tate-Shafarevich group vanishes precisely when the $p$-primary part of the Tate-Shafarevich group does.

Theorem 2.5 (Wuthrich) Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Then, $\mathcal{X}E_{p^{\infty}}(E_{/\mathbb{Q}}) \neq 0$ precisely when $\text{III}(E_{/\mathbb{Q}})[p^{\infty}] \neq 0$. Furthermore, if rank $E(\mathbb{Q}) > 0$, then, $\mathcal{X}E_{p^{\infty}}(E_{/\mathbb{Q}}) = \text{III}(E_{/\mathbb{Q}})[p^{\infty}]$.

Proof See [33, Theorems 3.4, 3.5]. \hfill $\square$

When rank $E(\mathbb{Q}) = 0$, $\mathcal{X}E_{p^{\infty}}(E_{/\mathbb{Q}})$ may be strictly smaller than $\text{III}(E_{/\mathbb{Q}})[p^{\infty}]$, as numerical examples in [33] show.

Wuthrich gives an explicit formula for the leading term of the characteristic element $a_{r}$, see [34, Corollary 6.2]. We let $D = D_{E,p}$ be the cokernel of the natural map $E(\mathbb{Q}) \otimes \mathbb{Z}_{p}$ to the $p$-adic completion of $E(\mathbb{Q}_{p})$. At a prime $\ell$ at which $E$ has bad reduction, $c_{\ell}(E)$ will denote the Tamagawa number at $\ell$. Given two numbers $a$, $b$, we write $a \sim b$ if $a = ub$ for some unit $u \in \mathbb{Z}_{p}^{\times}$. There is a $p$-adic height pairing on the Selmer group $R_{p^{\infty}}(E_{/\mathbb{Q}})$, see [34, section 5]. The regulator $\text{Reg} (R_{p^{\infty}}(E_{/\mathbb{Q}}))$ is the determinant of this height pairing.
The compact version of the fine Selmer group $\mathcal{R}_p^\infty(E/\mathbb{Q})$ is the kernel of the localization map

$$\mathcal{R}_p^\infty(E/\mathbb{Q}) := \ker \left( H^1(\mathbb{Q}_S/\mathbb{Q}, T_p(E)) \to H^1(\mathbb{Q}_p, T_p(E)) \right).$$

Here, $T_p(E)$ denotes the $p$-adic Tate-module associated to $E$.

**Theorem 2.6** (Wuthrich) Let $E$ be an elliptic curve over $\mathbb{Q}$ with potentially good reduction at $p$. Assume that the following conditions are satisfied:

(a) The fine Tate-Shafarevich group $\mathcal{A}E_p^\infty(E/\mathbb{Q})$ is finite.

(b) The cyclotomic height pairing on $\mathcal{R}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is nondegenerate.

Then, the following assertions hold

1. $r = \max(0, \text{rank } E(\mathbb{Q}) - 1)$.
2. There is an injection with finite cokernel $J$ of $\mathcal{R}_p^\infty(E/\mathbb{Q})$ into the cokernel of the corestriction map
   $$\text{cor} : \lim_{\leftarrow n} H^1(\mathbb{Q}_S/\mathbb{Q}_n, T_p(E)) \to H^1(\mathbb{Q}_S/\mathbb{Q}, T_p(E)).$$
3. We have the following formula for the leading term $a_r$
   $$a_r \sim \text{Reg} \left( \mathcal{R}_p^\infty(E/\mathbb{Q}) \right) \times \left( \frac{\# \text{Tors}_{\mathbb{Z}_p}(D) \times \prod_{\ell \neq p} c_\ell(E) \times \# \mathcal{A}E_p^\infty(E/\mathbb{Q})}{\# J} \right).$$

(2.2)

where, $\text{Tors}_{\mathbb{Z}_p}(D)$ denotes the $p$-primary torsion subgroup of $D$.

**Proof** The above result is [33, Theorem 1.1].

Note that under the assumptions of the above theorem, $r = 0$ and the regulator $\text{Reg} \left( \mathcal{R}_p^\infty(E/\mathbb{Q}) \right) = 1$ when $\text{rank } E(\mathbb{Q}) \leq 1$. As a result of the above formula, we obtain an important consequence towards the vanishing of the Iwasawa invariants of the fine Selmer group $\mathcal{R}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$.

**Corollary 2.7** Let $E$ be an elliptic curve over $\mathbb{Q}$ and $p$ an odd prime. Assume that $E$ has potentially good reduction at $p$ and satisfied the conditions of Theorem 2.6. Furthermore, assume that the following conditions hold:

1. $\text{rank } E(\mathbb{Q}) \leq 1$,
2. $p \nmid c_\ell(E)$ for all primes $\ell \neq p$,
3. $\mathcal{A}E_p^\infty(E/\mathbb{Q}) = 0$,
4. $\text{Tors}_{\mathbb{Z}_p}(D) = 0$.

Then, the $\mu$ and $\lambda$-invariants of the fine Selmer group $\mathcal{R}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ are 0. In particular, $\mathcal{R}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ has finite cardinality.

**Proof** It follows from Theorem 2.6 that $r = 0$. Furthermore, the regulator

$$\text{Reg} \left( \mathcal{R}_p^\infty(E/\mathbb{Q}) \right) = 1.$$

Furthermore, the conditions imply that $a_0 = 1$, hence the characteristic element of $\mathcal{R}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is a unit in $\Lambda$. The result follows from this.

$\Box$
The above result has an interesting consequence from a statistical point of view. Let us first introduce some notation. Given \( x > 0 \), recall that \( \pi(x) \) is the number of primes \( p \leq x \) and that the prime number theorem states that \( \pi(x) \sim \frac{x}{\log(x)} \), i.e.,

\[
\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1.
\]

Given a set of primes \( S \), set \( S(x) := \{ p \in S \mid p \leq x \} \), note that \( |S(x)| \leq \pi(x) \) by definition.

**Definition 2.8** Let \( \beta \in [0, 1] \) and \( S \) be a set of prime numbers. We say that \( S \) has density \( \beta \) if

\[
\lim_{x \to \infty} \frac{|S(x)|}{\pi(x)} = \beta.
\]

Note that part of the requirement is that the limit actually exists.

Thus, if the set \( S \) has density 1, we say that \( S \) consists of 100% of primes. If the complement of \( S \) in the set of all primes is finite, then indeed, \( S \) consists of 100% of primes, however, not conversely. Given an elliptic curve \( E/\mathbb{Q} \), let \( \Pi_{l,E} \) be the set of local torsion primes for \( E \), i.e., the set of all primes \( p \) such that \( E \) has good reduction at \( p \) and \( E(\mathbb{Q}_p) \) contains a \( p \)-torsion point. Let \( \Pi_{an,E} \) be the set of anomalous primes, i.e., primes \( p \) at which \( E \) has good reduction such that \( \tilde{E}(\mathbb{F}_p)[p] \neq 0 \). Here, \( \tilde{E} \) is the reduction of \( E \) at \( p \). Let \( \Pi_E \) be the set of primes \( p \) at which \( E \) has good reduction such that \( \text{Tors}_{\mathbb{Z}_p} D \neq 0 \).

**Proposition 2.9** Let \( E \) be an elliptic curve over \( \mathbb{Q} \), then, \( \Pi_{l,E} \subseteq \Pi_{an,E} \). Furthermore, if \( \text{rank}(E(\mathbb{Q})) = 0 \), then, \( \Pi_E \subseteq \Pi_{l,E} \).

**Proof** Let \( E \) have good reduction at \( p \), in other words, \( E \) can be viewed as an elliptic curve over \( \text{Spec} \mathbb{Z}_p \). Letting \( E_0 \) be the formal group of \( E \), we have a short exact sequence

\[
0 \to E_0(p\mathbb{Z}_p) \to E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p) \to 0.
\]

Note that \( E_0(p\mathbb{Z}_p) \simeq \mathbb{Z}_p \) does not contain any \( p \)-torsion, and therefore, there is an injection \( E(\mathbb{Q}_p)[p^\infty] \to \tilde{E}(\mathbb{F}_p)[p^\infty] \). This shows that if \( p \) is a local torsion prime, then \( p \) is an anomalous prime, i.e., \( \Pi_{l,E} \subset \Pi_{an,E} \). On the other hand, when \( \text{rank}(E(\mathbb{Q})) = 0 \) and \( E(\mathbb{Q}_p) \) has no nontrivial \( p \)-torsion, it follows that \( \text{Tors}_{\mathbb{Z}_p} D = 0 \). Therefore, \( \Pi_E \subseteq \Pi_{l,E} \), when the Mordell–Weil rank of \( E \) is 0. \( \square \)

**Corollary 2.10** Let \( E \) be a non-\( \text{CM} \) elliptic curve over \( \mathbb{Q} \) with \( \text{rank}(E(\mathbb{Q})) = 0 \) for which the Tate-Shafarevich group \( \text{III}(E/\mathbb{Q}) \) is finite. Then, for 100% of primes \( p \),

\[
\mu_p^{fn}(E/\mathbb{Q}_{\text{cyc}}) = 0 \quad \text{and} \quad \lambda_p^{fn}(E/\mathbb{Q}_{\text{cyc}}) = 0.
\]

The set of primes for which \( \mu_p^{fn}(E/\mathbb{Q}_{\text{cyc}}) > 0 \) or \( \lambda_p^{fn}(E/\mathbb{Q}_{\text{cyc}}) > 0 \) is contained in the set \( \Pi_{l,E} \cup \mathcal{S} \), where \( \mathcal{S} \) is the set of primes dividing \( 2\text{#III}(E/\mathbb{Q}) \times \prod_{e \neq p} c_e(E) \).

**Proof** Since it is assumed that \( \text{III}(E/\mathbb{Q}) \) is finite, it follows that \( \lambda E_{\mathbb{Q}_{\text{cyc}}} E/\mathbb{Q} = 0 \) for all but finitely many primes. It is also clear (from the fact that \( c_\ell(E) \) is a non-zero integer) that \( \prod_{e \neq p} c_e(E) \) is a unit in \( \mathbb{Z}_p \) for all but finitely many primes \( p \). It is well known that \( \Pi_{an,E} \) has density zero, see [23]. Since it is assumed that \( \text{rank}(E(\mathbb{Q})) = 0 \), Proposition 2.9 asserts that \( \Pi_E \subseteq \Pi_{an,E} \), and hence \( \Pi_E \) has density zero. Therefore, we have shown that the conditions of Corollary 2.7 hold for 100% of primes \( p \). \( \square \)
3 Statistics for local torsion primes

Let \( E/\mathbb{Q} \) be an elliptic curve. We recall that a prime \( p \) at which \( E \) has good reduction is said to be anomalous if \( p \mid \#\tilde{E}(\mathbb{F}_p) \). Given an elliptic curve \( E, \Pi_{an,E} \) is the set of anomalous primes for \( E \). The following result is due to Greenberg, see [11, Theorems 4.1 and 5.1].

**Theorem 3.1** (Greenberg) Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without complex multiplication such that \( \text{rank } E(\mathbb{Q}) = 0 \) and \( \Pi(E/\mathbb{Q}) \) is finite. Then, for 100\% of primes \( p \), the \( p \)-primary Selmer group \( \text{Sel}_p(E/\mathbb{Q}_{cyc}) \) has \( \mu = 0 \) and \( \lambda = 0 \). The set of primes \( p \) at which either \( \mu > 0 \) or \( \lambda > 0 \) is contained in \( \Pi_{an,E} \cup \mathcal{S} \), where \( \mathcal{S} \) is the finite set of primes dividing \( 2\#\Pi(E/\mathbb{Q}) \prod_{\ell \neq p} e_\ell(E) \). Furthermore, the set of primes at which \( \mu > 0 \) or \( \lambda > 0 \) is infinite if and only if \( \Pi_{an,E} \) is infinite.

Recall that for \( x > 0 \), the set \( \Pi_{an,E}(x) \) is the subset of \( \Pi_{an,E} \) consisting of primes \( p \leq x \). There are results about the asymptotic growth of \( \#\Pi_{an,E}(x) \) as a function in \( x \). The conjecture of Lang and Trotter [21] predicts that there is a constant \( C \geq 0 \) (depending on \( E \) and independent of \( p \)) such that

\[
\#\Pi_{an,E}(x) \sim C \frac{x^{\sqrt{2}}}{\log x}.
\]

This is only conjectural, in fact, the best known upper bound, due to V. K. Murty (see [23]) asserts that

\[
\#\Pi_{an,E}(x) \ll \frac{x (\log \log x)^2}{(\log x)^2}.
\]

In (3.1), the constant \( C \) may actually be 0, and there are examples of elliptic curves \( E \) such that the entire set of anomalous primes \( \Pi_{an,E} \) is finite. Such elliptic curves are known as finitely anomalous curves, and were studied by Ridgdill in her thesis [26].

In studying the fine Selmer group, anomalous primes no longer play a role since \( \tilde{E}(\mathbb{F}_p) \) is not a term in the Euler characteristic formula for the leading term of the characteristic element. Instead we turn our attention to local torsion primes. Let \( E \) be an elliptic curve over \( \mathbb{Q} \), and \( p \) a prime number. Recall that

\[
D = D(E, p) := \text{cok} \left( E(\mathbb{Q}) \otimes \mathbb{Z}_p \rightarrow E(\mathbb{Q}_p) \right),
\]

where \( E(\mathbb{Q}_p) \) is the \( p \)-adic completion of \( E(\mathbb{Q}) \). The torsion subgroup \( \text{Tors}_{\mathbb{Z}_p} D \) features in the numerator of (2.2). The following conjecture on the distribution of local torsion primes is supported by heuristics.

**Conjecture 3.2** (David-Weston) Let \( E \) be an elliptic curve over \( \mathbb{Q} \) without complex-multiplication. Then, the set of local torsion primes is finite.

The following heuristic is taken from [8, p.1]. Suppose \( p \) is a local torsion prime, i.e., \( E(\mathbb{Q}_p)[p] \neq 0 \) such that \( E \) has good reduction at \( p \). This in particular implies that \( E(\mathbb{F}_p)[p] \neq 0 \). If \( p \geq 7 \), then it follows from the Weil bound that \( a_p(E) = 1 \). On the other hand, \( a_p(E) = 1 \) occurs with probability \( \frac{1}{\sqrt{p}} \). Given an elliptic curve \( \tilde{E} \) over \( \mathbb{F}_p \) satisfying some additional conditions, 1 out of every \( p \) lifts \( E \) of \( \tilde{E} \) to \( \mathbb{Z}_p \) has a local torsion point, see [8, Corollary 3.5]. The sum \( \sum_n \frac{1}{\sqrt{p^n}} = \frac{1}{2} \sum_p p^{-3/2} \) is finite.

On the other hand, Conjecture 1.2 in [34] states that the fine Selmer group \( \mathcal{R}_{p,\infty}(E/\mathbb{Q}_{cyc}) \) associated to an elliptic curve with rank \( E(\mathbb{Q}) \leq 1 \) is finite for all but finitely many primes.
p. More generally, the $\mathbb{Z}_p$-corank of $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is expected to be equal to the $\mathbb{Z}_p$-corank of $R_p^\infty(E/\mathbb{Q})$ for all but finitely many primes $p$. We state the conjecture slightly differently from its original formulation.

**Conjecture 3.3** (Wuthrich) Let $E$ be an elliptic curve over $\mathbb{Q}$, then for all but finitely many primes $p$ of good reduction, the fine Selmer group $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ satisfies $\mu_p = 0$ and $\lambda_p = \max(\text{rank } E(\mathbb{Q}) - 1, 0)$.

We specialize to the case when $\text{rank } E(\mathbb{Q}) = 0$ to obtain the following easy observation.

**Proposition 3.4** Suppose that $E$ is an elliptic curve over $\mathbb{Q}$ with $\text{rank } E(\mathbb{Q}) = 0$. Assume that the following conditions are satisfied:

1. $E$ does not have complex multiplication,
2. Conjecture 3.2 holds for $E$,
3. $\text{III}(E/\mathbb{Q})$ is finite.

Then, Conjecture 3.3 holds for $E$.

**Proof** Note that $\text{Reg}(R_p^\infty(E/\mathbb{Q})) = 1$ since $\text{rank } E(\mathbb{Q}) = 0$. The conditions of Theorem 2.6 are satisfied. Since $\text{rank } E(\mathbb{Q}) = 0$, the order of vanishing of $f(T) = \text{char}(R_p^\infty(E/\mathbb{Q}_{\text{cyc}}))$ at $T = 0$ is 0. We appeal to Wuthrich’s formula (2.2) for the leading term $a_0$. Note that $a_0$ is a unit in $\mathbb{Z}_p$ if and only if $\mu_p^\text{fn}(E/\mathbb{Q}_{\text{cyc}}) = 0$ and $\lambda_p^\text{fn}(E/\mathbb{Q}_{\text{cyc}}) = 0$.

Conjecture 3.3 in this context states that $a_0 = a_0(E, p)$ is a $p$-adic unit for all but finitely many primes $p$. By Corollary 2.10, $a_0$ is a $p$-adic unit if an only if

1. $p \nmid c_\ell(E)$ for all primes $\ell \neq p$,
2. $\mathcal{K}_E p^\infty(E/\mathbb{Q}) = 0$,
3. $\text{Tors}_{\mathbb{Z}_p}(D) = 0$.

Theorem 2.5 implies that $\mathcal{K}_E p^\infty(E/\mathbb{Q}) = 0$ if and only if $\text{III}(E/\mathbb{Q})[p^\infty] = 0$. There are only finitely many primes $p$ which divide the Tamagawa product. Since it is assumed that $\text{III}(E/\mathbb{Q})$ is finite, it follows that $\mathcal{K}_E p^\infty(E/\mathbb{Q}) = 0$ for all but finitely many primes. If the set of local torsion primes is finite, then $\text{Tors}_{\mathbb{Z}_p}(D) = 0$ for all but finitely many primes $p$.

As a result, the above conditions imply that Conjecture 3.3 holds for $E$. $\square$

Let $E$ be an elliptic curve over $\mathbb{Q}$ with good reduction at $p$, in other words, $E/\mathbb{Q}_p$ admits a smooth local model $\mathcal{E}/\mathbb{Z}_p$. Given a finitely generated abelian group $M$, we set $\text{rank}_p M := \dim(M \otimes \mathbb{F}_p)$ to be the $p$-rank of $M$.

**Lemma 3.5** Let $E$ be an elliptic curve over $\mathbb{Z}_p$, then,

$$\text{rank}_p (\mathcal{E}(\mathbb{Z}/p^2\mathbb{Z})) = \begin{cases} 1 & \text{if } \mathbb{Q}(\mathbb{Q}_p)[p] = 0; \\ 2 & \text{if } \mathbb{Q}(\mathbb{Q}_p)[p] \neq 0. \end{cases}$$

**Proof** The assertion is a special case of [8, Lemma 3.1]. $\square$

Given a pair $(a, b)$, we let $E_{a,b}$ be the elliptic curve defined by $y^2 = x^3 + ax + b$.

**Proposition 3.6** Let $E_{a,b}$ be an elliptic curve associated to a pair $(a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ and such that the $j$-invariant $j(E_{a,b}) \neq 0, 1728$. Then, there are $p$ distinct pairs $(A_i, B_i) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ such that $(A_i, B_i) \equiv (a, b) \mod p$ and
The group $SL_2(\mathbb{Z})$.

Given that since $\varphi \rightarrow y$ implies $\varphi \rightarrow y$.

Consider the special case when $\#E \in \mathbb{Z}$.

See [8, Proposition 3.4] for a proof of the result.

**Proof.**

**Definition 3.7** Let $\mathcal{S}_p$ be the subset of $\mathbb{F}_p \times \mathbb{F}_p$ consisting of all pairs $(a, b)$ such that

$$\Delta_{a,b} \neq 0 \text{ and } E_{a,b}(\mathbb{F}_p)[p] \neq 0.$$  

Let $\mathcal{S}_p'$ be the subset of $\mathcal{S}_p$ consisting of pairs $(a, b)$ such that $j(E_{a,b}) = j$. Set $\mathcal{A}_p$ be the set of pairs $(A, B) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ such that

$$p \nmid \Delta_{A,B} \text{ and } \text{rank}_p (E_{A,B}(\mathbb{Z}/p^2)) = 2.$$  

Given $j \in \mathbb{F}_p$, let $\mathcal{A}_p \subseteq \mathcal{A}_p$ consist of the pairs for which $j(E_{A,B}) \equiv j \mod p$.

We would like to estimate $\#\mathcal{S}_p$ and $\#\mathcal{A}_p$. Note that by definition $\mathcal{A}_p$ reduces mod-$p$ to $\mathcal{S}_p$, and by Proposition 3.6, the fibers of the reduction map $\mathcal{S}_p \rightarrow \mathcal{S}_p' \rightarrow \mathcal{S}_p$ have order $p$ provided $j \neq 0, 1728$. The quantity $\#\mathcal{S}_p$ can be expressed in terms of Hurwitz class numbers associated to integral binary quadratic forms with fixed discriminant.

We follow the notation and conventions of [29, section 2]. Let $\Delta \in \mathbb{Z}_{>0}$ with $\Delta \equiv 0, 1 \mod 4$, and set

$$B(\Delta) := \{ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y] \mid a > 0, b^2 - 4ac = \Delta\}.$$  

The group $SL_2(\mathbb{Z})$ acts on $\mathbb{Z}[x,y]$, where a matrix $\sigma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ sends $x \mapsto (px + qy)$ and $y \mapsto (rx + sy)$. Thus, if $f = ax^2 + bxy + cy^2$, the matrix $\sigma$ acts by

$$f \circ \sigma = a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2.$$  

It can be checked that $B(\Delta)$ is stable under the action of $SL_2(\mathbb{Z})$ and $B(\Delta)/SL_2(\mathbb{Z})$ is finite, see *loc. cit.* for additional details.

**Definition 3.8** The *Hurwitz class number* $H(\Delta)$ is the order of $B(\Delta)/SL_2(\mathbb{Z})$.

Given an elliptic curve $E_{f_p}$, the Frobenius element $\varphi \in \text{End}(E)$ satisfies the equation $\varphi^2 - t\varphi + p = 0$. Here, $t$ is an integer given by $\#E(\mathbb{F}_p) = p + 1 - t$. According to the well-known Hurwitz bound, we have that $|t| \leq 2\sqrt{p}$. Note that $p$ divides $t$ if and only if $E$ is supersingular.

**Definition 3.9** (cf. [29, Definition 4.1]) Two elliptic curves $E$ and $E'$ over $\mathbb{F}_p$ are *isogenous* over $\mathbb{F}_p$ if

$$\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p).$$  

Let $I(t)$ be the isogeny class of elliptic curves over $\mathbb{F}_p$ with $\#E(\mathbb{F}_p) = p + 1 - t$. Let $N(t)$ denote the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves in $I(t)$.

Consider the special case when $\#E(\mathbb{F}_p)$ is divisible by $p$, in other words, $t \equiv 1 \mod p$. Note that since $|t| \leq 2\sqrt{p}$, it follows that if $p \geq 7$, then, $E(\mathbb{F}_p)$ contains a non-zero $p$-torsion point precisely when $t = 1$. However, if $p \leq 5$, then the two possibilities are $t = -p + 1$, in which case, $\#E(\mathbb{F}_p) = 2p$, and $t = 1$, i.e., $\#E(\mathbb{F}_p) = p$. 

\[\text{rank}_p E_{A_i,B_i}(\mathbb{Z}/p^2) = 2.\]
Let $\hat{S}_p$ be the set of isomorphism classes of elliptic curves $E$ over $\mathbb{F}_p$ such that $E(\mathbb{F}_p)[p] \neq 0$. Thus, we have that

$$\# \hat{S}_p = \begin{cases} N(1) & \text{for } p \geq 7, \\ N(-p + 1) + N(1) & \text{for } p \leq 5. \end{cases}$$

Waterhouse showed that the number of elliptic curves in a given isogeny class can be computed in terms of certain class numbers, see [32]. These results were later reformulated in terms of Hurwitz class numbers by Schoof.

**Theorem 3.10** (Waterhouse, Schoof) Let $t$ be an integer such that $p \nmid t$ and $t^2 < 4p$, then, $N(t) = H(t^2 - 4p)$.

**Proof** The reader is referred to [29, Theorem 4.6] for a proof of the result.

**Corollary 3.11** Let $p$ be a prime and let $\hat{S}_p$ be as above. Then, we have that

$$\# \hat{S}_p = \begin{cases} H(1 - 4p) & \text{for } p \geq 7, \\ H(p^2 + 1 - 6p) + H(1 - 4p) & \text{for } p \leq 5. \end{cases}$$

**Proof** From the discussion above Theorem 3.10,

$$\# \hat{S}_p = \begin{cases} N(1) & \text{for } p \geq 7, \\ N(-p + 1) + N(1) & \text{for } p \leq 5. \end{cases}$$

The result then follows from Theorem 3.10.

**Proposition 3.12** Let $p$ be any prime and $S_p$ be as above. Then, we have that

$$\# S_p \leq \left( \frac{p-1}{2} \right) \left( z_p H(p^2 + 1 - 6p) + H(1 - 4p) \right) < Cp^{3/2} \log p (\log \log p)^2,$$

where $C > 0$ is an effective constant (independent of $p$) and $z_p = \begin{cases} 1 & \text{if } p \leq 5, \\ 0 & \text{if } p \geq 7. \end{cases}$

**Proof** The elliptic curves $E_{a,b}$ and $E_{a',b'}$ are isomorphic over $\mathbb{F}_p$ if there exists $c \in \mathbb{F}_p^\times$ such that

$$a' = c^4 a \text{ and } b' = c^6 b.$$ 

Therefore, the number of elliptic curves $E_{a',b'}$ isomorphic to a given elliptic curve $E_{a,b}$ is at most $\left( \frac{p-1}{2} \right)$. Therefore, we have that

$$\# S_p \leq \left( \frac{p-1}{2} \right) \# \hat{S}_p < Cp^{3/2} \log p (\log \log p)^2,$$

where the first inequality is the assertion of Corollary 3.11, and the second follows from a well known bound on Hurwitz numbers [20, Proposition 1.8].

**Corollary 3.13** For $\mathfrak{A}_p$ be as in Definition 3.7, we have that

$$\frac{\mathfrak{A}_p}{p^2} < \frac{2}{p} + Cp^{-3/2} \log p (\log \log p)^2,$$

where $C > 0$ is an effective constant.
Proof. We subdivide $\mathfrak A_p$ into two disjoint sets $\mathfrak A_p^{(1)}$ and $\mathfrak A_p^{(2)}$. Set $\mathfrak A_p^{(1)} := \mathfrak A_p^0 \cup \mathfrak A_p^{1728}$, i.e., the pairs $(A, B) \in \mathfrak A_p$ such that the $j$-invariant is either $0$ or $1728$ modulo $p$. Note that $\mathfrak A_p^{(1)}$ consists of all pairs $(A, B) \in \mathfrak A_p$ such that $p \mid AB$. Clearly, the number of pairs $(A, B)$ such that $p \mid A$ is $p^3$. Thus we have the following obvious upper bound:

$$\#\mathfrak A_p^{(1)} < 2p^3. \quad (3.3)$$

Let $\mathfrak A_p^{(2)}$ be the complement of $\mathfrak A_p^{(1)}$ in $\mathfrak A_p$. For any pair $(A, B) \in \mathfrak A_p^{(2)}$, we have by construction that $j(E_{A,B}) \not\equiv 0, 1728 \mod p$. Proposition 3.6 asserts that given a pair $(a, b) \in \mathfrak S_p$ with $j$-invariant not equal to 0 or 1728, there are $p$ lifts $(A, B) \in \mathfrak A_p$ of $(a, b)$. Therefore, we have the following upper bound: $\#\mathfrak A_p^{(2)} < p\#\mathfrak S_p$. Invoking Proposition 3.12, we obtain the following bound:

$$\#\mathfrak A_p^{(2)} < Cp^{5/2} \log p(\log\log p)^2. \quad (3.4)$$

Putting together (3.3) and (3.4), we obtain

$$\frac{\#\mathfrak A_p}{p^4} = \frac{\#\mathfrak A_p^{(1)}}{p^4} + \frac{\#\mathfrak A_p^{(2)}}{p^4} < \frac{2}{p} + Cp^{-3/2} \log p(\log\log p)^2.$$

\[\square\]

Remark 3.14 In the proof of the above result, we have invoked the obvious upper bound for $\#\mathfrak A_p^{(1)}$, which contributes to the term $\frac{2}{p}$ in the estimate (3.2). Given a pair $(A, B)$ such that $p \mid AB$, note that the pair $(A, B)$ is contained in $\mathfrak A_p^{(1)}$ precisely when $(\bar A, \bar B) = (A, B) \mod p$ is contained in $\mathfrak S_p$. Let $\mathfrak S_p^*$ be the subset of $\mathfrak S_p$ consisting of all pairs $(a, b)$ such that either $a$ or $b$ is $0$. In the above proof, we have used the obvious bound $\#\mathfrak S_p^* < 2p$ to obtain that

$$\#\mathfrak A_p^{(1)} \leq p^2\#\mathfrak S_p^* < 2p^3.$$ 

The main term $2/p$ in the estimate (3.2) can be replaced by $\#\mathfrak S_p^*/p^2$. Thus, a better understanding of $\#\mathfrak S_p^*$ would potentially give a better estimate.

4 Results for a fixed prime and varying elliptic curve

Let $E/\mathbb Q$ be an elliptic curve. Note that $E$ is defined by a Weierstrass equation $E : y^2 = x^3 + ax + b$, where the integers $a$ and $b$ such that for all primes $\ell$, $\ell^6 \mid b$ whenever $\ell^4 \mid a$. Such a Weierstrass equation is unique and referred to as the minimal Weierstrass equation. The naive height of $E$ is defined to be the quantity $H(E) := \max \{|a|^3, b^2\}$.

Definition 4.1 Let $E$ be the set of isomorphism classes of elliptic curves defined over $\mathbb Q$. Given a subset $\mathcal S$ of $\mathcal E$, and $x > 0$, we set

$$\mathcal S_{<x} := \{E \in \mathcal S \mid H(E) < x\},$$

and $\delta(S, x) := \frac{\#\mathcal S_{<x}}{x}$. We say that $\mathcal S$ has upper (resp. lower) density $\delta$ if $\limsup_{x \to \infty} \delta(S, x) = \delta$ (resp. $\liminf_{x \to \infty} \delta(S, x) = \delta$). If

$$\lim_{x \to \infty} \delta(S, x) = \delta,$$

then, we say that $\mathcal S$ has density $\delta$. Part of the requirement here is that the above limit exists. We let $\delta(S)$ (resp. $\delta(S)$) be the upper (resp. lower) density of $\mathcal S$. The density is denoted
Note that when $\vartheta(S)$ is defined, so are $\bar{\vartheta}(S)$ and $\hat{\vartheta}(S)$, and

$$\vartheta(S) = \bar{\vartheta}(S) = \hat{\vartheta}(S).$$

The conjecture on rank distribution by Katz and Sarnak [19] predicts that when ordered by height, 50% of elliptic curves have rank 0, the other 50% of rank 1 and 0% of rank $> 1$. In other words, let $E^0$, $E^1$, and $E^{>1}$ be the subset of elliptic curves of rank 0, 1, and $> 1$ respectively. Then, the conjecture predicts that $\vartheta(E^0) = \vartheta(E^1) = \frac{1}{2}$ and $\vartheta(E^{>1}) = 0$.

Certain unconditional results have been proven by Bhargava and Shankar who study the average size of the the $p$-Selmer group $\text{Sel}_p(E/\mathbb{Q})$. This is the $p$-torsion subgroup of the $p$-primary Selmer group $\text{Sel}_p^\infty(E/\mathbb{Q})$. For instance, in the preprint [2], it is shown that the average size of the 5-Selmer group is 6 as $E$ varies over $E$. This result implies that $\vartheta(E^0) \geq \frac{1}{5}$ and $\vartheta(E^{>1}) \leq \frac{1}{5}$.

In this section, we fix a prime number $p \geq 5$ and study the following question.

**Question 4.2** As $E$ varies over all elliptic curves defined over $\mathbb{Q}$, what can be said about the proportion of elliptic curves $E$ for which the following equivalent conditions satisfied:

1. $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ has finite cardinality.
2. The $\mu$ and $\lambda$-invariants of $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ are both equal to 0.
3. The leading term $f(0)$ of the characteristic element $f(T)$ of $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is a unit in $\mathbb{Z}_p$.

Note that when the Selmer group $\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is finite, it is in fact equal to 0, see [17, Corollary 3.6]. This is only possible when the Mordell–Weil rank of $E$ is 0 and $E$ has ordinary reduction at $p$ (for further details, the reader may refer to [17, section 4]). Since the fine Selmer group is a subgroup of the Selmer group, it follows that if $\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}}) = 0$, then so is $R_p^\infty(E/\mathbb{Q}_{\text{cyc}}) = 0$. However, it is indeed possible for the fine Selmer group $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ to be finite, while the entire Selmer group $\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is infinite. As the following example shows, this may be so even in the special case when the elliptic curve $E$ has Mordell–Weil rank 0 and good ordinary reduction at $p$.

**Example 4.3** We refer to [34, section 9.1], consider the elliptic curve

$$E : y^2 + y = x^3 - x^2 - 10x - 20,$$

and consider the prime $p = 5$. The $\mu$-invariant of the Selmer group $\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is 1, in fact,

$$\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}})^\vee = \Lambda/p.$$

On the other hand, $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is finite and non-zero. In particular, the $\mu$ and $\lambda$-invariants of the fine Selmer group are zero, however, $R_p^\infty(E/\mathbb{Q}_{\text{cyc}}) \neq 0$.

More generally, if $R_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ is finite and non-zero at a prime of good ordinary reduction, then the Selmer group $\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ must be infinite, since otherwise it would be zero.

**4.1 Statistics for the Selmer group**

Before we proceed to prove results for the fine Selmer group, let us briefly recall the statistical results for the Selmer group $\text{Sel}_p^\infty(E/\mathbb{Q}_{\text{cyc}})$ proved by Kundu and the first
named author in [17, section 4]. Some of these results may be marginally refined using [25, Lemma 6.4]. In this subsection, we summarize the results from these sources. Let \( \mathfrak{S}_p \) be the the set of elliptic curves \( E \in \mathcal{E} \), such that

1. \( \text{rank } E(\mathbb{Q}) = 0 \),
2. \( E \) has good ordinary reduction at \( p \),
3. \( \text{Sel}_{p}\mathbb{Q}(E/\mathbb{Q}_{cyc}) \neq 0 \).

Let \( S_p \) be the set of elliptic curves \( E/\mathbb{Q} \) such that \( \text{III}(E/\mathbb{Q}[p^\infty]) \neq 0 \). A conjecture of Delaunay [6] predicts that \( \delta(S_p) = 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{2i-1}} \right) \). The heuristics supporting this conjecture have been further refined by Poonen and Rains, see [24].

**Conjecture 4.4** (Del-p) The proportion of all elliptic curves such that \( E \) for which \( p \mid \text{III}(E/\mathbb{Q}) \) is given by

\[
\left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{2i-1}} \right) \right).
\]

In preparation of the next result, recall the definition of the set \( \mathfrak{S}_p \) from Definition 3.7.

**Theorem 4.5** (Kundu & R.) Let \( p \geq 5 \) be a prime number and \( \mathfrak{S}_p \) be defined as above. Assume \( \text{III}(E/\mathbb{Q}[p^\infty]) \) is finite for all elliptic curves \( E/\mathbb{Q} \) and that the conjecture (Del-p) is satisfied. Then, there is an effective constant \( C_1 > 0 \) such that the following bounds are satisfied:

\[
\delta(\mathfrak{S}_p) \leq \left( 10 \right) \frac{\#\mathfrak{S}_p}{p^2} + \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{2i-1}} \right) \right) + (\zeta(p) - 1),
\]

\[
< C_1 \frac{\log p (\log \log p)^2}{\sqrt{p}} + \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{2i-1}} \right) \right) + (\zeta(p) - 1). \tag{4.1}
\]

Moreover, the effective constant \( C_1 \) can be taken to be \( \zeta(10)C \), where \( C \) is the constant from Proposition 3.12.

**Proof** The result is essentially a rephrasing of [17, Theorem 4.3], however, thanks to the minor update in the statement taken from [25], and for the convenience of the reader, we summarize the proof here. Let \( E \) be an elliptic curve with good ordinary reduction at \( p \), and \( f(T) \) be the characteristic element of \( \text{Sel}_{p}\mathbb{Q}(E/\mathbb{Q}_{cyc})' \). Express \( f(T) \) as a power series. Suppose that \( E \in \mathfrak{S}_p \), then, in particular, \( E \) has good ordinary reduction at \( p \) and \( \text{rank } E(\mathbb{Q}) = 0 \). On the other hand, it is assumed that \( \text{III}(E/\mathbb{Q}[p^\infty]) \) is finite, and therefore the Selmer group \( \text{Sel}_{p}\mathbb{Q}(E/\mathbb{Q}) \) is finite. It follows that the constant term \( f(0) \) is non-zero \( p \)-adic integer. By the well known Euler characteristic formula,

\[
f(0) \sim \frac{\#\text{III}(E/\mathbb{Q}[p^\infty]) \times (\prod_i c_i(E)) \times (\#\mathcal{E}(\mathbb{F}_p))^2}{\#(E(\mathbb{Q})[p^\infty])^2}.
\]

In particular, if the three terms \( \#\text{III}(E/\mathbb{Q}[p^\infty]), (\prod_i c_i(E)) \) and \( \#\mathcal{E}(\mathbb{F}_p) \) are units in \( \mathbb{Z}_p \), then \( f(0) \) will be a unit in \( \mathbb{Z}_p \). We study the average behaviour of the following quantities for fixed \( p \) and varying \( E \in \mathcal{E} \),
(1) \( s_p(E) := \# \Sha(E/\Q)[p^{\infty}] \),
(2) \( \tau_p(E) := \prod_i \xi_{\ell_i}(E) \),
(3) \( \delta_p(E) := \#(\tilde{E}(\F_p)[p]) \).

Let \( \mathcal{E}_1, \mathcal{E}_2 \) and \( \mathcal{E}_3 \) to be the set of all elliptic curves \( E/\Q \) with good reduction at \( p \), such that \( p \) divides \( s_p(E) \), \( \tau_p(E) \) and \( \delta_p(E) \) respectively. Note that if \( f(0) \) is a \( p \)-adic unit, then \( \Sel_p(E/\Q_{\text{cyc}}) = 0 \). Thus if \( E \in \mathcal{S}_p \), then \( f(0) \) is not a unit in \( \Z_p \), hence, \( E \in \mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_3 \).

From the containment \( \F_p \subseteq \bigcup_{i=1}^{3} \mathcal{E}_i \), we obtain the following bound:

\[
\hat{d}(\mathcal{S}_p) \leq \sum_{i=1}^{3} \hat{d}(\mathcal{E}_i).
\]

Since we assume that \( (\text{Del}-p) \) is satisfied, we have that

\[
\hat{d}(\mathcal{E}_1) \leq \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{2i-1}} \right) \right).
\]

It follows from [17, Theorem 4.2] or [13, Corollary 8.8] that

\[
\hat{d}(\mathcal{E}_2) \leq \zeta(p) - 1.
\]

Next, it follows from [17, Theorem 4.14] and Proposition 3.12 (or [25, Lemma 6.4]) that

\[
\hat{d}(\mathcal{E}_3) \leq \zeta(10) \frac{\# \mathcal{S}_p}{p^2} < C_1 \frac{\log p (\log \log p)^2 \sqrt{p}}{p^2},
\]

where \( C_1 = \zeta(10)C \). Putting everything together, the result follows. \( \square \)

**Remark 4.6**  The result shows that when \( p \) is suitably large the density of the set \( \mathcal{S}_p \) is quite small.

- Note that \( \sqrt{p} \) grows faster than \( \log p (\log \log p)^2 \) as \( p \to \infty \), hence, the term \( C_1 \frac{\log p (\log \log p)^2 \sqrt{p}}{p^2} \) goes to 0 as \( p \to \infty \). However, the exact values of \( \# \mathcal{S}_p \) can be calculated for small enough primes, and for this, we refer to Table 1 (or, [18, Table 2]).
- The function

\[
f(p) := \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{2i-1}} \right) \right) = \frac{1}{p} + \frac{1}{p^3} - \frac{1}{p^4} + \ldots
\]

is a function whose domain is the set of prime numbers \( p \). As a function of \( p \), it is asymptotic to \( \frac{1}{p} \). In other words,

\[
\lim_{p \to \infty} \frac{f(p)}{p} = 1,
\]

where the limit is over primes \( p \).

This is easy to prove, however, we provide details here. First, it is easy to see that for any integer \( m \geq 1 \),

\[
1 \geq \prod_{i \geq m} \left( 1 - \frac{1}{p^{2i-1}} \right) \geq 1 - \sum_{i \geq m} \frac{1}{p^{2i-1}}.
\]
Therefore, we have the following bounds
\[
f(p) = 1 - \left(1 - \frac{1}{p}\right) \prod_{i \geq 2} \left(1 - \frac{1}{p^{2i-1}}\right) \geq 1 - \left(1 - \frac{1}{p}\right) = \frac{1}{p}, \quad (4.2)
\]
\[
f(p) = 1 - \prod_{i \geq 1} \left(1 - \frac{1}{p^{2i-1}}\right) \leq \sum_{i \geq 1} \frac{1}{p^{2i-1}} = \frac{1}{p} + \frac{1}{p(p^2 - 1)}. \quad (4.3)
\]
Combining (4.2) and (4.3), we find that
\[
1 \leq f(p) \leq 1 + \frac{1}{p^2 - 1},
\]
and it thus follows that \( f(p) \sim \frac{1}{p} \). Therefore, in particular, \( f(p) \) is asymptotically smaller than the term \( C_1 \frac{\log p (\log \log p)^2}{\sqrt{p}} \) as a function of \( p \).

- It is easy to see that
  \[
  \zeta(p) - 1 = 2^{-p} + \sum_{n \geq 3} n^{-p} < 2^{-p} + \int_2^\infty x^{-p} dx = 2^{-p} \left( \frac{p + 1}{p - 1}\right) .
  \]

Thus, Theorem 4.5 shows that \( \delta(\mathfrak{F}_p) \to 0 \) as \( p \to \infty \), and in fact, as a function of \( p \) is \( O \left( \frac{\log p (\log \log p)^2}{\sqrt{p}} \right) \), thereby indicating that given a prime \( p \), most elliptic curves \( E/\mathbb{Q} \) of rank 0 and good ordinary reduction at \( p \) have \( \text{Sel}_{p}^\infty(E/\mathbb{Q}_{\text{cyc}}) = 0 \). In fact, the above remark shows that the contribution of the Tamagawa factors is very little in comparison to that of anomalous primes.

### 4.2 Statistics for the fine Selmer group in the rank-zero case

We now turn our attention to the fine Selmer group. In this subsection, we study the case when \( \text{rank} \ E(\mathbb{Q}) = 0 \). Let \( p \geq 5 \) be a prime number and let \( \mathfrak{B}_p \) be the set of elliptic curves \( E/\mathbb{Q} \) such that the following conditions are satisfied:

1. \( E \) has good reduction at \( p \),
2. \( \text{rank} \ E(\mathbb{Q}) = 0 \),
3. \( \mathcal{R}_p^{\infty}(E/\mathbb{Q}_{\text{cyc}}) \) is infinite (equivalently, either \( \mu_p^{\text{fn}}(E/\mathbb{Q}_{\text{cyc}}) > 0 \) or \( \lambda_p^{\text{fn}}(E/\mathbb{Q}_{\text{cyc}}) > 0 \)).

Thus, we no longer impose the good ordinary condition at \( p \).

**Theorem 4.7** Let \( p \geq 5 \) be a prime and \( \mathfrak{B}_p \) be defined as above. Assume that \( \Pi(E(\mathbb{Q})[p^{\infty}]) \) is finite for all elliptic curves \( E/\mathbb{Q} \) and that the conjecture (Del-p) is satisfied. Then, we have the following bound on the upper density of \( \mathfrak{B}_p \),

\[
\delta(\mathfrak{B}_p) \leq \zeta(10) \frac{\# \mathfrak{B}_p}{p^4} + \left( 1 - \prod_{i \geq 1} \left(1 - \frac{1}{p^{2i-1}}\right) \right) + (\zeta(p) - 1),
\]
\[
\leq \frac{2\zeta(10)}{p} + C_1 \frac{\log p (\log \log p)^2}{p^{5/2}} + \left( 1 - \prod_{i \geq 1} \left(1 - \frac{1}{p^{2i-1}}\right) \right) + (\zeta(p) - 1).
\]

(4.4)

Here \( C_1 \) is explicit constant given by \( C_1 = \zeta(10)C \) from Corollary 3.13.

**Proof** Consider the following quantities:
We prove an upper bound for $\bar{\mathcal{E}}_1$ and $\bar{\mathcal{E}}_2$ consist of all elliptic curves $E/Q$ such that $p$ divides $s_p(E)$ and $\tau_p(E)$ respectively. Let $\mathcal{E}_4$ be the set of all elliptic curves $E/Q$, with good reduction at $p$, such that $p$ divides $\beta_p(E)$. For these elliptic curves, $p$ is a local torsion prime over $\mathbb{Q}_p$. It follows from Corollary 2.7 that $\mathfrak{B}_p$ is contained in the union $\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_4$. Hence, $\delta(\mathfrak{B}_p) \leq \delta(\mathcal{E}_1) + \delta(\mathcal{E}_2) + \delta(\mathcal{E}_4). \tag{4.5}$ From the proof of Theorem 4.5, we have that $\delta(\mathcal{E}_1) + \delta(\mathcal{E}_2) \leq \left(1 - \prod_{i \geq 1} \left(1 - \frac{1}{p^{i-1}}\right)\right) + (\zeta(p) - 1).$ We prove an upper bound for $\delta(\mathcal{E}_4)$. We recall that $\mathfrak{A}_p$ is the set of pairs $(A, B) \in \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$ such that $p \nmid \Delta_{A,B}$ and $\text{rank}_p(E_{A,B}(\mathbb{Z}/p^2)) = 2$. It follows from Lemma 3.5 that an elliptic curve $E_{A,B}$ is contained in $\mathcal{E}_4$ if and only the reduction of $(A, B)$ modulo $p^2$ lies in $\mathfrak{A}_p$. Thus it would seem that $\delta(\mathcal{E}_4)$ is simply equal to $\frac{\#\mathfrak{A}_p}{\#(\mathbb{Z}/p^2 \times \mathbb{Z}/p^2)} = \frac{\#\mathfrak{A}_p}{p^4}$, but this is not quite the case, since not all pairs $(A, B) \in \mathbb{Z} \times \mathbb{Z}$ are minimal. It is well known that the proportion of all pairs $(A, B)$ that are minimal is $\frac{1}{\zeta(10)}$, see for instance [5]. In greater detail, let $\mathcal{W}$ be the set of all pairs of integers $(A, B)$, and $\mathcal{W}_{<x}$ be the subset of pairs such that the height is $< x$. Note that since each elliptic curve $E/Q$ admits a unique minimal Weierstrass equation, we may identify $\mathcal{E}$ with a subset of $\mathcal{W}$. It is easy to see that $\lim_{x \to \infty} \frac{\#\mathcal{E}_{4,<x}}{\#\mathcal{W}_{<x}} = \frac{\#\mathfrak{A}_p}{p^4}$ and since $\lim_{x \to \infty} \frac{\#\mathcal{E}_{<x}}{\#\mathcal{W}_{<x}} = \frac{1}{\zeta(10)},$ it follows that $\delta(\mathcal{E}_4) = \lim_{x \to \infty} \frac{\#\mathcal{E}_{4,<x}}{\#\mathcal{E}_{<x}} = \frac{\zeta(10)}{\#\mathcal{W}_{<x}} \frac{\#\mathfrak{A}_p}{p^4}.$ Appealing to Corollary 3.13, we have that $\delta(\mathcal{E}_4) < \frac{2\zeta(10)}{p} + C_1 p^{-3/2} \log p (\log \log p)^2.$ The result now follows from (4.5). \[\square\] Asymptotically in $p$, the bound (4.4) is $\frac{2\zeta(10) + 1}{p} + O \left( p^{-3/2} \log p (\log \log p)^2 \right),$ which is significantly smaller than the asymptotic estimate $O \left( p^{-1/2} \log p (\log \log p)^2 \right)$ from Theorem 4.5. This tells us that the fine Selmer group is finite a lot more often than the classical Selmer group over $\mathbb{Q}_{cyc},$ since we have saved on an entire factor of $p^{1/2} \log p (\log \log p)^2$ in our estimates.
4.3 Statistics for the fine Selmer group in the rank-one case

Let $E/\mathbb{Q}$ be an elliptic curve with positive Mordell–Weil rank $r = \text{rank } E(\mathbb{Q})$. Set $E(\overline{\mathbb{Q}}_p)$ to be the $p$-adic completion of $E(\mathbb{Q}_p)$ given by $E(\overline{\mathbb{Q}}_p) := \lim_{\leftarrow n} E(\mathbb{Q}_{p^n})$. Recall that $D$ is the cokernel of the map $E(\mathbb{Q}) \otimes \mathbb{Z}_p \rightarrow E(\overline{\mathbb{Q}}_p)$. The group $E(\overline{\mathbb{Q}}_p)$ decomposes into a direct sum $\mathbb{Z}_p \oplus T$, where $T$ is the torsion subgroup of $E(\overline{\mathbb{Q}}_p)$ (see [12, Lemma 2.1, (iv)]). Note that $T$ is non-zero when $p$ is a local torsion prime. The summand $\mathbb{Z}_p$ arises from the formal group of $E$. Write $E(\mathbb{Q}) \otimes \mathbb{Z}_p = \mathbb{Z}_p^r \oplus T'$, where $T'$ is a finite group. The map $E(\mathbb{Q}_p) \otimes \mathbb{Z}_p \rightarrow E(\overline{\mathbb{Q}}_p)$ gives rise to a map

$$\mathbb{Z}_p^r \oplus T' \rightarrow \mathbb{Z}_p \oplus T.$$

The map on the first factors is denoted by $\phi_E : \mathbb{Z}_p^r \rightarrow \mathbb{Z}_p$. This is the composite of the maps $\mathbb{Z}_p^r \hookrightarrow \mathbb{Z}_p^r \oplus T' \rightarrow \mathbb{Z}_p \oplus T \rightarrow \mathbb{Z}_p$,

where the first map is the inclusion into the first factor and the last map is the projection on the first factor.

**Lemma 4.8** Let $E$ be an elliptic curve and $p$ a prime as above and suppose that $\text{Tors}_{\mathbb{Z}_p}(D) \neq 0$. Then, at least one of the following hold:

1. $p$ is a local torsion prime of $E$,
2. $\phi_E$ is not surjective.

**Proof** Suppose that $p$ is not a local torsion prime. Then, it is clear $D$ is a quotient of $\text{cok } \phi_E$. Hence, if $D \neq 0$, it follows that $\text{cok } \phi_E$ is non-zero. This implies that $\phi_E$ is not surjective. 

We shift our attention to the case when our elliptic curves $E/\mathbb{Q}$ have Mordell–Weil rank 1. In this setting, the $p$-adic regulator $\text{Reg } (\mathcal{R}_{p^\infty}(E/\mathbb{Q})) = 1$, and this makes it possible to study this case. Since $r = 1$, the map $\phi_E : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is surjective if and only if it is an isomorphism. We let $\mathcal{E}_5$ be the set of elliptic curves $E/\mathbb{Q}$ such that

1. $\text{rank } E(\mathbb{Q}) = 1$,
2. the map $\phi_E$ is not an isomorphism.

The upper density $\delta(\mathcal{E}_5)$ shall play a role in our results. We are unable to prove any satisfactory bound on $\delta(\mathcal{E}_5)$ which is why we resort to heuristics. The probability that an elliptic curve has rank 1 is expected to be $\frac{1}{2}$. This follows from the rank distribution conjecture. The map $\phi_E : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is multiplication by an element $\alpha \in \mathbb{Z}_p$, and is an isomorphism precisely when $\alpha$ is a unit. Thus, the probability that $\phi_E$ is not an isomorphism can be expected to be $\frac{1}{2p}$. Thus, the heuristic indicates that $\delta(\mathcal{E}_5) = \frac{1}{2p}$. We state our results in terms of the the density $\delta(\mathcal{E}_5)$, and do not explicitly assume that this heuristic is correct. Let $p \geq 5$ be a prime number and let $\mathcal{D}_p$ be the set of elliptic curves $E/\mathbb{Q}$ such that the following conditions are satisfied:

1. $E$ has good reduction at $p$,
2. $\text{rank } E(\mathbb{Q}) = 1$,
3. $\mathcal{R}_{p^\infty}(E/\mathbb{Q}_{\text{cyc}})$ is infinite.
Theorem 4.9 Let $p \geq 5$ be a prime and $\mathcal{D}_p$ be defined as above. Assume that $\Pi(E/\mathbb{Q})[p^\infty]$ is finite for all elliptic curves $E/\mathbb{Q}$ and that the conjecture (Del-p) is satisfied. Then, we have the following bound on the upper density of $\mathcal{D}_p$.

$$\delta(\mathcal{D}_p) \leq \delta(\mathcal{E}_5) + \zeta(10) \frac{\#\mathbb{A}_p}{p^d} + \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{i-1}} \right) \right) + (\zeta(p) - 1),$$

$$\leq \delta(\mathcal{E}_5) + \frac{2 \zeta(10)}{p} + C_1 \frac{\log p \log \log p)^2}{p^{3/2}} + \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{i-1}} \right) \right) + (\zeta(p) - 1).$$

(4.6)

Here $C_1$ is explicit constant given by $C_1 = \zeta(10)C_1$ from Corollary 3.13.

Proof Let $E$ be an elliptic curve in $\mathcal{D}_p$. Consider the following quantities:

1. $s_p(E) := \#\Pi(E/\mathbb{Q})[p^\infty],$
2. $\tau_p(E) := \prod_1 \zeta_1^{(p)}(E),$
3. $\beta_p(E) := \# (E(\mathbb{Q}_p)[p]).$

Recall that $\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{E}_4$ consist of all elliptic curves $E/\mathbb{Q}$ such that $p$ divides $s_p(E)$, $\tau_p(E)$ and $\beta_p(E)$ respectively. It follows from Corollary 2.7 that $E$ is either contained in the union $\mathcal{E}_1 \cup \mathcal{E}_2$ or $\text{Tors}_{\mathbb{Z}_p}(D) \neq 0$. It follows from Lemma 4.8 that if $\text{Tors}_{\mathbb{Z}_p}(D) \neq 0$, then $E \in \mathcal{E}_4 \cup \mathcal{E}_5$. Therefore, combining the above observations, we find that $\mathcal{D}_p$ is contained in the union $\mathcal{E}_1 \cup \mathcal{E}_2 \cup \mathcal{E}_4 \cup \mathcal{E}_5$, and hence,

$$\delta(\mathcal{D}_p) \leq \delta(\mathcal{E}_1) + \delta(\mathcal{E}_2) + \delta(\mathcal{E}_4) + \delta(\mathcal{E}_5).$$

From the proof of Theorem 4.7,

$$\delta(\mathcal{E}_1) + \delta(\mathcal{E}_2) + \delta(\mathcal{E}_4) \leq \zeta(10) \frac{\#\mathbb{A}_p}{p^d} + \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{i-1}} \right) \right) + (\zeta(p) - 1)$$

$$< C_1 \frac{\log p \log \log p)^2}{p^{3/2}} + \left( 1 - \prod_{i \geq 1} \left( 1 - \frac{1}{p^{i-1}} \right) \right) + (\zeta(p) - 1),$$

and the result follows from this. \qed

5 Sieve methods and the distribution of local torsion primes

The distribution of local torsion primes is closely connected to the behavior of Iwasawa invariants of elliptic curves. Let $E/\mathbb{Q}$ be an elliptic curve with Mordell–Weil rank zero for which the Tate–Shafarevich group $\Pi(E/\mathbb{Q})$ is finite. Then Corollary 2.10 asserts that $\mu_p^{\infty}(E/\mathbb{Q}_{\text{cyc}}) = 0$ and $\lambda_p^{\infty}(E/\mathbb{Q}_{\text{cyc}}) = 0$ for all primes $p \notin \Pi_{l,E} \cup \mathcal{S}$. Here, $\mathcal{S}$ is the set of primes that divide $2\#\Pi(E/\mathbb{Q}) \times \prod_{c} c_\ell(E)$. In particular, if the set $\Pi_{l,E}$ is finite, then $\mu_p^{\infty}(E/\mathbb{Q}_{\text{cyc}}) = 0$ and $\lambda_p^{\infty}(E/\mathbb{Q}_{\text{cyc}}) = 0$ for all but finitely many primes $p$.

In this section we shall fix a number $Y > 0$, and prove results about the expectation for $\#\Pi_{l,E}(Y)$, as $E$ ranges over all elliptic curves over $\mathbb{Q}$. We shall prove our results for elliptic curves on average. For this purpose, the shall employ the use of a certain refined version of the Large sieve inequality due to Bombieri and Davenport [1]. The version that we use has previously been used in various other contexts, see [7, 15]. The version we
require is slightly more general than the sieve used in the aforementioned works. Given real numbers \( a \leq b \), let \([a, b]\) denote the closed interval from \( a \) to \( b \). Given a tuple of real numbers \((M_1, \ldots, M_k) \in \mathbb{R}^k\) and a tuple of positive real numbers \((N_1, \ldots, N_k) \in \mathbb{R}^k_{>0}\), the product \( \prod_{j=1}^k [M_j, M_j + N_j] \) consists of all tuples of real numbers \((x_1, \ldots, x_k)\) such that \( M_j \leq x_j \leq M_j + N_j \) for all \( j \). We shall refer to such a product of intervals as a box in \( \mathbb{R}^k \). For each point \( n \in B \cap \mathbb{Z}^k \) let \( c(n) \) be a complex number. Define a function on \( \mathbb{R}^k \) as follows

\[
S(x) := \sum_{n \in B} c(n)e(n \cdot x),
\]

where \( x \in \mathbb{R}^k \) and \( e(z) := e^{2\pi iz} \).

**Definition 5.1** Let \( A \subset \mathbb{R}^k \) be a finite subset and let \( \delta = (\delta_1, \ldots, \delta_k) \) be a tuple of positive numbers. We say that \( A \) is \( \delta \) well-spaced if for all \( \alpha = (\alpha_1, \ldots, \alpha_k) \in A \) and \( \beta = (\beta_1, \ldots, \beta_k) \in A \) such that \( \alpha \neq \beta \),

\[
\max \left\{ \frac{|\alpha_i - \beta_i|}{\delta_i} \mid i = 1, \ldots, k \right\} \geq 1.
\]

In other words, for each pair \((\alpha, \beta)\) such that \( \alpha \neq \beta \), there is a coordinate \( i \) such that \( |\alpha_i - \beta_i| \geq \delta_i \). The following generalization of the Large sieve inequality is due to Huxley, see [14, Theorem 1].

**Theorem 5.2** (Huxley) Let \( A \) be a \( \delta \) well-spaced finite set of vectors in \( \mathbb{R}^k \) and let \( B = \prod_{j=1}^k [M_j, M_j + N_j] \). Then, we have the following bound

\[
\sum_{\alpha \in A} |S(\alpha)|^2 \leq \left( \prod_{j=1}^k (N_j^{1/2} + \delta_j^{-1/2})^2 \right) \sum_{n \in B} |c(n)|^2.
\]

Fix a number \( N \in \mathbb{Z}_{>1} \) and for each prime \( p \), we fix a subset \( \Omega(p) \) of \( (\mathbb{Z}/p^N\mathbb{Z})^k \) for each prime \( p \). For each integral vector \( m \in \mathbb{Z}^k \), real number \( x > 0 \), we define

\[
P(x; m) := \# \left\{ p \leq x \mid m \mod p^N \in \Omega(p) \right\}
\]

and

\[
P(x) := \sum_{p \leq x} \#\Omega(p)p^{-Nk}.
\]

In the statement of the result below, \( x \) will refer to a positive real number.

**Theorem 5.3** For each prime \( p \), let \( \Omega(p) \) be a subset of \( (\mathbb{Z}/p^N\mathbb{Z})^k \). Let

\[
B = \prod_{j=1}^k [M_j, M_j + N_j]
\]

be a box in \( \mathbb{R}^k \) such that \( N_j \geq x^{2N} \) for all \( j \). Let \( V(B) \) be the volume of the box \( V(B) = \prod_j N_j \), then

\[
\sum_{m \in B \cap \mathbb{Z}^k} (P(x; m) - P(x))^2 \ll_{k,N} V(B)P(x).
\]

The notation above means that there is a constant \( C > 0 \) which depends only on \( k \) and \( N \), and not on \( x \), such that \( \sum_{m \in B \cap \mathbb{Z}^k} (P(x; m) - P(x))^2 \leq CV(B)P(x) \) for all real numbers \( x > 0 \).
Proof  Let $A = \bigcup_{p \leq x} A_p$, where
\[ A_p = \{ \alpha_1(p), \alpha_2(p), \ldots, \alpha_{p^{N+1}}(p) \} \]
is a complete set of representatives $\frac{1}{p^k}\mathbb{Z}/\mathbb{Z}$. The set is $\delta$ well-spaced for $\delta_i = \frac{1}{x^N}$ for all $i$. A standard argument shows that Theorem 5.2 can be applied to $A$, in order to deduce the statement of Theorem 5.3. This follows verbatim from the argument given in [10, p.93, l.15 to p.94, l.10].

We next apply the above result to studying the average distribution of local torsion primes. Let $k, N = 2$ and for each prime $p$, let $\Omega(p) := \mathfrak{X}_p \subset \mathbb{Z}/p^2 \times \mathbb{Z}/p^2$. Thus, for $Y > 0$, we have that $P(Y) = \sum_{p \leq Y} \frac{\# \mathfrak{X}_p}{p^2}$. Let $C, D > Y^4$, and consider the set $S_{C,D}$ of all pairs $m = (a, b) \in \mathbb{Z} \times \mathbb{Z}$ with $|a| < C$ and $|b| < D$. Fix a number $\beta > 0$. Let $S_{C,D}^\beta$ be the subset of $m = (a, b) \in S_{C,D}$ such that
\[ |\# \Pi_{lt,E_m}(Y) - P(Y)| < \beta \sqrt{P(Y)}, \]
and set $Q_{C,D}^\beta := S_{C,D} \setminus S_{C,D}^\beta$.

Theorem 5.4  Let $Y > 0$ be a fixed number. Then, there is an absolute constant $c > 0$ such that for any number $\beta > 0$ the proportion of elliptic curves $E$ for which
\[ |\# \Pi_{lt,E}(Y) - P(Y)| < \beta \sqrt{P(Y)} \tag{5.1} \]
is $\geq (1 - \frac{c}{Y^2})$. Furthermore, if $C, D > Y^4$, we have that $\frac{\#Q_{C,D}^\beta}{S_{C,D}} < \frac{\epsilon}{\beta^2}$ for any $\beta > 0$.

Remark 5.5  Setting $\beta = 10\sqrt{c}$, we find that $\geq 99\%$ of elliptic curves satisfy (5.1).

Proof  Let $C$ and $D$ be integers such that $C, D > Y^4$. We are to show that there is an absolute constant $c > 0$ such that $\frac{\#Q_{C,D}^\beta}{S_{C,D}} < \frac{\epsilon}{\beta^2}$ for any $\beta > 0$. This implies that the proportion of elliptic curves $E/\mathbb{Q}$ (ordered by height) for which
\[ |\# \Pi_{lt,E}(Y) - P(Y)| \geq \beta \sqrt{P(Y)} \]
is $\leq c/\beta^2$.

Let $E_{a,b}$ be an elliptic curve associated with a minimal pair $m = (a, b) \in \mathbb{Z} \times \mathbb{Z}$. Note that by definition, $P(Y; m) = \#\Pi_{lt,E}(Y)$.

According to the square sieve inequality of Theorem 5.3,
\[ \sum_{m \in S_{C,D}} (P(m; Y) - P(Y))^2 < c \#S_{C,D}P(Y), \tag{5.2} \]
where $c > 0$ is an absolute constant. On the other hand,
\[ \sum_{m \in S_{C,D}} (P(m; Y) - P(Y))^2 \geq \sum_{m \in Q_{C,D}} (P(m; Y) - P(Y))^2, \]
\[ = \sum_{m \in Q_{C,D}} (\#\Pi_{lt,E_m}(Y) - P(Y))^2, \tag{5.3} \]
\[ \geq \sum_{m \in Q_{C,D}} \beta^2 P(Y) = \#Q_{C,D} \beta^2 P(Y). \]
Combining the inequalities from (5.2) and (5.3), we have shown that \( \frac{\#Q_{C,D}}{\#S_{C,D}} < \frac{c}{\beta^2} \), and this completes the proof. \( \square \)

The above result thus proves an explicit result for the expectation for \( \# \Pi_{R,E}(Y) \), which is shown to be close to \( P(Y) = \sum_{p \leq Y} \frac{\#A_p}{p^2} \).

6 Numerical data

| \( p \) | \( \#S_p/p^2 \) | \( p \) | \( \#S_p/p^2 \) |
|---|---|---|---|
| 7 | 0.0816326530612245 | 71 | 0.0208292005554453 |
| 11 | 0.0413223140495868 | 73 | 0.0270219553387127 |
| 13 | 0.0710059171597633 | 79 | 0.0374939913475405 |
| 17 | 0.0276816608996540 | 83 | 0.0178545507330527 |
| 19 | 0.0581717451523546 | 89 | 0.0222194167403106 |
| 23 | 0.0415879017013233 | 97 | 0.0255074928260176 |
| 29 | 0.0323936979785969 | 101 | 0.00980296049406921 |
| 31 | 0.0312174817898023 | 103 | 0.0288434348194929 |
| 37 | 0.0306793279766253 | 107 | 0.00925845051969604 |
| 41 | 0.011897679524093 | 109 | 0.0181802878545577 |
| 43 | 0.0567874526771228 | 113 | 0.0263137285613595 |
| 47 | 0.0208239022181983 | 127 | 0.0169260338520677 |
| 53 | 0.027767889284443 | 131 | 0.0189382903094225 |
| 59 | 0.0166618787704683 | 137 | 0.010868860940913 |
| 61 | 0.0349368449341575 | 139 | 0.0142849748977796 |
| 67 | 0.014702603711294 | 149 | 0.0133327327597856 |
Acknowledgements
The first named author’s research is supported by the CRM-Simons postdoctoral fellowship. He would like to thank Jeffrey Hatley, Debanjana Kundu and Antonio Lei for helpful discussions and comments. He would also like to thank Christian Wuthrich and Will Sawin for their suggestions in response to a question posted by the first named author on Mathoverflow.org. The second named author gratefully acknowledges support from NSERC Discovery grant 2019-03987. The authors would like to thank the referees for helpful suggestions.

Data availability
No data was generated or analyzed in this paper.

Author details
1 Centre de Recherches Mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920 Chemin de la tour, Montréal, QC H3T 1J4, Canada, 2 Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada.

Received: 12 January 2022 Accepted: 13 July 2023 Published online: 29 July 2023

References
1. Bombieri, E., Davenport, E.: On the Large Sieve Method. Number Theory and Analysis, pp. 9–22. Springer, New York (1969)
2. Bhargava, E., Shankar, A.: The average size of the 5-selmer group of elliptic curves is 6, and the average rank is less than 1. http://arxiv.org/abs/1312.7859 (2013)
3. Coates, J., Sujatha, R.: Galois cohomology of elliptic curves tata inst. fund. res. Lecture Notes. Narosa Publishing House (2000)
4. Coates, J., Sujatha, R.: Fine Selmer groups of elliptic curves over p-adic lie extensions. Math. Ann. 331(4), 809–839 (2005)
5. Cremona, J.E., Sadek, M.: Local and global densities for Weierstrass models of elliptic curves. http://arxiv.org/abs/2003.08454 (2020)
6. Delaunay, C.: Heuristics on class groups and on tate-shafarevich groups: the magic of the cohen-lenstra heuristics. Rank Elliptic Curves Random Matrix Theory 341, 323–340 (2007)
7. Duke, W.: Elliptic curves with no exceptional primes. Comptes rendus de l’Académie des sciences. Série 1 Mathématique 235(8), 813–818 (1997)
8. David, C., Weston, T.: Local torsion on elliptic curves and the deformation theory of galois representations. Math. Res. Lett. 15(3), 599–611 (2008)
9. Ferrero, B., Washington, L.C.: The Iwasawa invariant μp vanishes for abelian number fields. Ann. Math. 109, 377–395 (1979)
10. Gallagher, P.X.: The large sieve and probabilistic galois theory. Proc. Symp. Pure Math 24, 91–101 (1973)
11. Greenberg, R.: Arithmetic Theory of Elliptic Curves: Lectures given at the 3rd Session of the Centro Internazionale Mathematico Estivo (CIME) held in Cetaro, Italy, 12–19 July, 1997. Springer (1999)
12. Hiranouchi, T.: Local torsion primes and the class numbers associated to an elliptic curve over Q. Hiroshima Math. J. 49(1), 117–127 (2019)
13. Hatley, J., Kundu, D., Ray, A.: Statistics for anticyclotomic iwasawa invariants of elliptic curves. http://arxiv.org/abs/2106.01517 (2021)
14. Huxley, M.N.: The large sieve inequality for algebraic number fields. Mathematika 15(2), 178–187 (1968)
15. Jones, N.: Almost all elliptic curves are serre curves. Trans. Am. Math. Soc. 362(3), 1547–1570 (2010)
16. Kato, K.: p-adic hodge theory and values of zeta functions of modular forms. Asterisque 295, 117–290 (2004)
17. Kundu, D., Ray, A.: Statistics for Iwasawa invariants of elliptic curves. Trans. Am. Math. Soc. 374, 7945–7965 (2021). https://doi.org/10.1090/tran/8478
18. Kundu, D., Ray, A.: Statistics for Iwasawa invariants of elliptic curves, II. http://arxiv.org/abs/2106.12095 (2021)
19. Katz, N., Sarnak, P.: Random Matrices, Frobenius Eigenvalues, and Monodromy, vol. 45. American Mathematical Society, Providence (1999)
20. Lenstra, H.W., Jr.: Factoring integers with elliptic curves. Ann. Math. 126, 649–673 (1987)
21. Lang, S., Trotter, H.: Frobenius Distributions in GL2-Extensions: Distribution of Frobenius Automorphisms in GL2-Extensions of the Rational Numbers, vol. 504. Springer, New York (2006)
22. Mazur, B.: Rational points of abelian varieties with values in towers of number fields. Invent. Math. 18(3–4), 183–266 (1972)
23. Murty, V.K.: Modular forms and the chebotarev density theorem II. Lond. Math. Soc. Lecture Note Ser. 58, 287–308 (1997)
24. Poonen, B., Rains, E.: Random maximal isotropic subspaces and Selmer groups. J. Am. Math. Soc. 25(1), 245–269 (2012)
25. Ray, A.: Arithmetic statistics and diphantine stability for elliptic curves. http://arxiv.org/abs/2109.06830 (2021)
26. Rudigill, P.C.: On the Frequency of Finitely Anomalous Elliptic Curves. University of Massachusetts, Amherst (2010)
27. Rohrlich, D.E.: On-funcions of elliptic curves and cyclotomic towers. Invent. Math. 75(3), 409–423 (1984)
28. Ray, A., Sujatha, R.: On the μ-invariants of residually reducible galois representations. http://arxiv.org/abs/2104.10797 (2021)
29. Schoof, R.: Nonsingular plane cubic curves over finite fields. J. Combin. Theory Ser. A 46(2), 183–211 (1987)
30. Serre, J.P.: Galois properties of finite order points of elliptic curves. Invent. Math. 15(4), 259–331 (1971)
31. Washington, L.C.: Introduction to Cyclotomic Fields, vol. 83. Springer, New York (1997)
32. Waterhouse, W.C.: Abelian varieties over finite fields. Annales scientifiques de l’École normale supérieure 2, 521–560 (1969)
33. Wuthrich, C.: The fine tate–shaferich group. In: Mathematical Proceedings of the Cambridge Philosophical Society, vol. 142, pp. 1–12. Cambridge University Press (2007)
34. Wuthrich, C.: Iwasawa theory of the fine Selmer group. J. Algebr. Geom. 16(1), 83–108 (2007)

Publisher’s Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s), author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.