RANK JUMPS AND GROWTH OF SHAFAREVICH–TATE GROUPS FOR ELLIPTIC CURVES IN $\mathbb{Z}/p\mathbb{Z}$-EXTENSIONS

LEA BENEISH, DEBANJANA KUNDU, AND ANWESH RAY

ABSTRACT. Let p be a prime. In this paper, we use techniques from Iwasawa theory to study questions about rank jump of elliptic curves in cyclic extensions of degree p. We also study growth of the p-primary Selmer group and the Shafarevich–Tate group in cyclic degree-p extensions and improve upon previously known results in this direction.

1. INTRODUCTION

A fundamental result in the theory of elliptic curves is the *Mordell–Weil Theorem*. It states that given an elliptic curve E defined over a number field F, its F-rational points form a finitely generated abelian group, i.e.,

$$E(F) \simeq \mathbb{Z}^r \oplus E(F)_{\text{tors}}$$

where r is a non-negative integer called the *rank* and $E(F)_{\text{tors}}$ is a finite group, called the *torsion subgroup*. Over $\mathbb{Q}$, the possible structures of $E(\mathbb{Q})_{\text{tors}}$ is known by the work of B. Mazur (see [Maz77, Maz78]). These techniques have been extended by S. Kamienny– M. Kenku–F. Momose (see for example [KM88, Kam92]) to provide the complete classification of torsion subgroups for quadratic fields. More recently, in a series of work by several authors the classification of torsion subgroups for cubic fields has been completed (see [JKS04, JKL11, Wan15, Naj16, BN16, DN19, DEvH$^+$21]). In [Mer96], L. Merel proved that for elliptic curves over any number field, the bound on the order of the torsion subgroup depends only on the degree of the number field. Despite remarkable advances made towards understanding the torsion subgroup, the rank remains mysterious and to-date there is no known algorithm to compute it. Almost always, obtaining information about the rank of the elliptic curve involves studying the *Selmer group*.

Let p be a prime number. In [Maz72], Mazur initiated the study of p-primary Selmer groups of elliptic curves in $\mathbb{Z}_p$-extensions. Since then, Iwasawa theory of elliptic curves has been successfully used by many authors to study rank growth in towers of number fields. However, the scope of this paper is different. We use results from Iwasawa theory of Selmer groups of elliptic curves to obtain results on rank growth in cyclic degree-p extensions. Let $L/\mathbb{Q}$ be a finite extension and E an elliptic curve over $\mathbb{Q}$. Mazur and Rubin [MRL18] define E to be *diophantine-stable* in L if $E(L) = E(\mathbb{Q})$. This property is of significant importance

and has applications to Hilbert's 10th problem for number fields. In this paper, we answer the following two questions about growth of Selmer groups in cyclic degree-p extensions.

(1) Given an elliptic curve $E_{/\mathbb{Q}}$ with trivial p-primary Selmer group, for what proportion of degree-p cyclic extensions does the p-primary Selmer group remain trivial upon base-change?

(2) Given a prime $p \neq 2, 3$, varying over all elliptic curves defined over $\mathbb{Q}$, for what proportion of elliptic curves does there exist *at least one* $\mathbb{Z}/p\mathbb{Z}$-extension where the p-primary Selmer group remains trivial upon base-change?

The proportion of elliptic curves is computed with respect to height (see (7)). Our results are proven for elliptic curves $E_{/\mathbb{Q}}$ with Mordell-Weil rank 0. Using standard arguments from Iwasawa theory, one can show that the p-primary Selmer group has rank 0 over the cyclotomic $\mathbb{Z}_p$-extension of a number field L (in particular, over L itself) if and only if the associated μ-invariant and λ-invariant are trivial (see for example [KR21a, Corollary 3.6]). Controlling the μ-invariant is relatively easy and it is known to behave well in p-extensions (see Theorem 2.3). So the key idea involves showing how often the λ-invariant remains trivial upon base-change to $L/\mathbb{Q}$. Given $n \geq 0$, let L_n denote the cyclotomic $\mathbb{Z}/p^n\mathbb{Z}$ extension of L. This is the unique $\mathbb{Z}/p^n\mathbb{Z}$-extension of L contained inside $L(\mu_{p^\infty})$. We note that we have at this point in our notation suppressed the dependence on the prime p. Since $\lambda_p(E/L) \geq \text{rank}_{\mathbb{Z}}(E(L_n))$ (see Lemma 2.2), proving triviality of the λ-invariant upon base-change implies the rank does not change in L. In fact, we prove a stronger result, and show that the rank does not in fact increase in L_n for all $n \geq 0$. To answer the first question, we prove the following result.

Theorem A. *Let $E_{/\mathbb{Q}}$ be a non-CM elliptic curve and p be a fixed prime number ≥ 5 such that the residual representation at p is surjective. Further suppose that $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$. Then, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$ in which the λ-invariant does not increase. In particular, in infinitely many cyclic degree-p number fields $L/\mathbb{Q}$ the rank does not grow in L_n for all $n \geq 0$, i.e.,*

$$\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \text{rank}_{\mathbb{Z}} E(L_n) \text{ for all } n \geq 0.$$

In the case that $E_{/\mathbb{Q}}$ is a CM elliptic curve, we can prove a similar result under an additional independence hypothesis which we make precise in Hyp CM.

The condition $\lambda_p(E/\mathbb{Q}) = 0$ can only be satisfied for elliptic curves $E_{/\mathbb{Q}}$ of Mordell-Weil rank 0, and thus the above result shows that the rank remains 0 in the fields L_n.

Even though our proof suggests that the λ-invariant does not jump in *many* $\mathbb{Z}/p\mathbb{Z}$-extensions, we are unable to show that this is true for a positive proportion of $\mathbb{Z}/p\mathbb{Z}$-extensions. It is known by the work of R. Greenberg [Gre99, Theorem 5.1] that given a rank 0 elliptic curve E over $\mathbb{Q}$, for *density one* good ordinary primes $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$.

In a recent paper (see [GJN20]), E. González-Jiménez and F. Najman investigated the question of when the torsion group does not grow upon base-change (see Theorem 3.9 for the precise statement). This, when combined with the above theorem, allows us to comment on when the Mordell–Weil group *does not* grow in $\mathbb{Z}/p\mathbb{Z}$-extensions. More precisely,

Corollary A. *Given a non-CM elliptic curve $E_{/\mathbb{Q}}$ and a prime $p > 7$ such that the residual representation at p is surjective and $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions $L/\mathbb{Q}$ such that*

$$E(L) = E(\mathbb{Q}).$$

.

The same assertion holds for elliptic curves with CM provided **Hyp CM** holds.

A natural extension of the previous question is the following: when does the p-primary Selmer group grow upon base-change? We address this question in Section 4. First, we prove a result regarding the growth of the p-primary Selmer group of an elliptic curve $E_{/\mathbb{Q}}$ upon base-change up a $\mathbb{Z}/p\mathbb{Z}$-extension (see Proposition 4.1). This result gives a criterion for either the rank to jump, or the order of the Shafarevich–Tate group to increase upon base-change. It applies to all primes $p \geq 5$ and the method relies on exploiting the relationship between Iwasawa invariants and the Euler characteristic. It is motivated by ideas from [RS19, RS20], as well as the use of Kida's formula (Theorem 2.3). This criterion is then used to show that the Selmer group becomes non-zero in a large family of $\mathbb{Z}/p\mathbb{Z}$-extensions. Given an elliptic curve $E_{/\mathbb{Q}}$ and a prime p, we set $E[p]$ to denote the p-torsion subgroup of $E(\bar{\mathbb{Q}})$. The residual representation at p refers to the Galois representation

$$\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

on $E[p]$. More precisely, we can prove the following result.

Theorem B. *Let $p \geq 5$ be a fixed prime and $E_{/\mathbb{Q}}$ be an elliptic curve with good ordinary reduction at p. Suppose that the image of the residual representation is surjective, the p-primary Selmer group over $\mathbb{Q}$ is trivial, and $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$. Then, there is a set of primes of the form $q \equiv 1 \pmod{p}$ with density at least $\frac{p}{(p-1)^2(p+1)}$ such that the p-primary Selmer group becomes non-trivial in the unique $\mathbb{Z}/p\mathbb{Z}$-extension contained in $\mathbb{Q}(\mu_q)$.*

However, we remark that this method is unable to distinguish between jumps in rank and jumps in the order of the Shafarevich–Tate group. These methods are currently being refined by the third named author, and in a subsequent paper, will be applied to a large number of problems in Diophantine stability and arithmetic statistics.

In response to the second question, we show the following.

Theorem C. *Suppose that the Shafarevich–Tate group is finite for all rank 0 elliptic curves defined over $\mathbb{Q}$ and **Hyp ind** holds. For a positive proportion of rank 0 elliptic curves defined over $\mathbb{Q}$, there is at least one $\mathbb{Z}/p\mathbb{Z}$-extension over $\mathbb{Q}$ disjoint from the cyclotomic $\mathbb{Z}_p$-extension, $\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}$, with trivial p-primary Selmer group upon base-change.*

Hyp ind is the assumption that the proportion of rank 0 elliptic curves (ordered by height) with a fixed reduction type at a prime q is the same as the proportion of all elliptic curves (ordered by height) with the same property. In other words, the reduction type at q is independent of the rank of the elliptic curve.

We remark that the main reason for us to restrict the study to elliptic curves at primes of good ordinary reduction is to ensure that we can use results on λ-invariants of elliptic

curves from [HM99]. There are recent results which extend the aforementioned theorem to the non-ordinary case. It seems reasonable to expect that our results should extend to the supersingular case using the work of J. Hatley and A. Lei in [HL19, Theorem 6.7].

In [Čes17], K. Česnavičius showed that the p-Selmer group of elliptic curves over a number field becomes arbitrarily large when varying over $\mathbb{Z}/p\mathbb{Z}$-extensions. This result is not surprising, as it is widely believed that the growth of ideal class groups and Selmer groups of elliptic curves are often analogous. The unboundedness of the 2-part of the ideal class group in quadratic extensions goes back to Gauss; for its generalization to an odd prime see [BCH$^+$66, VII-12, Theorem 4]. The *rank boundedness conjecture* for elliptic curves asks whether there is an upper bound for the Mordell–Weil rank of elliptic curves over number fields. This question is widely open and experts are unable to come to a consensus on what to expect, see [PPVW19, Section 3] for a historical survey. Those in favour of unboundedness argue that this phenomenon provably occurs in other global fields, and that the proven lower bound for this upper bound increases every few years. For instance, N. Elkies discovered an elliptic curve over $\mathbb{Q}$ with Mordell–Weil rank at least 28. On the other hand, a recent series of papers by B. Poonen et. al. provides a justified heuristic inspired by ideas from arithmetic statistics which suggests otherwise (see for example, [Poo18]).

The interplay between the rank, Selmer group, and the Shafarevich–Tate group raises the question of producing elliptic curves with "large Shafarevich–Tate groups." More precisely, given a number field F, a prime p, and a positive integer n, does there exist an elliptic curve $E_{/F}$ whose Shafarevich–Tate group contains at least n elements of order p? A dual question one can ask is the following: given $E_{/\mathbb{Q}}$, a positive integer n, and a prime p, does there exist a number field $F/\mathbb{Q}$ (with additional properties) such that the Shafarevich–Tate group, denoted by $\Sha(E/F)$, contains at least n elements of order p?

In the final section, we study growth questions for Shafarevich–Tate groups. When $p = 2$, K. Matsuno showed that the 2-rank of the Shafarevich–Tate group becomes arbitrarily large in quadratic extensions of number fields (see [Mat09]). In Theorem 5.6 we prove an effective version of this theorem for elliptic curves without any exceptional primes. In particular, given $n > 0$ we find an upper bound on the minimal conductor of the quadratic extension (say K) such that $\mathrm{rank}_2 \Sha(E/K) := \dim_{\mathbb{F}_2} \Sha(E/K)[2] > n$. Recently it has been shown in [MP22] that there are infinitely many elliptic curves with large $\mathrm{rank}_2 \Sha(E/K)$. When $p \neq 2$, P. Clark and S. Sharif showed that varying over all degree-p extensions of $\mathbb{Q}$, not necessarily Galois, the p-rank of the Shafarevich–Tate group can become arbitrarily large, see [CS10]. They further raised a question as to whether this result is the best possible. In Section 5.2, we show that if a conjecture of C. David–J. Fearnley–H. Kisilevsky is true (see §2.2 for the precise statement), then the result of Clark–Sharif can be improved. In particular, instead of varying over all degree-p extensions, it suffices to vary over all $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$.

Organization: Including this Introduction, the article has 6 sections. Section 2 is preliminary in nature; after introducing the main objects of interest, we record relevant results from Iwasawa theory. We also mention some conjectures and heuristics on rank growth of elliptic curves in Galois extensions. In Section 3, we use techniques from Iwasawa theory

to prove results on rank jump of elliptic curves in cyclic degree-p extensions. In Section 4, we study arithmetic statistics related questions pertaining to the growth of the p-primary Selmer groups in $\mathbb{Z}/p\mathbb{Z}$-extensions. In Section 5, we study the growth of the p-rank of Shafarevich–Tate group in cyclic degree-p extensions. One of our results on rank growth requires a mild hypothesis, we provide computational evidence for the same. The table is included in Section 6.

2. Preliminaries

Let F be a number field and $E_{/F}$ be an elliptic curve defined over F. Fix an algebraic closure of F and write G_F for the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$. For a given integer m, set $E[m]$ to be the Galois module of all m-torsion points in $E(\overline{F})$. If v is a prime in F, we write F_v for the completion of F at v. The main object of interest is the Selmer group.

Definition 2.1. For any integer $m \geq 2$, the *m-Selmer group* is defined as follows

$$\mathrm{Sel}_m(E/F) = \ker\left(H^1\left(G_F, E[m]\right) \to \prod_v H^1\left(G_{F_v}, E\right)[m]\right).$$

This m-Selmer group fits into the following short exact sequence

(1) $$0 \to E(F)/mE(F) \to \mathrm{Sel}_m(E/F) \to \text{Ш}(E/F)[m] \to 0.$$

Here, $\text{Ш}(E/F)$ is the *Shafarevich–Tate group* which is conjecturally finite. Throughout this article, we will assume the finiteness of the Shafarevich–Tate group.

2.1. **Recollections from Iwasawa theory.** For details, we refer the reader to standard texts in Iwasawa theory (e.g. [Was97, Chapter 13]). Let p be a fixed prime. Consider the (unique) *cyclotomic* $\mathbb{Z}_p$-extension of $\mathbb{Q}$, denoted by $\mathbb{Q}_{\mathrm{cyc}}$. Set $\Gamma := \mathrm{Gal}(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}) \simeq \mathbb{Z}_p$. The *Iwasawa algebra* Λ is the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$. Fix a topological generator γ of Γ; there is the following isomorphism of rings

$$\Lambda \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!]$$
$$\gamma \mapsto 1 + T.$$

Let M be a cofinitely generated cotorsion Λ-module. The *Structure Theorem of Λ-modules* asserts that the Pontryagin dual of M, denoted by $M^\vee$, is pseudo-isomorphic to a finite direct sum of cyclic Λ-modules. In other words, there is a map of Λ-modules

$$M^\vee \longrightarrow \left(\bigoplus_{i=1}^s \Lambda/(p^{m_i})\right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(h_j(T))\right)$$

with finite kernel and cokernel. Here, $m_i > 0$ and $h_j(T)$ is a distinguished polynomial (i.e., a monic polynomial with non-leading coefficients divisible by p). The *characteristic ideal* of $M^\vee$ is (up to a unit) generated by the *characteristic element*,

$$f_M^{(p)}(T) := p^{\sum_i m_i} \prod_j h_j(T).$$

The μ-invariant of M is defined as the power of p in $f_M^{(p)}(T)$. More precisely,

$$\mu(M) = \mu_p(M) := \begin{cases} 0 & \text{if } s = 0 \\ \sum_{i=1}^{s} m_i & \text{if } s > 0. \end{cases}$$

The λ-invariant of M is the degree of the characteristic element, i.e.

$$\lambda(M) = \lambda_p(M) := \sum_{j=1}^{t} \deg h_j(T).$$

Let $E_{/F}$ be an elliptic curve with good reduction at p. We shall assume throughout that the prime p is odd. Let $N = N_E$ denote the conductor of E and denote by S the (finite) set of primes which divide Np. Let F_S be the maximal algebraic extension of F which is unramified at the primes $v \notin S$. Set $E[p^\infty]$ to be the Galois module of all p-power torsion points in $E(\overline{F})$. For a prime $v \in S$ and any finite extension L/F contained in the unique cyclotomic $\mathbb{Z}_p$-extension of F (denoted by F_{cyc}), write

$$J_v(E/L) = \bigoplus_{w|v} H^1 \left(G_{L_w}, E \right) [p^\infty]$$

where the direct sum is over all primes w of L lying above v. Then, the *p-primary Selmer group over L* is defined as follows

$$\mathrm{Sel}_{p^\infty}(E/L) := \ker \left\{ H^1 \left(\mathrm{Gal}\left(F_S/L \right), E[p^\infty] \right) \longrightarrow \bigoplus_{v \in S} J_v(E/L) \right\}.$$

It is easy to see that $\mathrm{Sel}_{p^\infty}(E/L) = \varinjlim_n \mathrm{Sel}_{p^n}(E/L)$, see for example [CS00, §1.7]. By taking direct limits of (1), the p-primary Selmer group over F fits into a short exact sequence

(2) $$0 \to E(F) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/F) \to Ш(E/F)[p^\infty] \to 0.$$

Next, define

$$J_v(E/F_{\mathrm{cyc}}) = \varinjlim J_v(E/L)$$

where L ranges over finite extensions contained in F_{cyc} and the inductive limit is taken with respect to the restriction maps. The *p-primary Selmer group over F_{cyc}* is defined as follows

$$\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}}) := \ker \left\{ H^1 \left(\mathrm{Gal}\left(F_S/F_{\mathrm{cyc}} \right), E[p^\infty] \right) \longrightarrow \bigoplus_{v \in S} J_v(E/F_{\mathrm{cyc}}) \right\}.$$

When E is an elliptic curve defined over $\mathbb{Q}$, p is an odd prime of good *ordinary* reduction, and $F/\mathbb{Q}$ is an abelian extension, K. Kato proved (see [Kat04, Theorem 14.4]) that the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})$ is a cofinitely generated cotorsion Λ-module. Therefore, in view of the Structure Theorem of Λ-modules, we can define the μ and λ-invariants, which we denote as $\mu_p(E/F)$ and $\lambda_p(E/F)$, respectively.

Given a number field F, we set F_{cyc} to be the composite of F with $\mathbb{Q}_{\mathrm{cyc}}$. It is the unique $\mathbb{Z}_p$-extension of F which is contained in the infinite cyclotomic field $F(\mu_{p^\infty})$. Given $n \geq 0$,

let F_n be the subfield of F_{cyc} such that $[F_n : F] = p^n$. The following lemma relating the λ-invariant of the Selmer group to the rank of the elliptic curve is well-known but we include it for the sake of completeness.

Lemma 2.2. *Let $E_{/F}$ be an elliptic curve and assume that $\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})$ is cotorsion as a Λ-module, and let $n \geq 0$. Then, $\lambda_p(E/F) \geq \mathrm{rank}_{\mathbb{Z}}(E(F_n))$.*

Proof. Denote by Γ_n the Galois group $\mathrm{Gal}(F_{\mathrm{cyc}}/F_n)$ and let r_n denote the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})^{\Gamma_n}$. Since $\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})$ is cotorsion over the Iwasawa algebra, it has finite $\mathbb{Z}_p$-corank, and it is an easy consequence of the structure theorem that

$$\lambda_p(E/F) = \mathrm{corank}_{\mathbb{Z}_p}\left(\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})\right).$$

We deduce from (2) that

(3) $$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/F_n) \geq \mathrm{rank}_{\mathbb{Z}}(E(F_n)),$$

with equality if $\mathrm{III}(E/F_n)[p^\infty]$ is finite. It follows from the structure theory of Λ-modules that $\lambda_p(E/F_n) \geq r_n$. It suffices to show that $r_n \geq \mathrm{rank}_{\mathbb{Z}}(E(F_n))$. This is indeed the case, since Mazur's Control Theorem asserts that there is a natural map

$$\mathrm{Sel}_{p^\infty}(E/F_n) \to \mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})^{\Gamma_n}$$

with finite kernel. From (3), we see that $r_n \geq \mathrm{rank}_{\mathbb{Z}}(E(F_n))$ and the result follows. $\square$

Let $L/\mathbb{Q}$ be a degree-p Galois extension. The following theorem relates the λ-invariants of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$ and $\mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}})$.

Theorem 2.3. *Let $p \geq 5$ be a fixed prime. Let $L/\mathbb{Q}$ be a Galois extension of degree a power of p disjoint from the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $E_{/\mathbb{Q}}$ be a fixed elliptic curve with good ordinary reduction at p and suppose that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$ is a cofinitely generated $\mathbb{Z}_p$-module. Then, $\mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}})$ is also a cofinitely generated $\mathbb{Z}_p$-module. Moreover, their respective λ-invariants are related by the following formula*

$$\lambda_p(E/L) = p\lambda_p(E/\mathbb{Q}) + \sum_{w \in P_1}\left(e_{L_{\mathrm{cyc}}/\mathbb{Q}_{\mathrm{cyc}}}(w) - 1\right) + 2\sum_{w \in P_2}\left(e_{L_{\mathrm{cyc}}/\mathbb{Q}_{\mathrm{cyc}}}(w) - 1\right)$$

where $e_{L_{\mathrm{cyc}}/\mathbb{Q}_{\mathrm{cyc}}}(w)$ is the ramification index, and P_1, P_2 are sets of primes in L_{cyc} such that

$$P_1 = \left\{w : \ w \nmid p, \ E \text{ has split multiplicative reduction at } w\right\},$$

$$P_2 = \left\{w : \ w \nmid p, \ E \text{ has good reduction at } w, \ E(L_{\mathrm{cyc},w}) \text{ has a point of order } p\right\}.$$

Proof. [HM99, Theorem 3.1]. $\square$

Remark. We remind the reader that a cofinitely generated cotorsion Λ-module M is a cofinitely generated $\mathbb{Z}_p$-module precisely when the associated μ-invariant is 0.

We record the following result which was first proven by Greenberg.

Proposition 2.4. *Let $E_{/\mathbb{Q}}$ be a rank 0 elliptic curve and assume that the Shafarevich–Tate group is finite. Then, for density one good (ordinary) primes, $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$.*

Proof. See [Gre99, Theorem 5.1] or [KR21a, Theorem 3.7].   □

Remark. In [KR21a, Corollary 3.6], it is shown that $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$ is equivalent to the vanishing of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$. This happens when $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 0$, the Tamagawa numbers at the primes of bad reduction of E are not divisible by p, and p is not an anomalous prime in the sense of [Maz72].

2.2. **Results, conjectures, and heuristics on ranks of elliptic curves.** There are several important conjectures in the theory of elliptic curves. The first one of interest is the *rank distribution conjecture* which claims that over any number field, half of all elliptic curves (when ordered by height) have Mordell–Weil rank zero and the remaining half have Mordell–Weil rank one. Finally, higher Mordell–Weil ranks constitute zero percent of all elliptic curves, even though there may exist infinitely many such elliptic curves. Therefore, a suitably-defined *average rank* would be 1/2. The best results in this direction are by M. Bhargava and A. Shankar (see [BS15a, BS15b]). They show that the average rank of elliptic curves over $\mathbb{Q}$ is strictly less than one, and that both rank zero and rank one cases comprise non-zero densities across all elliptic curves over $\mathbb{Q}$ (see [BS13]).

Given an elliptic curve E defined over $\mathbb{Q}$ and base-changed to F, we have the associated Hasse–Weil L function, $L_E(s, F)$. Let $F/\mathbb{Q}$ be an abelian extension with Galois group G and conductor f. Let $\hat{G}$ be the group of Dirichlet characters, $\chi : (\mathbb{Z}/f\mathbb{Z})^\times \to \mathbb{C}^\times$. We further know that

$$L_E(s, F) = \prod_{\chi \in \hat{G}} L_E(s, \chi),$$

where the terms appearing on the right hand side are the L-functions of $E_{/\mathbb{Q}}$ twisted by the character χ.

Conjecture (Birch and Swinnerton-Dyer)**.** *The Hasse–Weil L-function has analytic continuation to the whole complex plane, and*

$$\mathrm{ord}_{s=1} L_E(s, F) = \mathrm{rank}_{\mathbb{Z}}(E(F)).$$

It follows from the BSD Conjecture that the vanishing of the twisted L-functions $L_E(s, \chi)$ at $s = 1$ is equivalent to the existence of rational points of infinite order on $E(F)$.

The following conjecture of David–Fearnley–Kisilevsky predicts that given an elliptic curve over $\mathbb{Q}$, the rank "rarely" jumps in $\mathbb{Z}/p\mathbb{Z}$-extensions with $p \neq 2$. More precisely,

Conjecture ([DFK07, Conjecture 1.2])**.** *Let p be an odd prime and $E_{/\mathbb{Q}}$ be an elliptic curve. Define*

$$N_{E,p}(X) := \#\{\chi \text{ of order } p \mid \mathrm{cond}(\chi) \leq X \text{ and } L_E(1, \chi) = 0\}.$$

(1) If $p = 3$, then as $X \to \infty$

$$\log N_{E,p}(X) \sim \frac{1}{2} \log X.$$

(2) If $p = 5$, then as $X \to \infty$, the set $N_{E,p}(X)$ is unbounded but $N_{E,p}(X) \ll X^\epsilon$ for any $\epsilon > 0$.

(3) If $p \geq 7$, then $N_{E,p}(X)$ is bounded.

Under BSD, $\#N_{E,p}(X)$ can be rewritten as

$$(p-1)\#\{F/\mathbb{Q} \text{ is cyclic of degree } p \mid \mathrm{cond}(F) \leq X \text{ and } \mathrm{rank}_{\mathbb{Z}}(E(F)) > \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))\}.$$

In [Dok07, Theorem 1], T. Dokchitser showed that given an elliptic curve $E_{/\mathbb{Q}}$, there are infinitely many $\mathbb{Z}/3\mathbb{Z}$ extensions where the rank jumps. More recently, B. Mazur and K. Rubin have shown (see [MRL18, Theorem 1.2]) that given an elliptic curve E, there is a positive density set of primes (call it $\mathcal{S}$) such that for each $p \in \mathcal{S}$ there are infinitely many cyclic degree-p extensions over $\mathbb{Q}$ with $\mathrm{rank}_{\mathbb{Z}}(E(L)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. However, the result is unable to provide a positive proportion. Mazur–Rubin revisited this conjecture in a recent preprint (see [MR19]) and their heuristics, based on the distribution of modular symbols, predicts the same statement as the conjecture of David–Fearnley–Kisilevsky.

3. Rank Jump in Degree-p Galois Extensions

Let $E_{/\mathbb{Q}}$ be a rank 0 elliptic curve and p be an odd prime number. In this section, we are interested in studying two questions for a given pair (E, p). First, we analyze in how many (or what proportion of) cyclic degree-p Galois extensions over $\mathbb{Q}$ does the rank of E *not* jump. This question is addressed in Theorem 3.8: for non-CM elliptic curves, the result is unconditional; whereas, for the CM-case we prove the same result under an additional independence hypothesis **Hyp CM**. Next, we study the *dual problem*, i.e., for what proportion of elliptic curves does the rank *not* jump in at least one degree-p Galois extension over $\mathbb{Q}$. This question is discussed in Section 3.2.

Even though such questions have been studied in the past, our approach involving Iwasawa theory is new. Let $E_{/\mathbb{Q}}$ be an elliptic curve with *good ordinary reduction* at a fixed odd prime p. In Lemma 2.2 we showed that over any number field, $\lambda_p(E/F) \geq \mathrm{rank}_{\mathbb{Z}}(E(F))$. It is well-known (see for example, [KR21a, Corollary 3.6]) that if $E_{/\mathbb{Q}}$ is a rank 0 elliptic curve with good (ordinary) reduction at an odd prime p then $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$ if and only if $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}) = 0$. We remind the reader that in Proposition 2.4 we showed that the triviality of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$ is observed *often*. The same statement holds for any number field, under the additional hypothesis that the Shafarevich–Tate group is finite in every layer of its cyclotomic $\mathbb{Z}_p$-extension. Our key idea is to start with a rank 0 elliptic curve $E_{/\mathbb{Q}}$ for which $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$ and count how often is $\mu_p(E/L) = \lambda_p(E/L) = 0$, where $L/\mathbb{Q}$ is a cyclic degree-p extension.

For a number field F, it is possible that $\lambda_p(E/F) > \mathrm{rank}_{\mathbb{Z}}(E(F))$. So, our method fails to measure *all* instances when the rank of the elliptic curve does not change; i.e., our results only provide a lower bound. However, we succeed in answering a stronger question, i.e., how often is the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})$ trivial upon base-change.

3.1. Let $E_{/\mathbb{Q}}$ be a fixed rank 0 elliptic curve of conductor N with good ordinary reduction at a fixed prime $p \geq 5$ such that $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$. Recall that the *rank distribution conjecture* predicts that half of the elliptic curves (ordered by height or conductor) have rank 0. Moreover, Proposition 2.4 asserts that there are density one good ordinary primes satisfying the condition of vanishing Iwasawa invariants. Lastly, when an elliptic curve does

not have complex multiplication (CM), density one of the primes are good ordinary; in the CM case, the good ordinary and the good supersingular primes each have density $1/2$.

Throughout this section, $L/\mathbb{Q}$ denotes a $\mathbb{Z}/p\mathbb{Z}$-extension disjoint from the cyclotomic $\mathbb{Z}_p$-extension. Let q be a prime number distinct from p such that E has good reduction at q, i.e., $\gcd(q, N) = 1$. Let $w|q$ be a prime in L, L_w be the completion at w, and κ be the residue field of characteristic q. We know that there is an exact sequence of abelian groups (see [Sil09, Prop VII.2.1])

$$0 \to E_1(L_w) \to E_0(L_w) \to \widetilde{E}_{\mathrm{ns}}(\kappa) \to 0,$$

where $\widetilde{E}_{\mathrm{ns}}(\kappa)$ is the set of non-singular points of the reduced elliptic curve, $E_0(L_w)$ is the set of points with non-singular reduction, and $E_1(L_w)$ is the kernel of reduction map. Since $p \neq q$, we know that $E_1(L_w)[p]$ is trivial (see [Sil09, VII.3.1]). Because q is assumed to be a prime of good reduction $E_0(L_w) = E(L_w)$. Hence,

$$E(L_w)[p] \simeq \widetilde{E}(\kappa)[p].$$

Since $L/\mathbb{Q}$ is a $\mathbb{Z}/p\mathbb{Z}$-extension, the residue field is either $\mathbb{F}_{q^p}$ or $\mathbb{F}_q$ depending on whether q is inert in the extension or not.

As explained above, (under standard hypothesis) we know that $\lambda_p(E/L) \geq \mathrm{rank}_{\mathbb{Z}}(E(L))$. Since we have assumed that $\mu_p(E/\mathbb{Q}) = 0$, it follows from Theorem 2.3 that $\mu_p(E/L) = 0$. To show that $\lambda_p(E/L) = 0$, it suffices to show that

$$\sum_{w \in P_1} \left(e_{L_{\mathrm{cyc}}/\mathbb{Q}_{\mathrm{cyc}}}(w) - 1 \right) = \sum_{w \in P_2} \left(e_{L_{\mathrm{cyc}}/\mathbb{Q}_{\mathrm{cyc}}}(w) - 1 \right) = 0.$$

Recall that all primes in the cyclotomic $\mathbb{Z}_p$-extension are finitely decomposed and the only primes that ramify are those above p. Moreover, $L \cap \mathbb{Q}_{\mathrm{cyc}} = \mathbb{Q}$ and $p \notin P_1 \cup P_2$ (recall the definition of these sets from Theorem 2.3). Therefore, $e_{L_{\mathrm{cyc}}/\mathbb{Q}_{\mathrm{cyc}}} = e_{L/\mathbb{Q}}$. Since $p \geq 5$, the reduction type does not change upon base-change. In particular, if $q(\neq p)$ is a prime of additive reduction for $E_{/\mathbb{Q}}$, then it has additive reduction over L_{cyc} (see [ST68, p. 498] or [HM99, p. 587]). Finally, since $L_{\mathrm{cyc},w}/L_w$ is a pro-p group we have that $E(L_{\mathrm{cyc},w})[p^{\infty}] = 0$ if and only if $E(L_w)[p^{\infty}] = 0$. Thus, it *suffices* to show that

$$(4) \qquad \sum_{w \in P_1} \left(e_{L/\mathbb{Q}}(w) - 1 \right) = \sum_{w \in P_2} \left(e_{L/\mathbb{Q}}(w) - 1 \right) = 0,$$

where P_1, P_2 are now sets of primes in L. More precisely,

$$P_1 = \left\{ w \in L : w \nmid p, \ E \text{ has split multiplicative reduction at } w \right\},$$

$$P_2 = \left\{ w \in L : w \nmid p, \ E \text{ has good reduction at } w, \ E(L_w) \text{ has a point of order } p \right\}.$$

It is often possible that $P_1 = \emptyset$ but the set P_2 is never empty. In fact, it is known that (see for example [Coj04, §2])

$$(5) \qquad \lim_{X \to \infty} \frac{\#\{q \leq X \mid q \nmid pN, \ p \mid \#\widetilde{E}(\mathbb{F}_q)\}}{\pi(X)} \approx \frac{1}{p}.$$

Here, $\pi(X)$ is the prime counting function.

Remark. Henceforth, the sets P_1, P_2 will denote sets of primes in L (rather than L_{cyc}). By our assumption that $L \cap \mathbb{Q}_{\mathrm{cyc}} = \mathbb{Q}$, we have excluded the case that p is the only ramified prime. If two or more primes are ramified, then it is possible that p is (wildly) ramified in L. But by definition, $p \notin P_1 \cup P_2$. Therefore, the ramification of p in $L/\mathbb{Q}$ does not contribute to the λ-jump. It suffices to focus on the ramification of primes $q \neq p$.

The above discussion can be summarized in the result below.

Proposition 3.1. *Let $E_{/\mathbb{Q}}$ be a rank 0 elliptic curve with good ordinary reduction at $p \geq 5$ such that $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$. Let $L/\mathbb{Q}$ be any cyclic degree-p extension disjoint from $\mathbb{Q}_{\mathrm{cyc}}$ such that (4) holds. Then $\mu_p(E/L) = \lambda_p(E/L) = 0$. This implies in particular that $\mathrm{rank}_{\mathbb{Z}}(E(L_n)) = 0$ for all $n \geq 0$.*

The conditions imposed in Proposition 3.1 will be required throughout this section. Therefore, we make the following definition.

Definition 3.2. Given an elliptic curve $E_{/\mathbb{Q}}$ of rank 0, a prime p is called *irrelevant* if at least one of the following properties hold.
  (i) p is a prime of bad reduction.
  (ii) p is a prime of supersingular reduction.
  (iii) At p, the μ-invariant associated to the p-primary Selmer group is positive.
  (iv) At p, the λ-invariant associated to the p-primary Selmer group is positive.
Otherwise, it is called a *relevant prime*.

Let E be an elliptic curve and let p, q be two distinct primes. Given a triple (E, p, q) we aim to understand when (4) holds. We begin by recalling the following well-known result.

Proposition 3.3. *Let p be an odd prime. Let $L/\mathbb{Q}$ be any $\mathbb{Z}/p\mathbb{Z}$-extension disjoint from the cyclotomic $\mathbb{Z}_p$-extension which is ramified at exactly one prime $q \neq p$. Such an extension exists precisely when $q \equiv 1 \pmod{p}$. Moreover, L is unique and has conductor q.*

Proof. See for example [JR08, Proposition 1.1]. $\qquad\square$

In fact, it follows from class field theory (see [MSM16, Lemma 2.5]) that the primes that ramify in a $\mathbb{Z}/p\mathbb{Z}$-extension are either p or precisely those of the form $q \equiv 1 \pmod{p}$. By local class field theory, the discriminant of $L/\mathbb{Q}$ (denoted $d(L/\mathbb{Q})$) is given by (see [MSM16, Lemma 2.4])

$$d(L/\mathbb{Q}) = \begin{cases} \prod_{i=1}^{r} q_i^{p-1} & \text{if } q_i's \text{ are ramified.} \\ \prod_{i=1}^{r} q_i^{p-1} p^{2(p-1)} & \text{if } q_i's \text{ and } p \text{ are ramified.} \end{cases}$$

If $q(\neq p)$ ramifies in a $\mathbb{Z}/p$-extension then the ramification is tame.

For primes of the form $q \equiv 1 \pmod{p}$ (i.e., primes that can ramify in $\mathbb{Z}/p\mathbb{Z}$-extensions), we introduce the notion of *friendly* and *enemy primes*.

Definition 3.4. Let p be a fixed odd prime and $E_{/\mathbb{Q}}$ be a fixed elliptic curve of rank 0 for which p is a *relevant prime* (see Definition 3.2). Define *enemy primes* to be those primes which are of the form $q \equiv 1 \pmod{p}$ and such that either of the following conditions hold

(i) q is a prime of split multiplicative reduction *or*

(ii) q is a prime of good reduction and $p \mid \#\widetilde{E}(\mathbb{F}_q)$.

If a prime is of the form $q \equiv 1 \pmod{p}$ with the additional properties that q is a prime of good reduction and $p \nmid \#\widetilde{E}(\mathbb{F}_q)$, then q will be called *friendly*.

Remark. (i) A prime $q \equiv 1 \pmod{p}$ which is a prime of bad reduction but not of split multiplicative type is neither an *enemy prime* nor a *friendly prime*.

(ii) For our purpose, it is enough to work with the residue field $\mathbb{F}_q$ because eventually we want the primes q to *ramify* in the extension L.

Primes $w|q$ in L will also be called an *enemy* or a *friendly* prime depending on the behaviour of q. The following lemma will play a crucial role in the subsequent discussion.

Lemma 3.5. *Let $L/\mathbb{Q}$ be a cyclic degree-p extension disjoint from $\mathbb{Q}_{\mathrm{cyc}}$. Then (4) holds precisely when no ramified prime is an* enemy *prime.*

Proof. Recall that P_1 consists of primes $w \nmid p$ such that E *has* split multiplicative reduction at w. Observe that
$$\sum_{w \in P_1} \left(e_{L/\mathbb{Q}}(w) - 1 \right) \neq 0$$
if and only if there exists a ramified prime in $L/\mathbb{Q}$ of split multiplicative type. The assertion is immediate from the definition of an *enemy prime*.

Since L is disjoint from $\mathbb{Q}_{\mathrm{cyc}}$, we know that if p is ramified in $L/\mathbb{Q}$, there must be at least one other prime which is also ramified. Now,
$$\sum_{w \in P_2} \left(e_{L/\mathbb{Q}}(w) - 1 \right) \neq 0$$
precisely when there exists a $q(\neq p)$ satisfying *all* of the following conditions:

(i) q is a prime of good reduction for E,

(ii) q is ramified in the extension $L/\mathbb{Q}$, *and*

(iii) w is a prime above q with $E(L_w)[p] \neq 0$,

The conclusion of the lemma is now straightforward. □

3.1.1. For a given pair (E, p), we denote the set of *enemy primes* by $\mathcal{E}_{(E,p)}$ and the set of *friendly primes* by $\mathcal{F}_{(E,p)}$. Write $\mathcal{N}_{(E,p)}$ for the set of primes of the form $q \equiv 1 \pmod{p}$ where E has bad reduction not of split multiplicative type. The three sets are disjoint. We further subdivide the first two of these sets into disjoint sets, namely
$$\mathcal{F}_{(E,p)} = \mathcal{F}_{(E,p)}^{\mathrm{ord}} \cup \mathcal{F}_{(E,p)}^{\mathrm{ss}} \text{ and}$$
$$\mathcal{E}_{(E,p)} = \mathcal{E}_{(E,p)}^{\mathrm{split}} \cup \mathcal{E}_{(E,p)}^{\mathrm{ord}} \cup \mathcal{E}_{(E,p)}^{\mathrm{ss}}.$$

Here, $\mathcal{F}_{(E,p)}^{\mathrm{ord}}$ (resp. $\mathcal{F}_{(E,p)}^{\mathrm{ss}}$) is the set of primes of the form $q \equiv 1 \pmod{p}$ such that q is a prime of good *ordinary* (resp. *supersingular*) reduction and $p \nmid \#\widetilde{E}(\mathbb{F}_q)$. The set $\mathcal{E}_{(E,p)}^{\mathrm{split}}$ consists of all the primes $q \equiv 1 \mod p$ of split multiplicative reduction. Finally, $\mathcal{E}_{(E,p)}^{\mathrm{ord}}$

(resp. $\mathcal{E}^{\mathrm{ss}}_{(E,p)}$) is the set of primes of the form $q \equiv 1 \pmod{p}$ such that q is a prime of good *ordinary* (resp. *supersingular*) reduction and $p | \# \widetilde{E}(\mathbb{F}_q)$.

Lemma 3.6. *Let $E_{/\mathbb{Q}}$ be an elliptic curve and $p \geq 5$ be a relevant prime. Then, $\mathcal{E}^{\mathrm{ss}}_{(E,p)} = \emptyset$. In particular, $\mathcal{E}_{(E,p)} = \mathcal{E}^{\mathrm{split}}_{(E,p)} \cup \mathcal{E}^{\mathrm{ord}}_{(E,p)}$.*

Proof. When $q \geq 7$ is a prime of supersingular reduction then it follows from the Hasse bound that $a_q = 0$. Therefore,

$$\# \widetilde{E}(\mathbb{F}_q) = q + 1 - a_q = q + 1.$$

Note that we require that $q \equiv 1 \pmod{p}$. Thus, $p \nmid \# \widetilde{E}(\mathbb{F}_q)$. $\qquad\square$

For any subset $\mathcal{S}'$ of the set of primes, let $\mathfrak{d}(\mathcal{S}')$ denote the Dirichlet density of $\mathcal{S}'$. With notation as above, we have that

$$(6) \qquad \mathfrak{d}\left(\mathcal{E}_{(E,p)}\right) + \mathfrak{d}\left(\mathcal{F}_{(E,p)}\right) + \mathfrak{d}\left(\mathcal{N}_{(E,p)}\right) = \frac{1}{\varphi(p)} = \frac{1}{p-1}.$$

The first equality follows from Dirichlet's theorem on primes in arithmetic progressions, which asserts that the proportion of primes that are congruent to 1 modulo p is $1/\varphi(p)$. The set $\mathcal{N}_{(E,p)}$ is finite, hence $\mathfrak{d}\left(\mathcal{N}_{(E,p)}\right) = 0$. We will henceforth disregard the primes q which are of non-split multiplicative and additive reduction type. For the same reason, we may also disregard (for the purpose of proportion) the primes of split multiplicative reduction. As $X \to \infty$, the contribution to $\mathcal{E}_{(E,p)}$ is primarily from primes q such that

(a) q is a prime of good ordinary reduction,
(b) $q \equiv 1 \pmod{p}$, *and*
(c) $p \mid \# \widetilde{E}(\mathbb{F}_q)$.

For non-CM elliptic curves, the set of primes of good ordinary reduction has density 1. In the case of non-CM elliptic curves with surjective residual Galois representation at p, we know how to calculate the proportion of primes satisfying conditions (a)–(c).

Lemma 3.7. *Let $E_{/\mathbb{Q}}$ be a non-CM elliptic curve and $p \geq 5$ be a fixed prime of good ordinary reduction such that the residual Galois representation at p is surjective. Then,*

$$\mathfrak{d}\left(\mathcal{E}_{(E,p)}\right) = \frac{p}{(p-1)^2(p+1)}.$$

Proof. The result is well known and follows from the proof of [GFP20, Proposition 4.6]. For the convenience of the reader, we shall briefly sketch the details here. A more detailed argument is provided in Section 4.2. Since $p \geq 5$, it follows from the proof of Lemma 3.6 that if conditions (b) and (c) are satisfied, then (a) is automatically satisfied for any prime q of good reduction. Since there are only finitely many primes q at which E has bad reduction, we may as well assume that q is a prime of good reduction.

Let Frob_q denote the Frobenius at q and set $\mathcal{S}$ to be the set of matrices $A \in \mathrm{GL}_2(\mathbb{F}_p)$ such that $\mathrm{trace}(A) = 2$ and $\det(A) = 1$. Let $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ denote the residual

representation at p, i.e., the representation on the group of p-torsion points $E[p]$. By assumption, $\bar{\rho}$ is surjective.

Since q is a prime of good reduction, $\bar{\rho}$ is unramified at q and the characteristic polynomial of $\bar{\rho}(\mathrm{Frob}_q)$ is given by

$$\det\left(\mathrm{Id} - T\bar{\rho}(\mathrm{Frob}_q)\right) = T^2 - (q + 1 - \#\tilde{E}(\mathbb{F}_q))T + q.$$

Thus, q is satisfies both conditions (b) and (c) above if and only if $\bar{\rho}(\mathrm{Frob}_q)$ is contained in $\mathcal{S}$. According to Lemma 4.7, the cardinality of $\mathcal{S}$ is p^2. The cardinality of $\mathrm{Image}(\bar{\rho}) = \mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2 - 1)(p^2 - p)$. The result follows from the Chebotarev density theorem, according to which the density of $\mathcal{E}_{(E,p)}$ is

$$\frac{\#\mathcal{S}}{\#\mathrm{GL}_2(\mathbb{F}_q)} = \frac{p}{(p-1)^2(p+1)}.$$

$\square$

We performed calculations using SageMath [Sag20] to get an estimate of the proportion of *enemy primes* in the CM case. More precisely, fix $5 \leq p \leq 50$. Fix an elliptic curve $E_{/\mathbb{Q}}$ of rank 0 and conductor less than 100. Running through all primes q less than 200 million, we computed the proportion of *enemy primes*. The results are recorded at the end of the article, in Table 2. The data suggests that for elliptic curves with CM, the proportion of *enemy primes* is *half* of that in the non-CM case. We know from Deuring's Criterion that for a CM elliptic curve, the density of the set of good ordinary primes is $1/2$. It therefore, seems reasonable to assume that the *enemy primes* are equally likely to be primes of good ordinary or good supersingular reduction. More precisely,

Hyp CM   Let $E_{/\mathbb{Q}}$ be an elliptic curve with CM and p be a fixed odd prime of good ordinary reduction. Then, $\mathfrak{d}\left(\mathcal{E}_{(E,p)}\right) = \frac{p}{2(p-1)^2(p+1)}$.

We can now prove the main result of this section.

Theorem 3.8. *Let (E, p) be a given pair of a rank 0 elliptic curve over $\mathbb{Q}$ and a relevant prime $p \geq 5$. Then the following assertions hold.*

(1) Suppose that the residual representation at p is surjective. Then, there are infinitely many cyclic number fields of degree-p in which the λ-invariant does not jump. In particular, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions $L/\mathbb{Q}$ in which the rank does not jump in L_n for all $n \geq 0$.

(2) Let (E, p) be a pair of rank 0 elliptic curve (defined over $\mathbb{Q}$) with complex multiplication and $p \geq 5$ be a relevant prime. Suppose further that Hyp CM holds. Then the same conclusions hold as in the non-CM case.

Proof. Since p is assumed to be a relevant prime, we know that $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$. It follows from Theorem 2.3 that $\mu_p(E/L) = 0$ for every degree p extension $L/\mathbb{Q}$. The result will follow from Proposition 3.1 if we can show that there are infinitely many cyclic degree p extensions such that (4) holds.

Observe that

$$\mathfrak{d}\left(\mathcal{F}_{(E,p)}\right) = \frac{1}{p-1} - \mathfrak{d}\left(\mathcal{E}_{(E,p)}\right) = \begin{cases} \frac{p^2-p-1}{(p-1)^2(p+1)} & \text{if } E \text{ does not have CM.} \\ \frac{2p^2-p-2}{2(p-1)^2(p+1)} & \text{if } E \text{ does not have CM.} \end{cases}$$

It follows from Lemma 3.5 that (4) holds when every ramified prime is a *friendly prime*. From the above discussion, we see that there are infinitely many *friendly primes*. We have also shown in Proposition 3.3 that corresponding to each *friendly prime* (say q) there is one $\mathbb{Z}/p\mathbb{Z}$-extension where only q ramifies. This completes the proof. $\qquad\square$

Note that the condition in Theorem 3.8, part (1) requiring that the residual representation is surjective implies that the elliptic curve does not have complex multiplication. The Galois representations associated to CM elliptic curves are studied for instance in [LR22]. The following application of our theorem was pointed out by J. Morrow. We begin by stating a result of González-Jiménez–Najman.

Theorem 3.9. *Let $E_{/\mathbb{Q}}$ be an elliptic curve and $p > 7$ be a prime number. Let $L/\mathbb{Q}$ be a Galois extension with Galois group $G \simeq \mathbb{Z}/p\mathbb{Z}$. Then $E(L)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$.*

Proof. See [GJN20, Theorem 7.2]. $\qquad\square$

Combining Theorems 3.8 and 3.9, the following corollary is immediate.

Corollary 3.10. *Let (E, p) be a given pair of rank 0 elliptic curve over $\mathbb{Q}$ and a relevant prime $p > 7$. If $E_{/\mathbb{Q}}$ is an elliptic curve without CM, suppose that the residual representation at p is surjective. If $E_{/\mathbb{Q}}$ is an elliptic curve with CM, suppose that* **Hyp CM** *holds. Then, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$ where the Mordell–Weil group does not grow.*

Remark. To show that there are "infinitely many" $\mathbb{Z}/p\mathbb{Z}$-extensions with no λ-jump, we only counted those where *exactly one friendly prime* is ramified. In particular, we counted only those $\mathbb{Z}/p\mathbb{Z}$-extensions which are contained in the cyclotomic field $\mathbb{Q}(\mu_q)$ where q is a prime of the form 1 (mod p). Our count ignored the contribution from $\mathbb{Z}/p\mathbb{Z}$-extensions where two or more primes are ramified, all of which are either *friendly primes* or the prime p. It was pointed out to us by R. Lemke Oliver that Theorem 3.8 can be made explicit using standard analytic number theory techniques (see for example [Ser74, Théorème 2.4]); however, our approach is still likely to fall short of proving a positive proportion.

A recent and significant result in this direction is by Mazur–Rubin (see [MRL18, Theorem 1.2]). They show that given an elliptic curve E, there is a positive density set of primes (call it $\mathcal{S}$) such that for each $p \in \mathcal{S}$ there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions over $\mathbb{Q}$ with $E(L) = E(\mathbb{Q})$. In the case of rank 0 elliptic curves (defined over $\mathbb{Q}$), our result is stronger, in the sense that for $p > 7$, Corollary 3.10 holds unconditionally for density 1 primes if E is an elliptic curve without CM. On the other hand, for CM elliptic curves, the result is conditional and applies to a set of primes of density 1/2.

3.1.2. *Example: CM case.* Now, we work out a particular example in the CM case. As before, let $p \geq 5$ be a fixed prime and $q \equiv 1 \pmod{p}$ be a different prime. Let $k \not\equiv 0 \pmod{q}$ and consider the family of curves

$$E_k : y^2 = x^3 - kx.$$

Then either of the two statements are true (see [Was08, §4.4]).

(i) If $q \equiv 3 \pmod{4}$, then $\#\widetilde{E_k}(\mathbb{F}_q) = q + 1$.
(ii) If $q \equiv 1 \pmod{4}$, write $q = s^2 + t^2$ with $s \in \mathbb{Z}$, $t \in 2\mathbb{Z}$ and $s + t \equiv 1 \pmod{4}$. Then

$$\#\widetilde{E_k}(\mathbb{F}_q) = \begin{cases} q + 1 - 2s & \text{if } k \text{ is a fourth power mod } q \\ q + 1 + 2s & \text{if } k \text{ is a square mod } q \text{ but not a fourth power} \\ q + 1 \pm 2t & \text{if } k \text{ is not a square mod } q. \end{cases}$$

For this family of elliptic curves, the primes $q \equiv 3 \pmod{4}$ are *supersingular*. Recall from Lemma 3.6 that if q is a supersingular prime and $q \equiv 1 \pmod{p}$ then the primes $w|q$ are *friendly* (except for possibly finitely many). For the sake of concreteness, suppose that $k = 1$ (the argument goes through more generally). By the Chinese Remainder Theorem we know that if

$$q \equiv 3 \pmod{4} \text{ and}$$
$$q \equiv 1 \pmod{p}$$

then, $q \equiv 2p+1 \pmod{4p}$. By Dirichlet's theorem for primes in arithmetic progressions, we know that there are infinitely many primes satisfying this congruence condition. Moreover, the proportion of such primes is

$$\frac{1}{\varphi(4p)} = \frac{1}{2(p-1)}.$$

By Proposition 3.3, we know that corresponding to each such q there is *exactly one* cyclic degree-p extension $L/\mathbb{Q}$ in which q is the unique ramified prime. Therefore, we have produced infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions where the ramified primes are *friendly*. By Proposition 3.1, if $\mathrm{rank}_{\mathbb{Z}}(E_k/\mathbb{Q}) = 0$ and $\mu_p(E/\mathbb{Q}) = 0$ (e.g. when $k = 1$) then there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions over $\mathbb{Q}$ where the rank does *not* jump.

We record a specific case of the above discussion.

Theorem 3.11. *Let $p \geq 5$ be a fixed prime, and consider the elliptic curve*

$$E : y^2 = x^3 - x.$$

Then, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions $L/\mathbb{Q}$ such that $\mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}}) = 0$. In particular, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions such that $\mathrm{rank}_{\mathbb{Z}}(E(L)) = 0$.

3.2. In the last section, we fixed a rank 0 elliptic curve over $\mathbb{Q}$ and analyzed *in how many* $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$ did the rank jump. Now, we ask the following question.

Question. *Let $p \geq 5$ be a fixed odd prime. For what proportion of rank 0 elliptic curves does there exist at least one degree-p Galois extension over $\mathbb{Q}$ disjoint from $\mathbb{Q}_{\mathrm{cyc}}$ such that its rank remains 0 upon base-change?*

Let E be a rank 0 elliptic curve of conductor N and p be a *relevant prime*. Throughout this section we assume that the Shafarevich–Tate group of rank 0 elliptic curves defined over $\mathbb{Q}$ is finite. Proposition 2.4 asserts that density one good ordinary primes are *relevant*. Further assume that N is divisible by at least one prime of the form 1 (mod p). The following lemma is a special case of Proposition 3.1.

Lemma 3.12. *Keep the setting as above. If E has no prime of split multiplicative reduction, i.e., $P_1 = \emptyset$, then there exists at least one degree-p cyclic extension $L/\mathbb{Q}$ such that $\lambda_p(E/L) = 0$. In particular, $\mathrm{rank}_{\mathbb{Z}}(E(L)) = 0$.*

Proof. By Proposition 3.3, there exists one and only one cyclic degree-p extension $L/\mathbb{Q}$ of conductor q if and only if $q \equiv 1 \pmod{p}$. By assumption, N has a prime divisor of this form (say q_0). Let $L/\mathbb{Q}$ be the $\mathbb{Z}/p\mathbb{Z}$-extension of conductor q_0. Moreover, there is no contribution from the last term of the formula in Theorem 2.3; indeed, for any $w \in P_2$ the ramification index is $e_{L/\mathbb{Q}}(w) = 1$. Since L is a $\mathbb{Z}/p\mathbb{Z}$-extension, it follows from Theorem 2.3 that $\mu_p(E/L) = 0$. In this $\mathbb{Z}/p\mathbb{Z}$-extension, we have forced $\lambda_p(E/L) = 0$. Therefore, $\mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}}) = 0$. Clearly, $\mathrm{Sel}_{p^\infty}(E/L)$ is trivial as well; this forces $\mathrm{rank}_{\mathbb{Z}}(E(L)) = 0$. $\square$

It follows from the proof of the above result that to obtain a lower bound of the proportion of rank 0 elliptic curves for which there is *at least one* degree-p cyclic extension over $\mathbb{Q}$ such that $\mathrm{Sel}_{p^\infty}(E/L) = 0$, it is enough to count elliptic curves with the following properties

(i) E has good ordinary reduction at $p \geq 5$.
(ii) E has *any* reduction type at primes $q \not\equiv 1 \pmod{p}$.
(iii) E has at least one prime of bad reduction which is not of split multiplicative type at a prime $q \equiv 1 \pmod{p}$.

Before proceeding with such a count, we need to define the notion of height. For an elliptic curve defined over $\mathbb{Q}$, consider the long Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Define the *height* of this Weierstrass equation with integer coefficients $\boldsymbol{a} = (a_1, a_2, a_3, a_4, a_6)$ to be

$$\mathrm{height}(\boldsymbol{a}) = \max_i \left\{ |a_i|^{1/i} \right\}.$$

Let S be a set of Weierstrass equations with integer coefficients $\boldsymbol{a}$ which are ordered by height. The *proportion of Weierstrass equations which lie in the set S* is defined as

$$(7) \qquad \lim_{X \to \infty} \frac{\# \left\{ \boldsymbol{a} \in S : \mathrm{height}(\boldsymbol{a}) < X \right\}}{\# \left\{ \boldsymbol{a} \in \mathbb{Z}^5 : \mathrm{height}(\boldsymbol{a}) < X \right\}}.$$

For our purposes, we restrict to Weierstrass equations which are globally minimal.

Lemma 3.13. *Let q be any prime. Suppose that all elliptic curves defined over $\mathbb{Q}$ are ordered by height. Then,*

(i) *the proportion with split multiplicative reduction at q is $\frac{q-1}{2q^2}$.*

(ii) *the proportion with good reduction at q is $\left(1 - \frac{1}{q}\right)$.*

Proof. For (i), see [CS21, Theorem 5.1]. For (ii), see [CS21, Proposition 2.2]. $\qquad\square$

Henceforth, we will assume that the rank of the elliptic curve and the reduction type at ℓ are independent of each other. In other words, we will assume that even if we only order the rank 0 elliptic curves by height, the proportion of elliptic curves with split multiplicative reduction or good reduction is the same as that in Lemma 3.13.

We know from [CS21, Section 3] that the local conditions such as the reduction type of elliptic curves at distinct primes are independent.

We now record the assumptions we have made:

Hyp ind   The reduction type of an elliptic curve at a prime q is independent of its rank.

What we mean is that density results from Lemma 3.13 hold even when we restrict to rank 0 elliptic curves defined over $\mathbb{Q}$. We can now prove the main result in this section.

Theorem 3.14. *Let $p \geq 5$ be a fixed odd prime. Suppose that **Hyp ind** holds. Varying over all rank 0 elliptic curves defined over $\mathbb{Q}$ and ordered by height, the proportion with*

(i) *good reduction at p,*
(ii) *any reduction type at $q \not\equiv 1 \pmod{p}$, and*
(iii) *at least one prime of bad reduction where the reduction type is* not *split multiplicative at a prime $q \equiv 1 \pmod{p}$ is given by*

$$(8) \qquad \left(1 - \frac{1}{p}\right)\left(1 - \prod_{q \equiv 1 (mod\ p)}\left(\frac{q-1}{2q^2} + 1 - \frac{1}{q}\right)\right).$$

Further, suppose that the Shafarevich–Tate group is finite for all rank 0 elliptic curves defined over $\mathbb{Q}$. There is a positive proportion of rank 0 elliptic curves for which there is at least one *degree-p cyclic extension over $\mathbb{Q}$ such that $\mathrm{Sel}_{p^\infty}(E/L) = 0$ upon base-change.*

Proof. Let $q \equiv 1 \pmod{p}$. We require that among all such primes there is "at least one prime of bad reduction where the reduction type is *not* split multiplicative". Equivalently, among all primes of the form $1 \pmod{p}$ there is "at least one prime of additive or non-split multiplicative reduction". In other words, at $q \equiv 1 \pmod{p}$ we want the *negation* of "all primes have either good or split multiplicative reduction". This gives (8) from Lemma 3.13.

From our earlier discussion, to prove the second assertion it remains to show that (8) is strictly positive. For any fixed prime p, note that

$$\prod_{q \equiv 1 (\mathrm{mod}\ p)}\left(\frac{q-1}{2q^2} + 1 - \frac{1}{q}\right) = \prod_{q \equiv 1 (\mathrm{mod}\ p)}\left(1 - \left(\frac{q+1}{2q^2}\right)\right) < 1.$$

The inequality follows from the fact that each term in the product is < 1. Therefore,

$$\left(1 - \prod_{q \equiv 1 (\mathrm{mod}\ p)} \left(1 - \left(\frac{q+1}{2q^2}\right)\right)\right) > 0.$$

The claim follows. $\qquad\square$

In Table 1, we compute the expression (8) for $3 \le p < 50$ and $q \le 179,424,673$ (i.e., the first 10 million primes).

A reasonable question to ask at this point is the following.

Question. *Let $p \ge 5$ be a fixed prime and $L/\mathbb{Q}$ be a fixed $\mathbb{Z}/p\mathbb{Z}$-extension. Varying over all rank 0 elliptic curves over $\mathbb{Q}$ ordered by height, for what proportion is $\mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}}) = 0$?*

In this direction, we can provide partial answers. Given a number field $L/\mathbb{Q}$, we can find a lower bound for the proportion of elliptic curves (defined over $\mathbb{Q}$) for which (4) holds.

Proposition 3.15. *Let p be a fixed odd prime. Let $L/\mathbb{Q}$ be a fixed $\mathbb{Z}/p\mathbb{Z}$-extension which is tamely ramified at primes $q_1, \ldots, q_r$. The proportion of elliptic curves defined over $\mathbb{Q}$ (ordered by height) such that (4) holds has a lower bound of*

$$\prod_{q_i=1}^{r} \left(\frac{q_i+1}{2q_i^2}\right).$$

Proof. Note that for (4) to hold, the reduction type at p does not matter. To find a lower bound, it suffices that *all* the ramified primes (i.e., the q_i's) are primes of bad reduction of non-split multiplicative or additive reduction type. Indeed, this would ensure $P_1 = \emptyset$ and the primes of good reduction are not ramified. Equivalently, each q_i is such that it does *not* have good ordinary or split multiplicative reduction. By Lemma 3.13, the lower bound is

$$\prod_{q_i=1}^{r} \left(1 - \left(\frac{q_i-1}{2q_i^2} + 1 - \frac{1}{q_i}\right)\right) = \prod_{q_i=1}^{r} \left(\frac{q_i+1}{2q_i^2}\right).$$

$\qquad\square$

Remark. The above proposition is not sufficient to answer the question because given p, we are unable compute the proportion of elliptic curves for which p is *relevant*. In particular, we do not know precisely for what proportion of elliptic curves is p a good *ordinary* prime. A lower bound for this proportion has been computed for small primes and can be found in [KR21b, Table 1]. From the Hasse interval, one may conclude (roughly) that supersingular elliptic curves should be rare among elliptic curves with good reduction over $\mathbb{F}_p$ (approx. $\frac{1}{2\sqrt{p}}$). Therefore, as p becomes large, 100% of the elliptic curves with good reduction at p is of ordinary type (see [Bir68]). It is also reasonable to expect that as p becomes large, the proportion of rank 0 elliptic curves with $\mu_p(E/\mathbb{Q}) = \lambda_p(E/\mathbb{Q}) = 0$ approaches 100% (see [KR21a, Conjecture 4.7]). Thus, assuming the rank distribution conjecture, it might be reasonable to expect that as p becomes large, varying over all elliptic curves ordered by height, the proportion with good ordinary reduction at p approaches $\frac{1}{2}\left(1 - \frac{1}{2\sqrt{p}}\right)\left(1 - \frac{1}{p}\right)$.

4. Growth of the Selmer group of an elliptic curve in a $\mathbb{Z}/p\mathbb{Z}$-extension

Throughout this section, $p \geq 5$ is a fixed prime number and $E_{/\mathbb{Q}}$ an elliptic curve with good ordinary reduction at p for which the following equivalent conditions are satisfied

(i) $\mu_p(E/\mathbb{Q}) = 0$ and $\lambda_p(E/\mathbb{Q}) = 0$,
(ii) $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}}) = 0$.

Let L be a $\mathbb{Z}/p\mathbb{Z}$-extension of $\mathbb{Q}$. First, in Proposition 4.1, we establish a criterion for there to be either a rank-jump or growth in the Shafarevich–Tate group. The result also explores conditions under which the Selmer group

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 0 \text{ and } \mathrm{Sel}_{p^\infty}(E/L) \neq 0.$$

This result will then be applied to study a problem in arithmetic statistics which we prove in Theorem 4.8.

4.1. Here, we first prove a criterion for non-triviality of the p-primary Selmer group.

Proposition 4.1. *Let p be an odd prime and $L/\mathbb{Q}$ be a $\mathbb{Z}/p\mathbb{Z}$-extension linearly disjoint from $\mathbb{Q}_{\mathrm{cyc}}$. In other words, $L \neq \mathbb{Q}_1$, where $\mathbb{Q}_1$ is the first layer in the cyclotomic $\mathbb{Z}_p$-extension. Let $E_{/\mathbb{Q}}$ be an elliptic curve with good ordinary reduction at p and Σ_L be the set of primes $\ell \neq p$ that are ramified in L. Assume that the following conditions are satisfied*

(i) $\mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ and $E(\mathbb{Q})[p^\infty] = 0$,
(ii) $\mu_p(E/\mathbb{Q}) = 0$ and $\lambda_p(E/\mathbb{Q}) = 0$,
(iii) there is a prime $\ell \in \Sigma_L$ at which E has good reduction and $p | \# \widetilde{E}(\mathbb{F}_\ell)$,
(iv) at each prime $\ell \in \Sigma_L$ at which E has bad reduction, the Kodaira-type of $E_{/\mathbb{Q}_\ell}$ is not I_m for any integer $m \in \mathbb{Z}_{\geq 1}$,
(v) $\text{Ш}(E/L)[p^\infty]$ is finite.

Then, $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \text{Ш}(E/\mathbb{Q})[p^\infty] = 0$ and at least one of the following is true

(a) $\mathrm{rank}_{\mathbb{Z}} E(L) > 0$,
(b) $\text{Ш}(E/L)[p^\infty] \neq 0$.

In particular, the Selmer group $\mathrm{Sel}_{p^\infty}(E/L)$ becomes non-zero.

Remark. Condition (iv) above is automatically satisfied when E has good reduction at all primes $\ell \in \Sigma_L$. In a preprint from 2014, J. Brau has made an attempt at a comparable result on the growth of Selmer groups (see [Bra14, Corollary 1.3]). Our methods differ significantly from those of Brau and do not require the semi-stability hypothesis.

In order to prove the above result, we briefly recall some key properties of the Euler characteristic associated to an elliptic curve. The reader is referred to [CS00, RS19, RS20] for a more comprehensive discussion of the topic.

Let $E_{/\mathbb{Q}}$ be an elliptic curve and $L/\mathbb{Q}$ a number field extension. Assume that the following conditions are satisfied.

(i) $\mathrm{rank}_{\mathbb{Z}} E(L) = 0$,
(ii) E has good ordinary reduction at p,
(iii) $\text{Ш}(E/L)[p^\infty]$ is finite.

Then, the cohomology groups $H^i\left(L_{\mathrm{cyc}}/L, \mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}})\right)$ are finite and the *Euler charac-teristic* $\chi\left(L_{\mathrm{cyc}}/L, E[p^\infty]\right)$ is defined as follows

$$\chi\left(L_{\mathrm{cyc}}/L, E[p^\infty]\right) := \frac{\#H^0\left(L_{\mathrm{cyc}}/L, \mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}})\right)}{\#H^1\left(L_{\mathrm{cyc}}/L, \mathrm{Sel}_{p^\infty}(E/L_{\mathrm{cyc}})\right)}.$$

The Euler characteristic is an important invariant associated to the Selmer group, and captures its key Iwasawa theoretic properties. There is an explicit formula for this invariant, which we now describe. At each prime $v \nmid p$ of L, let $c_v(E/L)$ denote the Tamagawa number at v, and let $c_v^{(p)}(E/L)$ be the p-part, given by $c_v^{(p)}(E/L) := |c_v(E/L)|_p^{-1}$. Here $|\cdot|_p$ is the absolute value, normalized by $|p|_p = p^{-1}$. At each prime v of L, let k_v be the residue field at v, and $\widetilde{E}(k_v)$ be the group of k_v-valued points of the reduction of E at v.

Theorem 4.2. *Let $E_{/\mathbb{Q}}$ be an elliptic curve, p an odd prime, and $L/\mathbb{Q}$ be a number field extension. Assume that the following conditions are satisfied*

(i) $\mathrm{rank}_{\mathbb{Z}} E(L) = 0$,

(ii) E *has good ordinary reduction at* p,

(iii) $\mathrm{III}(E/L)[p^\infty]$ *is finite.*

Then, the following assertions hold:

(a) the Euler characteristic $\chi\left(L_{\mathrm{cyc}}/L, E[p^\infty]\right)$ is an integer; further, it is a power of p,

(b) the Euler characteristic is given by the following formula

$$(9) \qquad \chi\left(L_{\mathrm{cyc}}/L, E[p^\infty]\right) = \frac{\#\mathrm{III}(E/L)[p^\infty] \times \prod_v c_v^{(p)}(E/L) \times \prod_{v|p}\left(\#\widetilde{E}(k_v)[p^\infty]\right)^2}{\left(\#E(L)[p^\infty]\right)^2}.$$

Proof. The assertion (a) follows from [HKR21, Lemma 3.4 and Remark 3.5], and for (b), the reader is referred to [CS00, Theorem 3.3]. $\square$

The next result relates the Euler characteristic and Iwasawa invariants.

Proposition 4.3. *Let $E_{/L}$ be an elliptic curve satisfying the following conditions:*

(i) E *has good ordinary reduction at all primes* $v|p$,

(ii) $\mathrm{rank}_{\mathbb{Z}} E(L) = 0$,

(iii) $\mathrm{III}(E/L)[p^\infty]$ *is finite.*

Then, the following are equivalent

(a) $\mu_p(E/L) = 0$ *and* $\lambda_p(E/L) = 0$,

(b) $\chi(L_{\mathrm{cyc}}/L, E[p^\infty]) = 1$.

Proof. The conditions on the elliptic curve are in place in order for the Euler characteristic to be defined. The result follows from [HKR21, Proposition 3.6]. However, the first proof of this result was given in [RS19], in a more general context. $\square$

Lemma 4.4. *Let $E_{/\mathbb{Q}}$ be an elliptic curve which satisfies the following conditions*

(i) E *has good ordinary reduction at* p,

(ii) $\text{III}(E/\mathbb{Q})[p^\infty]$ is finite,
(iii) $\text{rank}_\mathbb{Z} E(\mathbb{Q}) = 0$,
(iv) $E(\mathbb{Q})[p^\infty] = 0$,
(v) $\mu_p(E/\mathbb{Q}) = 0$ and $\lambda_p(E/\mathbb{Q}) = 0$.
Then, we have that $\text{Sel}_{p^\infty}(E/\mathbb{Q}) = \text{III}(E/\mathbb{Q})[p^\infty] = 0$.

Proof. Recall the well-known short exact sequence (see 2),

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \text{Sel}_{p^\infty}(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[p^\infty] \to 0.$$

Since the $E(\mathbb{Q})$ is finite and $E(\mathbb{Q})[p^\infty] = 0$, it follows from the above that

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}) = \text{III}(E/\mathbb{Q})[p^\infty].$$

It follows from Proposition 4.3 that $\chi(\mathbb{Q}_{\text{cyc}}/\mathbb{Q}, E[p^\infty]) = 1$. On the other hand, by (9),

$$\chi\left(\mathbb{Q}_{\text{cyc}}/\mathbb{Q}, E[p^\infty]\right) = \#\text{III}(E/\mathbb{Q})[p^\infty] \times \prod_\ell c_\ell^{(p)}(E/\mathbb{Q}) \times \left(\#\widetilde{E}(\mathbb{F}_p)[p^\infty]\right)^2.$$

As a result, it is indeed the case the $\text{III}(E/\mathbb{Q})[p^\infty] = 0$.   □

Lemma 4.5. *Let $p \geq 5$ be a prime, $L/\mathbb{Q}$ be a $\mathbb{Z}/p\mathbb{Z}$ extension, and $\ell \neq p$ be a prime which ramifies in L. Assume that the Kodaira type of $E_{/\mathbb{Q}_\ell}$ is not I_m for any integer $m \in \mathbb{Z}_{\geq 1}$. Then, $\prod_{v|\ell} c_v^{(p)}(E/L) = 1$.*

Proof. Since $\ell \neq p$, and $L/\mathbb{Q}$ is a $\mathbb{Z}/p\mathbb{Z}$-extension, it follows that ℓ is tamely ramified in L. Thus, the results for base-change of Tamagawa numbers in [Kid03, Table 1, pp. 556-557] apply. Fix a prime $v|\ell$ and let $e = e_{L/\mathbb{Q}}(v)$ be the ramification index. Since it is assumed that ℓ is ramified in L, it follows that $e = p$. Since $p \geq 5$, the Tamagawa number $c_v^{(p)}(E/L) \neq 1$ if and only if the Kodaira type of $E_{/L_v}$ is I_n for an integer $n \in \mathbb{Z}_{\geq 1}$ that is divisible by p (see [Sil09, p. 448]). According to *loc. cit.*, the only way this is possible is if the Kodaira type of $E_{/\mathbb{Q}_\ell}$ is I_m for $m \in \mathbb{Z}_{\geq 1}$. Indeed, if the Kodaira type of $E_{/\mathbb{Q}_\ell}$ is I_m, then upon base-change to L_v, it becomes $I_{me} = I_{mp}$. However, by assumption, this case does not occur. Therefore, $c_v^{(p)}(E/L) = 1$ for all primes $v|\ell$ of L. This completes the proof.   □

We now give a proof of Proposition 4.1.

proof of Proposition 4.1. According to Lemma 4.4, we have that

$$\text{Sel}_{p^\infty}(E/\mathbb{Q}) = \text{III}(E/\mathbb{Q})[p^\infty] = 0.$$

Assume by way of contradiction that

$$\text{rank}_\mathbb{Z} E(L) = 0 \text{ and } \text{III}(E/L)[p^\infty] = 0.$$

Since $\text{rank}_\mathbb{Z} E(L) = 0$, it follows from Theorem 4.2 that the Euler characteristic $\chi(L_{\text{cyc}}/L, E[p^\infty])$ is defined and given by the formula

$$(10) \qquad \chi\left(L_{\text{cyc}}/L, E[p^\infty]\right) = \frac{\#\text{III}(E/L)[p^\infty] \times \prod_v c_v^{(p)}(E/L) \times \prod_{v|p}\left(\#\widetilde{E}(k_v)[p^\infty]\right)^2}{\left(\#E(L)[p^\infty]\right)^2}.$$

On the other hand, the Euler characteristic $\chi\left(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E[p^\infty]\right)$ is given by the formula

$$\chi\left(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E[p^\infty]\right) = \#\mathrm{III}(E/\mathbb{Q})[p^\infty] \times \prod_\ell c_\ell^{(p)}(E/\mathbb{Q}) \times \left(\#\widetilde{E}(\mathbb{F}_p)[p^\infty]\right)^2.$$

Note that $E(\mathbb{Q})[p^\infty]$ does not contribute to the above formula since it is assumed to be trivial. Since it is assumed that $\mu_p(E/\mathbb{Q}) = 0$ and $\lambda_p(E/\mathbb{Q}) = 0$, it follows from Proposition 4.3 that $\chi\left(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E[p^\infty]\right) = 1$.

We shall use this, and the assumptions on E to show that $\chi\left(L_{\mathrm{cyc}}/L, E[p^\infty]\right) = 1$ as well. Since $\chi\left(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E[p^\infty]\right) = 1$, it follows that

$$\#\mathrm{III}(E/\mathbb{Q})[p^\infty] = 1, \ \prod_\ell c_\ell^{(p)}(E/\mathbb{Q}) = 1, \ \text{and} \ \#\widetilde{E}(\mathbb{F}_p)[p^\infty] = 1.$$

In order to show that $\chi\left(L_{\mathrm{cyc}}/L, E[p^\infty]\right) = 1$, we show that

$$\#\mathrm{III}(E/L)[p^\infty] = 1, \ \prod_v c_v^{(p)}(E/L) = 1, \ \text{and} \ \prod_{v|p} \#\widetilde{E}(k_v)[p^\infty] = 1.$$

By assumption, $\mathrm{III}(E/L)[p^\infty] = 0$, and hence, $\#\mathrm{III}(E/L)[p^\infty] = 1$. It follows from Lemma 4.5 that $\prod_{v|p} c_v^{(p)}(E/L) = 1$. If p splits or ramifies in L, then $k_v = \mathbb{F}_p$ for all primes $v|p$. Since $\#\widetilde{E}(\mathbb{F}_p)[p^\infty] = 1$, it follows that $\#\widetilde{E}(k_v)[p^\infty] = 1$ as well. On the other hand, suppose p is inert in L and $v|p$ is the only prime above p in L. Then, since $k_v/\mathbb{F}_p$ is a p-extension, it follows from [NSW13, Proposition 1.6.12] that

$$\#\widetilde{E}(\mathbb{F}_p)[p^\infty] = 1 \Rightarrow \#\widetilde{E}(k_v)[p^\infty] = 1.$$

Hence, the numerator of (10) is 1. Theorem 4.2 asserts the Euler characteristic is an integer, and so, we deduce that $\chi(L_{\mathrm{cyc}}/L, E[p^\infty]) = 1$. We deduce from Proposition 4.3 that

$$\mu_p(E/L) = 0 \ \text{and} \ \lambda_p(E/L) = 0.$$

In particular, we find that

$$\lambda_p(E/L) = \lambda_p(E/\mathbb{Q}) = 0.$$

On the other hand, recall that according to Kida's formula

$$\lambda_p(E/L) = p\lambda_p(E/\mathbb{Q}) + \sum_{w \in P_1}\left(e_{L/\mathbb{Q}}(w/\ell) - 1\right) + \sum_{w \in P_2} 2\left(e_{L/\mathbb{Q}}(w/\ell) - 1\right).$$

However, there is a prime $\ell \in \Sigma_L$ for which E has good reduction at ℓ and $p|\#\widetilde{E}(\mathbb{F}_\ell)$, we deduce that

$$\sum_{w \in P_2} 2\left(e_{L/\mathbb{Q}}(w/\ell) - 1\right) > 0.$$

Thus, from the above formula shows that

$$\lambda_p(E/L) > \lambda_p(E/\mathbb{Q}).$$

In particular, $\lambda_p(E/L) > 0$, this is a contradiction. Therefore, we have shown that either $\mathrm{rank}_{\mathbb{Z}} E(L) > 0$ or $\mathrm{III}(E/L)[p^\infty] \neq 0$. $\qquad\square$

We illustrate Proposition 4.1 through an example in the case when $p = 5$.

Example: Let $L/\mathbb{Q}$ be the unique degree 5 Galois extension contained in $\mathbb{Q}(\mu_{31})$. The only prime that ramifies in L is $\ell = 31$. Consider the elliptic curve $E : y^2 = x^3 + 42$. Explicit calculation shows that E satisfies conditions (i)-(iv) of the aforementioned proposition. Assuming the finiteness of the Shafarevich–Tate group over L, we conclude that either there is a rank jump, or an increase in the size of the Shafarevich–Tate group. It can be checked via standard computations on `Magma` that $E(L) = E(\mathbb{Q})$. Therefore, the growth occurs in the Shafarevich–Tate group.

4.2.   We now come to an application to arithmetic statistics. Recall that we have fixed an elliptic curve $E_{/\mathbb{Q}}$ and a prime p for which the aforementioned conditions are satisfied. Consider the family of $\mathbb{Z}/p\mathbb{Z}$-extensions L of $\mathbb{Q}$ not contained in $\mathbb{Q}_{\mathrm{cyc}}$ and ramified at precisely one prime. For each prime $q \equiv 1 \pmod{p}$, there is exactly one such extension $L_q/\mathbb{Q}$, which is ramified at q (see 3.3). Note that L_q is contained in $\mathbb{Q}(\mu_q)$. For $X > 0$, let $\pi(X)$ be the prime counting function (i.e., denote the number of primes $q \le X$) and $\pi'(X)$ be the number of primes $q \le X$ for which

  (i) $q \equiv 1 \pmod{p}$ *and*
  (ii) $\mathrm{Sel}_{p^\infty}(E/L_q) \ne 0$.

Note that since $L_q/\mathbb{Q}$ is a $\mathbb{Z}/p\mathbb{Z}$-extension, we have the following implication

$$E(\mathbb{Q})[p^\infty] = 0 \Rightarrow E(L_q)[p^\infty] = 0,$$

see [NSW13, Proposition 1.6.12]. Therefore, the non-vanishing of $\mathrm{Sel}_{p^\infty}(E/L_q)$ is equivalent to at least one of the following conditions being satisfied

(1) $\mathrm{rank}_{\mathbb{Z}} E(L_q) > 0$,
(2) $\text{Ш}(E/L_q)[p^\infty] \ne 0$.

Thus, if the Selmer group becomes non-zero after base-change, then, either there is a rank jump, or the Shafarevich-Tate group witnesses growth. The main result of this section is Theorem 4.8, where it is shown that the set of primes $q \equiv 1 \pmod{p}$ for which the above conditions are satisfied is cut out by explicit Chebotarev conditions. In other words, there is an explicit subset $\mathcal{S} \subset \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ such that for any prime $q \ne p$ coprime to the conductor of E,

$$\mathrm{Frob}_q \in \mathcal{S} \Rightarrow \mathrm{Sel}_{p^\infty}(E/L_q) \ne 0.$$

Which is to say that if the Frobenius of a prime $q \nmid Np$ lies in the Chebotarev set $\mathcal{S}$, then, the Selmer group becomes non-zero when base changed to L_q. We calculate the size of $\mathcal{S}$ and apply the Chebotarev Density Theorem to obtain a lower bound for $\limsup_{X \to \infty} \pi'(X)/\pi(X)$. Said differently, we are able to show there is growth in the Selmer group in L_q for a positive density set of primes q. Let $\bar\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ be the Galois representation on $E[p]$. We make the simplifying assumption that $\bar\rho$ is surjective. By the well-known open image theorem of Serre, this assumption is satisfied for all but finitely many primes p, as long as E does not have complex multiplication. Let $\mathbb{Q}(E[p])$ be the Galois extension of $\mathbb{Q}$ which is fixed by $\ker \bar\rho$. We identify $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ with its image under $\bar\rho$, which according to our assumption is all of $\mathrm{GL}_2(\mathbb{F}_p)$. Let $N = N_E$ be the conductor of E. If q is a prime

which is coprime to Np, then q is unramified in $\mathbb{Q}(E[p])$. Set $a_q(E) := q + 1 - \#\widetilde{E}(\mathbb{F}_q)$; then the characteristic polynomial of $\bar{\rho}(\text{Frob}_q)$ is $x^2 - a_q x + q$. Let $\mathcal{S}$ consist of elements $\sigma \in \text{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ such that

$$\text{trace } \bar{\rho}(\sigma) = 2 \text{ and } \det \bar{\rho}(\sigma) = 1.$$

We arrive at the following useful criterion for p to divide $\#\widetilde{E}(\mathbb{F}_q)$.

Lemma 4.6. *Let $q \nmid Np$ be a prime. Then, the following conditions are equivalent*

(i) $q \equiv 1 \pmod{p}$ *and p divides* $\#\widetilde{E}(\mathbb{F}_q)$,
(ii) $\text{Frob}_q \in \mathcal{S}$.

Proof. Since $\det \bar{\rho}(\text{Frob}_q) = q$, we find that $\det \bar{\rho}(\text{Frob}_q) = 1$ if and only if $q \equiv 1 \pmod{p}$. Assume that these equivalent conditions are satisfied. Note that p divides $\#\widetilde{E}(\mathbb{F}_q)$ if and only if $q + 1 - \text{trace}\left(\bar{\rho}(\text{Frob}_q)\right) = 0$. Since $q \equiv 1 \pmod{p}$, it follows that p divides $\#\widetilde{E}(\mathbb{F}_q)$ if and only if $\text{trace}\left(\bar{\rho}(\text{Frob}_q)\right) = 2$. $\square$

Lemma 4.7. *The cardinality of $\mathcal{S}$ is p^2.*

Proof. Since $\bar{\rho}$ is assumed to be surjective, we identify $\mathcal{S}$ with the set of all matrices in $\text{GL}_2(\mathbb{F}_p)$ with trace 2 and determinant 1. These matrices are all of the form $g = \begin{pmatrix} a & b \\ c & 2-a \end{pmatrix}$, where $a(2-a) - bc = 1$. We count the number of of such matrices. Rewrite the equation as $bc = -1 + a(2-a) = -(a-1)^2$. For each choice of a such that $a \neq 1$, the number of solutions is $(p-1)$. For $a = 1$, either $b = 0$ or $c = 0$, or both. Thus the number of solutions for $a = 1$ is $2p - 1$. Putting it all together,

$$\#\mathcal{S} = (p-1)^2 + (2p-1) = p^2.$$

$\square$

We now prove Theorem B, which is the main result of this section.

Theorem 4.8. *Let $p \geq 5$ be a fixed prime and $E_{/\mathbb{Q}}$ an elliptic curve for which the following conditions are satisfied*

(i) *E has good ordinary reduction at p,*
(ii) $\text{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ *and* $E(\mathbb{Q})[p^\infty] = 0$,
(iii) $\mu_p(E/\mathbb{Q}) = 0$ *and* $\lambda_p(E/\mathbb{Q}) = 0$,
(iv) *the image of the residual representation $\bar{\rho}$ is surjective.*

For $X > 0$, let $\pi'(X)$ be the number of primes $q \equiv 1 \pmod{p}$ for which the following equivalent conditions are satisfied

(i) $\text{Sel}_{p^\infty}(E/L_q) \neq 0$,
(ii) *Either, $\text{rank}_{\mathbb{Z}} E(L_q) > 0$ or $\text{Ш}(E/L_q)[p^\infty] \neq 0$ (or both conditions are satisfied).*

Then,

$$\limsup_{X \to \infty} \frac{\pi'(X)}{\pi(X)} \geq \frac{p}{(p-1)^2(p+1)}.$$

Proof. Let q be a prime such that $q \nmid Np$. It follows from Lemma 4.6 that if $\mathrm{Frob}_q \in \mathcal{S}$, then $q \equiv 1 \pmod{p}$ and $p | \#E(\mathbb{F}_q)$. Note that $\Sigma_{L_q} = \{q\}$ and E has good reduction at q. Since $p | \#E(\mathbb{F}_q)$, it follows from that Proposition 4.1 that $\mathrm{Sel}_{p^\infty}(E/L_q) \neq 0$. Therefore, by the Chebotarev Density Theorem, and Lemma 4.7,

$$\limsup_{X \to \infty} \frac{\pi'(X)}{\pi(X)} \geq \frac{\#\mathcal{S}}{\#\left(\mathrm{GL}_2(\mathbb{F}_p)\right)} = \frac{p^2}{(p^2-1)(p^2-p)} = \frac{p}{(p-1)^2(p+1)}.$$

$\square$

5. Growth of Shafarevich–Tate groups in cyclic extensions

In this section, we study the growth of the Shafarevich–Tate group. First, when $p = 2$ we prove an effective version of Matsuno's theorem (see Theorem 5.4).

When $p \neq 2$, it was shown by Clark and Sharif (see [CS10, Theorem 3]) that there exists a degree-p extension over $\mathbb{Q}$, not necessarily Galois such that the p-rank of the Shafarevich–Tate group becomes arbitrarily large. We study the possibility of improving this result to Galois degree-p extensions.

Definition 5.1. Let p be any prime. Fix an elliptic curve $E_{/\mathbb{Q}}$ with good reduction at p. Let $K/\mathbb{Q}$ be a cyclic degree-p extension. Define the set $T_{E/K}$ to be the set of primes in K above $\ell(\neq p)$ satisfying either of the following properties

   (i) ℓ is a prime of good reduction of E which is ramified in $K/\mathbb{Q}$ and $E(\mathbb{Q}_\ell)$ contains an element of order p.
   (ii) ℓ is a prime of split multiplicative reduction which is inert in $K/\mathbb{Q}$ and the Tamagawa number c_ℓ is divisible by p.

Definition 5.2. Let G be an abelian group. Define the *p-rank* of G as

$$\mathrm{rank}_p(G) = \mathrm{rank}_p(G[p]) := \dim_{\mathbb{F}_p}\left(G[p]\right).$$

The following lemma plays a key role in answering questions pertaining to both sections.

Lemma 5.3. *With notation as above,*

$$\mathrm{rank}_p \mathrm{Sel}_p(E/K) \geq \#T_{E/K} - 4.$$

Proof. See [Mat09, Proposition 4.3]. $\square$

5.1. **Large 2-rank of the Shafarevich–Tate group in quadratic extensions.** Given an elliptic curve $E_{/\mathbb{Q}}$, it is known that the 2-part of the Shafarevich–Tate group becomes arbitrarily large over *some* quadratic extension. More precisely,

Theorem 5.4. *Given an elliptic curve $E_{/\mathbb{Q}}$ and a non-negative integer n, there exists a quadratic number field $K/\mathbb{Q}$ such that $\dim_{\mathbb{F}_2} \mathrm{III}(E/K)[2] \geq n$.*

Proof. See [Mat09, Proposition B]. $\square$

A reasonable question to ask is whether the above result can be made effective, i.e.,

Question. *Given an elliptic curve $E_{/\mathbb{Q}}$ and a fixed non-negative integer n, varying over all quadratic number fields ordered by conductor, what is the minimal conductor of a number field such that one can guarantee $\mathrm{III}(E/K)[2] \geq n$?*

5.1.1. *Reviewing the proof of Matsuno's construction.* In this section, we briefly review the proof of Matsuno's theorem, for details we refer the reader to the original article [Mat09]. Fix an elliptic curve $E_{/\mathbb{Q}}$ of conductor $N = N_E$. Let $K/\mathbb{Q}$ be a quadratic extension. Let S be a finite set of primes in $\mathbb{Q}$ containing precisely the prime number 2, the primes of bad reduction of E, and the archimedean primes.

Let $\ell_1, \ldots, \ell_k$ be odd rational primes that are coprime to N and split completely in $\mathbb{Q}(E[2])/\mathbb{Q}$. Recall that $\mathbb{Q}(E[2])/\mathbb{Q}$ is a Galois extension with Galois group isomorphic to either $\mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z}$ or S_3. By the Chebotarev Density Theorem there is a positive proportion of primes that split completely in $\mathbb{Q}(E[2])/\mathbb{Q}$. Having picked the primes $\ell_1, \ldots, \ell_k$, it is clear that there exists a quadratic extension $K/\mathbb{Q}$ such that the chosen primes ramify. However, more is true. Results of J.-L. Waldspurger (see [BFH90, Theorem in Section 0]) and V. Kolyvagin (see [Kol89]) guarantee the existence of $K/\mathbb{Q}$ such that the chosen primes ramify *and* the Mordell–Weil rank of $E'(\mathbb{Q})$ is 0 where E' is the quadratic twist of E corresponding to K. It follows that

$$\mathrm{rank}_{\mathbb{Z}}(E(K)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + \mathrm{rank}_{\mathbb{Z}}(E'(\mathbb{Q})) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})).$$

Observe that the primes $\ell_1, \ldots, \ell_k$ are primes of good ordinary reduction that lie in $T_{E/K}$. Therefore, it follows from Lemma 5.3 that

$$\mathrm{rank}_2 \, \mathrm{Sel}_2(E/K) \geq k - 4.$$

Using the Kummer sequence, we see that

(11)
$$\mathrm{rank}_2 \, \mathrm{III}(E/K)[2] \geq \mathrm{rank}_2 \, \mathrm{Sel}_2(E/K) - \mathrm{rank}_{\mathbb{Z}}(E/K) - 2$$
$$\geq k - 6 - \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})).$$

Even though the results of Waldspurger and Kolyvagin guarantee that there exists a quadratic extension $K/\mathbb{Q}$ with the desired properties, it is not easy to determine all the primes which ramify in K. Using the proof of Matsuno as our inspiration, combined with more recent results of K. Ono we will prove an effective version of the theorem in Section 5.1.3. Assuming Goldfeld's Conjecture, we prove an effective version using simpler arguments in Section 5.1.2.

5.1.2. *Effective version conditional on Goldfeld's conjecture.* Let us begin by reminding the reader of Goldfeld's Conjecture. This conjecture predicts that given an elliptic curve, 50% of the quadratic twists have rank 0 and 50% of the quadratic twists have rank 1. Therefore, if Goldfeld's Conjecture is true then a 100% of the time, the Mordell–Weil rank of $E'(\mathbb{Q})$ is either 0 or 1, where E' is the quadratic twist of E (corresponding to a quadratic field K). Since

$$\mathrm{rank}_{\mathbb{Z}}(E(K)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + \mathrm{rank}_{\mathbb{Z}}(E'(\mathbb{Q})),$$

for a 100% of the time $\mathrm{rank}_{\mathbb{Z}}(E(K)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ or $\mathrm{rank}_{\mathbb{Z}}(E(K)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + 1$. Suppose that the primes $\ell_1, \ldots, \ell_k$ are chosen as in Matsuno's theorem. These are primes

of good ordinary reduction that lie in $T_{E/K}$. Therefore, it follows from Lemma 5.3 that

$$\operatorname{rank}_2 \operatorname{Sel}_2(E/K) \geq k - 4.$$

Using the Kummer sequence, we see that for a 100% of the quadratic fields K,

$$\begin{aligned}
(12) \qquad \operatorname{rank}_2 \text{Ш}(E/K)[2] &\geq \operatorname{rank}_2 \operatorname{Sel}_2(E/K) - \operatorname{rank}_{\mathbb{Z}}(E(K)) - 2 \\
&\geq k - 7 - \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})).
\end{aligned}$$

Given $E_{/\mathbb{Q}}$ of conductor N and $n \in \mathbb{Z}_{\geq 0}$, we want to find an imaginary quadratic field $K/\mathbb{Q}$ with minimal conductor $\mathfrak{f}_K$ such that we can guarantee $\operatorname{rank}_2 \text{Ш}(E/K)[2] \geq n$. Let $\mathcal{P} = \{\ell_1, \dots, \ell_k\}$ be a set of (distinct) rational primes not dividing N with the additional property that they split completely in $\mathbb{Q}(E[2])/\mathbb{Q}$ and that precisely the primes in $\mathcal{P}$ ramify in K. From (12), we need that

$$\operatorname{rank}_2 \text{Ш}(E/K)[2] \geq k - 7 - \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) \geq n.$$

Equivalently,

$$k \geq n + \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + 7.$$

Note that this inequality ensures that k can take all but finitely many values. Therefore, in view of Goldfeld's Conjecture there exists a non-negative integer ϵ_E such that the set $\mathcal{P}$ contains $k + \epsilon_E$ (which we still call k by abuse of notation) many primes instead. To answer our question, we need to carefully pick the distinct primes $\ell_1, \dots, \ell_k$. Given any integer M, the number of distinct prime factors denoted by $\omega(M)$ is asymptotically $\log \log M$. Recall that the Prime Number Theorem asserts that the average gap between consecutive primes among the first x many primes is $\log x$. Since ℓ_1 is a prime of good reduction, $\ell_1 \nmid N$. The Prime Number Theorem implies that $\ell_1 \sim \log\left(\omega(N)\right) \sim \log_{(3)}(N)$. However, we need to do more. We require that ℓ_1 splits completely in $\mathbb{Q}(E[2])/\mathbb{Q}$. Using the Chebotarev Density Theorem, we can conclude that $\ell_1 \sim c \cdot \log\left(\omega(N)\right)$, where c is either 2, 3 or 6 depending on the degree of the Galois extension $\mathbb{Q}(E[2])/\mathbb{Q}$. Of course, asymptotically $\ell_1 \sim \log\left(\omega(N)\right)$. Next, $\ell_2 \nmid N\ell_1$ and splits completely in $\mathbb{Q}(E[2])/\mathbb{Q}$. Note that the number of distinct prime divisors of $N\ell_1 \sim \omega(N) + 1$. Using the same argument, we see that $\ell_2 \sim \log\left(\omega(N) + 1\right)$. Continuing this process, we have

$$(13) \qquad \mathfrak{f} = \prod_{i=1}^{k} \ell_i \sim \prod_{i=1}^{k} \left(\log\left(\omega(N) + (i-1)\right)\right)$$

$$(14) \qquad \sim \frac{(\log(\omega(N) - 1 + k))^{\omega(N) + 2 + k}}{\exp \operatorname{li}(\omega(N) - 1 + k)}$$

$$(15) \qquad \sim \frac{(\log n)^{n+c}}{\exp \operatorname{li}(n)}$$

where $\operatorname{li}(x) := \int_0^x \frac{dt}{\log t}$ is the logarithmic integral and c is a constant depending on E. Let us explain the above estimates in greater detail. Setting

$$P(k) := \prod_{i=1}^{k} \log(\omega(N) + (i-1)),$$

we wish to estimate the sum

$$\log(P(k)) = \sum_{i=1}^{k} \log\left(\log(\omega(N) + (i-1))\right).$$

Using Abel's partial summation formula (see, for example [Apo76, Theorem 4.2]) with $f(t) = \log(\log(\omega(N) - 1 + t))$, $a(n) = 1$, and $A(x) = \sum_{n \leq x} a(n))$, one obtains

$$\log P(k) = \sum_{i=1}^{k} \log\log(\omega(N) - 1 + i)$$

$$= k \log\log(\omega(N) - 1 + k) - \int_0^k \frac{\lfloor x \rfloor}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)}\, dx$$

$$= k \log\log(\omega(N) - 1 + k) - \int_0^k \frac{x}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)}\, dx$$

$$+ O\left(\int_0^k \frac{dx}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)}\right)$$

$$= k \log\log(\omega(N) - 1 + k) - \left(\mathrm{li}(\omega(N) - 1 + x) - (\omega(N) - 1)\log\log(\omega(N) - 1 + x)\right)\Big|_0^k$$

$$+ O\left(\int_0^k \frac{dx}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)}\right)$$

$$= k \log\log(\omega(N) - 1 + k) - \mathrm{li}(\omega(N) - 1 + k) + (\omega(N) - 1)\log\log(\omega(N) - 1 + k)$$

$$+ O(\log\log(\omega(N) - 1 + k))$$

$$= (k + \omega(N) + 1)\log\log(\omega(N) - 1 + k) - \mathrm{li}(\omega(N) - 1 + k) + O(\log\log(\omega(N) - 1 + k)).$$

This tells us that

$$P(k) = \exp\left((k + \omega(N) + 1)\log\log(\omega(N) - 1 + k) - \mathrm{li}(\omega(N) - 1 + k) + O(\log\log(\omega(N) - 1 + k))\right)$$

$$= \frac{\exp((k + \omega(N) + 1)\log\log(\omega(N) - 1 + k))}{\exp(\mathrm{li}(\omega(N) - 1 + k))}\left(\exp(O(\log\log(\omega(N) - 1 + k)))\right)$$

$$= \frac{\exp((k + \omega(N) + 1)\log\log(\omega(N) - 1 + k))}{\exp(\mathrm{li}(\omega(N) - 1 + k))}\left(O(\log(\omega(N) - 1 + k))\right)$$

$$= \frac{\log(\omega(N) - 1 + k)^{k + \omega(N) + 2}}{\exp(\mathrm{li}(\omega(N) - 1 + k))}.$$

For obtaining (15), we note that for the given n, the difference between n and k depends on the rank of E, and further $\omega(N)$ depends on E. Thus, we can rewrite $\omega(N) + 2 + k$ as $n + c$ where c is a constant depending only on the elliptic curve E.

We have therefore proven the following result.

Theorem 5.5. *Suppose that Goldfeld's Conjecture is true. Given an elliptic curve $E_{/\mathbb{Q}}$ and a positive integer n, there exists a quadratic extension $K/\mathbb{Q}$ with conductor $\mathfrak{f}_K \sim \frac{(\log n)^{n+c}}{\exp \mathrm{li}(n)}$ such that $\mathrm{rank}_2 \, \mathrm{III}(E/K)[2] \geq n$. Here c is an explicit constant depending only on E.*

Using a result of Ono we can prove an unconditional statement which we now explain.

5.1.3. *An unconditional effective version.* Given an elliptic curve $E_{/\mathbb{Q}}$ of conductor N and a positive integer n, we want to find an imaginary quadratic field $K/\mathbb{Q}$ with minimal conductor $\mathfrak{f}_K$ such that we can guarantee $\mathrm{rank}_2 \, \mathrm{III}(E/K)[2] \geq n$.

For this section, we consider elliptic curves $E_{/\mathbb{Q}}$ which have no exceptional primes p, i.e., no primes p such that the   mod p Galois representation attached to E is non-surjective. This condition is a mild one: W. Duke has shown in [Duk97, Theorem 1] that almost all elliptic curves defined over $\mathbb{Q}$ have no exceptional primes.

For such elliptic curves $E_{/\mathbb{Q}}$, [Ono01, Theorem 1] asserts that there exists a fundamental discriminant D_E such that the twisted curve E^d has rank 0 where $d = D_E \ell_1 \cdots \ell_k$ for some even integer k and where the primes ℓ_i are chosen from a set (of primes) with density 1. Indeed, the aforementioned theorem asserts (more generally) that there is a set of primes (call it S) with positive Frobenius density[1] such that E^d has rank 0 where $d = D_E \ell_1 \cdots \ell_k$ for some even integer k and the primes ℓ_i are chosen from S. But it follows from [Ono01, proof of Theorem 2.2] that the field $L/\mathbb{Q}$ in the definition of the Frobenius density is the field which contains the coefficients of the newform associated to E. Since the elliptic curves we are working with are defined over $\mathbb{Q}$, it follows from the Modularity Theorem that the newform will have integral coefficients i.e., $L = \mathbb{Q}$. Since there is only one Frobenius class in $\mathbb{Q}$, namely the trivial class, [Ono01, Theorem 1] says that the density of the set S is 1.

Let K be the quadratic field associated with the twist d. Since E^d has rank 0, we know that $\mathrm{rank}_{\mathbb{Z}}(E(K)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$. It follows that

$$\mathrm{rank}_2 \, \mathrm{III}(E/K)[2] \geq k - 6 - \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})).$$

If K is a quadratic field arising from Ono's theorem such that $\mathrm{rank}_2 \, \mathrm{III}(E/K)[2] > n$, it is required that

$$k \geq n + \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + 6.$$

To answer our question, we pick the distinct primes $\ell_1, \ldots, \ell_k$ using the exact same process as before. We have that

$$\mathfrak{f} = D_E \prod_{i=1}^{k} \ell_i \sim \prod_{i=1}^{k} \left(\log \left(\omega(N) + (i-1) \right) \right) \sim \frac{(\log(\omega(N) + k))^{\omega(N)+k}}{\exp \mathrm{li}(\omega(N) + k)} \sim \frac{(\log n)^{n+c}}{\exp \mathrm{li}(n)}$$

where $\mathrm{li}(x) := \int_0^x \frac{dt}{\log t}$ is the logarithmic integral and c is a constant depending on E.

We have therefore proven the following result.

───────────

[1] i.e., there exists a finite Galois extension $L/\mathbb{Q}$ such that for all but finitely many primes in this set, these primes represent a fixed Frobenius conjugacy class in $\mathrm{Gal}(L/\mathbb{Q})$

Theorem 5.6. *Given an elliptic curve $E_{/\mathbb{Q}}$ with no exceptional primes and a positive integer n, there exists a quadratic extension $K/\mathbb{Q}$ with conductor $\mathfrak{f}_K \sim \frac{(\log n)^{n+c}}{\exp \mathrm{li}(n)}$ such that* $\mathrm{rank}_2 \, \mathrm{III}(E/K)[2] \geq n$. *Here c is an explicit constant depending only on E.*

5.2. **Arbitrarily large III in $\mathbb{Z}/p\mathbb{Z}$-Extensions.** Let $E_{/\mathbb{Q}}$ be a fixed rank 0 elliptic curve of conductor N. Let p be a fixed odd prime. Let F be any number field, we have the obvious short exact sequence

$$0 \to E(F)/pE(F) \to \mathrm{Sel}_p(E/F) \to \mathrm{III}(E/F)[p] \to 0.$$

It follows that

(16) $\mathrm{rank}_p \, \mathrm{Sel}_p(E/F) = \mathrm{rank}_{\mathbb{Z}}(E(F)) + \mathrm{rank}_p \, E(F)[p] + \mathrm{rank}_p \, \mathrm{III}(E/F)[p].$

When $F/\mathbb{Q}$ is a cyclic degree-p Galois extension, we know from Lemma 5.3 that

$$\mathrm{rank}_p \, \mathrm{Sel}_p(E/F) \geq \#T_{E/F} - 4.$$

Given an integer n, there exists a number field $F_{(n)}$ such that (see [Čes17, Theorem 1.2])

$$\mathrm{rank}_p \, \mathrm{Sel}_p(E/F_{(n)}) \geq \#T_{E/F} - 4 \geq n.$$

Denote the conductor of $F_{(n)}$ by $\mathfrak{f}(F_{(n)})$. Varying over *all* $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$, there are infinitely many number fields $L/\mathbb{Q}$ such that $T_{E/L} \supseteq T_{E/F_{(n)}}$, i.e., $\mathfrak{f}(F_{(n)}) \mid \mathfrak{f}(L)$. For each such L,

$$\mathrm{rank}_p \, \mathrm{Sel}_p(E/L) \geq n.$$

Recall the conjecture of David–Fearnley–Kisilevsky from Section 2. If $p \geq 7$, it predicts the boundedness of the set

$$N_{E,p}(X) := \{L/\mathbb{Q} \text{ cyclic of degree } p : \mathfrak{f}(L) < X \text{ and } \mathrm{rank}_{\mathbb{Z}}(E/L) > \mathrm{rank}_{\mathbb{Z}}(E/\mathbb{Q})\}.$$

If this conjecture is true, then varying over *all* $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$, there are only finitely many cyclic p-extensions $L/\mathbb{Q}$ in which there is a rank jump upon base-change. Therefore, given an integer n, one can find an integer $M = M(n)$ and a number field $L/\mathbb{Q}$ such that

  (i) $\mathfrak{f}(L) > M(n)$,
 (ii) $\mathfrak{f}(F_{(n)}) \mid \mathfrak{f}(L)$,
(iii) $\mathrm{rank}_{\mathbb{Z}}(E(L)) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$.

Thus, given n, there exists a cyclic extension $L/\mathbb{Q}$ of degree $p \geq 7$ such that (16) becomes

$$\mathrm{rank}_p \, \mathrm{Sel}_p(E/L) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + \mathrm{rank}_p \, E(L)[p] + \mathrm{rank}_p \, \mathrm{III}(E/L)[p] \geq n.$$

Since $\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ is independent of L and $\mathrm{rank}_p \, E(L)[p]$ is at most 2, it means that given n, there exists a $\mathbb{Z}/p\mathbb{Z}$-extension $L/\mathbb{Q}$ such that $\mathrm{rank}_p \, \mathrm{III}(E/L)[p] \geq n$.

  We feel that the full force of the conjecture of David–Fearnley–Kisilevsky is required. In particular, we do not see if the result of Mazur–Rubin is sufficient. This is because it is not obvious to us as to why even if there are infinitely many number fields $\mathcal{L}/\mathbb{Q}$ with $\mathrm{rank}_{\mathbb{Z}}(E(\mathcal{L})) = \mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$, there should be any (of these) satisfying $\mathfrak{f}(F_{(n)}) \mid \mathfrak{f}(\mathcal{L})$.

6. TABLES

6.1. In Table 1, we compute the following expression

$$\left(1 - \frac{1}{p}\right)\left(1 - \prod_{q \equiv 1 (\bmod\ p)} \left(\frac{q-1}{2q^2} + 1 - \frac{1}{q}\right)\right).$$

for $3 \le p < 50$ and $q \le 179,424,673$ (i.e., the first 10 million primes).

Table 1: Values for expression (8)

Primes	Value for Expression	Primes	Value for Expression
3	0.293282	23	0.0404621
5	0.189719	29	0.0303331
7	0.121798	31	0.0198836
11	0.0866316	37	0.0197385
13	0.0647841	41	0.019329
17	0.0453478	43	0.0165664
19	0.0342828	47	0.0141439

6.2. In Table 2, we record the proportion of enemy primes for CM elliptic curves with conductor < 100 and $p < 50$. Here, "-" indicates that for a given elliptic curve, p is an *irrelevant* prime. Since $p = 47$ is an *irrelevant prime* for the four elliptic curves of interest, we have excluded it from our table. In the first row, the value of $\frac{p}{2(p+1)(p-1)^2}$ is recorded. Note that the reduction type depends only on the isogeny class. The same is true for the λ-invariant of the p-primary Selmer group. However, it is possible that one or more of the curves in a given isogeny class has positive μ-invariant, but the others do not (see also [Gre99, Conjecture 1.11]). To keep the tables succinct, since the Iwasawa invariants are the same for all curves in the isogeny class, they are clubbed together.

The data in the table is obtained from the code available here.

Table 2: Proportion of enemy primes

E	5	7	11	13	17	19
$p/2(p+1)(p-1)^2$	0.002604	0.012153	0.004583	0.003224	0.001845	0.001466
27a	0.020833	0.013881	-	0.003471	-	0.001533
36a	-	0.013880	-	0.003471	-	0.001538
49a	-	-	0.004989	-	-	-
64a	0.031260	-	-	0.003478	0.001950	-

Proportion of enemy primes continued

E	23	29	31	37	41	43
$p/2(p+1)(p-1)^2$	0.000990	0.000616	0.000538	0.000376	0.000305	0.000277
27a	-	-	0.000551	0.000424	-	0.000279
36a	-	-	0.000550	0.000422	-	0.000282
49a	0.001028	0.000638	-	0.000423	-	0.000282
64a	-	0.000640	-	0.000426	0.000312	-

Acknowledgements

References

[Apo76]   Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[BCH+66]   Armand Borel, Sarvadaman Chowla, Carl S Herz, Kenkichi Iwasawa, and Jean-Pierre Serre. *Seminar on Complex Multiplication: Seminar Held at the Institute for Advanced Study, Princeton, NY, 1957-58*, volume 21 of *Lecture Notes in Mathematics*. Springer, 1966.

[BFH90]   Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for l-functions of modular. *Invent. math*, 102:543–618, 1990.

[Bir68]   Bryan J Birch. How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.*, 1(1):57–60, 1968.

[BN16]   Peter Bruin and Filip Najman. A criterion to rule out torsion groups for elliptic curves over number fields. *Res. Number Theory*, 2(1):3, 2016.

[Bra14]   Julio Brau. Selmer groups of elliptic curves in degree p extensions, 2014. arXiv:1401.3304.

[BS13]   Manjul Bhargava and Arul Shankar. The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1, 2013. arXiv:1312.7859.

[BS15a]   Manjul Bhargava and Arul Shankar. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves. *Ann. Math.*, pages 191–242, 2015.

[BS15b]   Manjul Bhargava and Arul Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. Math.*, pages 587–621, 2015.

[Čes17]   Kęstutis Česnavičius. p-Selmer growth in extensions of degree p. *J. London Math. Soc.*, 95(3):833–852, 2017.

[Coj04]   Alina Carmen Cojocaru. Questions about the reductions modulo primes of an elliptic curve. In *Proc. 7th Meeting of the Canadian Number Theory Association (Montreal, 2002)*, pages 61–79. Citeseer, 2004.

[CS00]   John Coates and Ramdorai Sujatha. *Galois cohomology of elliptic curves.* Narosa, 2000.

[CS10]   Pete L Clark and Shahed Sharif. Period, index and potential, III. *Algebra Number Theory*, 4(2):151–174, 2010.

[CS21]   J. E. Cremona and M. Sadek. Local and global densities for Weierstrass models of elliptic curves. *accepted for publication in Mathematical Research Letters*, 2021. preprint, arXiv:2003.08454.

[DEvH$^+$21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021.

[DFK07]   Chantal David, Jack Fearnley, and Hershy Kisilevsky. Vanishing of L-functions of elliptic curves over number fields. *Ranks of elliptic curves and random matrix theory*, (341):247, 2007.

[DN19]   Maarten Derickx and Filip Najman. Torsion of elliptic curves over cyclic cubic fields. *Math. Comput.*, 88(319):2443–2459, 2019.

[Dok07]   Tim Dokchitser. Ranks of elliptic curves in cubic extensions. *Acta Arithmetica*, 4(126):357–360, 2007.

[Duk97]   William Duke. Elliptic curves with no exceptional primes. *Proceedings of the Académie des sciences. Series 1, Mathématics*, 325(8):813–818, 1997.

[GFP20]   Natalia Garcia-Fritz and Hector Pasten. Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points. *Math. Ann.*, 377(3):989–1013, 2020.

[GJN20]   Enrique González-Jiménez and Filip Najman. Growth of torsion groups of elliptic curves upon base change. *Math. Comput.*, 89(323):1457–1485, 2020.

[Gre99]   R Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716, pages 51–144. Springer, 1999.

[HKR21]   Jeffrey Hatley, Debanjana Kundu, and Anwesh Ray. Statistics for anticyclotomic Iwasawa invariants of elliptic curves, 2021. arXiv:2106.01517.

[HL19]   Jeffrey Hatley and Antonio Lei. Arithmetic properties of signed Selmer groups at non-ordinary primes. *Ann. Inst. Fourier*, 69(3):1259–1294, 2019.

[HM99]   Yoshitaka Hachimori and Kazuo Matsuno. An analogue of Kida's formula for the Selmer groups of elliptic curves. *J. Alg. Geom.*, 8(3):581–601, 1999.

[JKL11]   Daeyeol Jeon, Chang Kim, and Yoonjin Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comput.*, 80(273):579–591, 2011.

[JKS04]   Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arithmetica*, 113:291–301, 2004.

[JR08]   John W Jones and David P Roberts. Number fields ramified at one prime. In *International Algorithmic Number Theory Symposium*, pages 226–239. Springer, 2008.

[Kam92]   Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. math.*, 109(1):221–229, 1992.

[Kat04]   Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[Kid03]   Masanari Kida. Variation of the reduction type of elliptic curves under small base change with wild ramification. *Central European J. Math.*, 1(4):510–560, 2003.

[KM88]   Monsur A Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, 1988.

[Kol89]   Viktor Alexandrovich Kolyvagin. Finiteness of and for a subclass of Weil curves. *Mathematics of the USSR-Izvestiya*, 32(3):523, 1989.

[KR21a]   Debanjana Kundu and Anwesh Ray. Statistics for Iwasawa invariants of elliptic curves. *Trans. Am. Math. Soc.*, 374:7945–7965, 2021. DOI: https://doi.org/10.1090/tran/8478.

[KR21b]   Debanjana Kundu and Anwesh Ray. Statistics for Iwasawa invariants of elliptic curves, II, 2021. arXiv:2106.12095.

[LR22]   Álvaro Lozano-Robledo. Galois representations attached to elliptic curves with complex multiplication. *Algebra Number Theory*, 16(4):777–837, 2022.

[Mat09]   Kazuo Matsuno. Elliptic curves with large Tate–Shafarevich groups over a number field. *Math. Res. Lett.*, 16(3):449–461, 2009.

[Maz72]   Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. math.*, 18(3-4):183–266, 1972.

[Maz77]   Barry Mazur. Modular curves and the Eisenstein ideal. *Publ. Math. IHES*, 47(1):33–186, 1977.

[Maz78]   Barry Mazur. Rational isogenies of prime degree. *Invent. math.*, 44(2):129–162, 1978.

[Mer96]   Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. math.*, 124(1-3):437–449, 1996.

[MP22]   Adam Morgan and Ross Paterson. On 2-Selmer groups of twists after quadratic extension. *J. London Math. Soc.*, 105(2):1110–1166, 2022.

[MR19]   Barry Mazur and Karl Rubin. Arithmetic conjectures suggested by the statistical behavior of modular symbols. *arXiv preprint arXiv:1910.12798*, 2019.

[MRL18]   Barry Mazur, Karl Rubin, and Michael Larsen. Diophantine stability. *Am. J. Math.*, 140(3):571–616, 2018.

[MSM16]   Guillermo Mantilla-Soler and Marina Monsurrò. The shape of $\mathbb{Z}/\ell\mathbb{Z}$-number fields. *Ramanujan J.*, 3(39):451–463, 2016.

[Naj16]   Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272, 2016.

[NSW13]   Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323. Springer, 2013.

[Ono01]   Ken Ono. Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves. *J. reine angew. math.*, 533:81–97, 2001.

[Poo18]   Bjorn Poonen. Heuristics for the arithmetic of elliptic curves. In *Proceedings of the International Congress of Mathematicians-Rio de*, volume 2, pages 399–414. World Scientific, 2018.

[PPVW19]   Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood. A heuristic for boundedness of ranks of elliptic curves. *J. European Math. Soc.*, 21(9):2859–2903, 2019.

[RS19]   Anwesh Ray and Ramdorai Sujatha. Euler characteristics and their congruences in the positive rank setting. *Canad. Math. Bull.*, pages 1–19, 2019.

[RS20]   Anwesh Ray and R Sujatha. Euler characteristics and their congruences for multisigned Selmer groups. *Canadian J. Mathematics*, pages 1–24, 2020.

[Sag20]   Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. https://www.sagemath.org.

[Ser74]   Jean-Pierre Serre. Divisibilité de certaines fonctions arithmétiques. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 16(1):1–28, 1974.

[Sil09]   Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2009.

[ST68]   Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. Math.*, pages 492–517, 1968.

[Wan15]   Jian Wang. *On the torsion structure of elliptic curves over cubic number fields*. PhD thesis, 2015.

[Was97]   Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer, 1997.

[Was08]   Lawrence C Washington. *Elliptic curves: number theory and cryptography.* CRC press, 2008.

(Beneish) Department of Mathematics, University of California, Berkeley, 970 Evans Hall, Berkeley, CA 94720, USA.
    Email address: `leabeneish@berkeley.edu`

(Kundu) 222 College Street, Fields Institute, ON, M5T 3J1, Canada.
    Email address: `dkundu@math.toronto.edu`

(Ray) Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920 Chemin de la tour, Montréal (Québec) H3T 1J4, Canada
    Email address: `anwesh.ray@umontreal.ca`