J. Aust. Math. Soc. **116** (2024), 1–38
doi:10.1017/S1446788723000034

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

(Received 25 October 2022; accepted 16 April 2023; first published online 29 May 2023)

Communicated by Michael Coons

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.

2020 *Mathematics subject classification*: primary 11R23; secondary 11G05, 11R34.

Keywords and phrases: rank growth, Selmer group, Shafarevich–Tate group, λ-invariant, Kida's formula.

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, that is,

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

where r is a nonnegative integer called the *rank* and $E(F)_{\text{tors}}$ is a finite group, called the *torsion subgroup*. Over $\mathbb{Q}$, the possible structures of $E(\mathbb{Q})_{\text{tors}}$ are known by the work of Mazur (see [Maz77, Maz78]). These techniques have been extended by Kamienny, Kenku, and Momose (see for example [KM88, Kam92]) to provide the complete classification of torsion subgroups for quadratic fields. More recently, in a series of works by several authors, the classification of torsion subgroups for cubic fields has been completed (see, for example, [BN16, DEvH+21, DN19, JKL11, JKS04, Naj16, Wan15]). In [Mer96], Merel proved that for elliptic curves over any number field, the bound of the order of the torsion subgroup depends only on the degree of the number

LB acknowledges the support of the CRM-ISM Postdoctoral Fellowship. DK acknowledges the support of the PIMS Postdoctoral Fellowship. AR's research is supported by the CRM Simons postdoctoral fellowship.

field. Despite remarkable advances made toward 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 10^{th} 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 Equation (3-3)). 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 (complex multiplication) 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 $n \geq 0$, that is,*

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 Hypothesis 3.10.

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 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]), González-Jiménez and Najman investigated the question of when the torsion group does not grow upon base-change (see Theorem 3.12 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, we have the following corollary.

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 Hypothesis 3.10 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 of 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 nonzero 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*

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

$p/(p-1)^2(p+1)$ such that the p-primary Selmer group becomes nontrivial 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 Hypothesis 3.19 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.*

Hypothesis 3.19 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 nonordinary case. It seems reasonable to expect that our results should extend to the supersingular case using the work of Hatley and Lei in [HL19, Theorem 6.7].

In [Čes17], 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 favor 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. However, 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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 $Ш(E/F)$, 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 5.7, 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 $\operatorname{rank}_2 Ш(E/K) := \dim_{\mathbb{F}_2} Ш(E/K)[2] > n$. Recently, it has been shown in [MP22] that there are infinitely many elliptic curves with large $\operatorname{rank}_2 Ш(E/K)$. 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, and H. Kisilevsky is true (see Section 2.2 for the precise statement), then the result of Clark and 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 six 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 the 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 $\operatorname{Gal}(\overline{F}/F)$. 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:

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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

$$0 \to E(F)/mE(F) \to \mathrm{Sel}_m(E/F) \to Ш(E/F)[m] \to 0. \tag{2-1}$$

Here, $Ш(E/F)$ is the *Shafarevich–Tate group* which is conjecturally finite. Throughout this article, we 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 (for example, [Was97, Ch. 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:

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

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

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

with finite kernel and cokernel. Here, $m_i > 0$ and $h_j(T)$ is a distinguished polynomial (that is, a monic polynomial with nonleading 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,

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

The λ-invariant of M is the degree of the characteristic element, that is,

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

Let $E_{/F}$ be an elliptic curve with good reduction at p. We 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 that divide Np. Let F_S be the maximal algebraic extension of F that is unramified at the primes $v \notin S$. Set $E[p^\infty]$ to be the Galois module of all p-power

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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

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

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:

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

It is easy to see that $\mathrm{Sel}_{p^\infty}(E/L) = \varinjlim_n \mathrm{Sel}_{p^n}(E/L)$, see for example [CS00, Section 1.7]. By taking direct limits of Equation (2-1), the p-primary Selmer group over F fits into a short exact sequence,

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

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:

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

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 that 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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

We deduce from Equation (2-2) that

$$\operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/F_n) \geq \operatorname{rank}_{\mathbb{Z}}(E(F_n)), \tag{2-3}$$

with equality if $Ш(E/F_n)[p^\infty]$ 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 $r_n \geq \operatorname{rank}_{\mathbb{Z}}(E(F_n))$. This is indeed the case, since Mazur's control theorem asserts that there is a natural map

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

with finite kernel. From Equation (2-3), we see that $r_n \geq \operatorname{rank}_{\mathbb{Z}}(E(F_n))$ and the result follows. □

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

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 $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$ is a cofinitely generated $\mathbb{Z}_p$-module. Then, $\operatorname{Sel}_{p^\infty}(E/L_{\mathrm{cyc}})$ is also a cofinitely generated $\mathbb{Z}_p$-module. Moreover, their respective λ-invariants are related by the following formula:*

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

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

$$P_1 = \{w : w \nmid p, E \text{ has split multiplicative reduction at } w\},$$
$$P_2 = \{w : w \nmid p, E \text{ has good reduction at } w, E(L_{\mathrm{cyc},w}) \text{ has a point of order } p\}.$$

PROOF. [HM99, Theorem 3.1]. □

REMARK 2.4. 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 2.5. *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 2.6. 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 $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}_{\mathrm{cyc}})$. This happens when $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}) = 0$, 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].

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 Bhargava and 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 nonzero 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 2.7 (Birch and Swinnerton-Dyer). *The Hasse–Weil L-function has analytic continuation to the whole complex plane, and*

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

It follows from the Birch and Swinnerton-Dyer (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, and 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, we have the following conjecture.

CONJECTURE 2.8 [DFK07, Conjecture 1.2]. *Let p be an odd prime and $E_{/\mathbb{Q}}$ be an elliptic curve. Define*

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

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

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

(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 $p \ge 7$, then $N_{E,p}(X)$ is bounded.*

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 and 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, and 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 3.11: for non-CM elliptic curves, the result is unconditional; whereas for the CM-case, we prove the same result under an additional independence Hypothesis 3.10. Next, we study the *dual problem*, that is, 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 show 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 2.5, we show 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 $\mu_p(E/L) = \lambda_p(E/L) = 0$, 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; that is, our results only provide a lower bound. However, we succeed in answering a stronger question, that is, how often the p-primary Selmer group $\mathrm{Sel}_{p^\infty}(E/F_{\mathrm{cyc}})$ is 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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

or conductor) have rank 0. Moreover, Proposition 2.5 asserts that there are density one good ordinary primes satisfying the condition of vanishing Iwasawa invariants. Lastly, when an elliptic curve does *not* have 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, that is, $\gcd(q, N) = 1$. 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, Proposition 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 nonsingular points of the reduced elliptic curve, $E_0(L_w)$ is the set of points with nonsingular reduction, and $E_1(L_w)$ is the kernel of the 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 hypotheses) 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

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

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, page 498] or [HM99, page 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

$$\sum_{w \in P_1} (e_{L/\mathbb{Q}}(w) - 1) = \sum_{w \in P_2} (e_{L/\mathbb{Q}}(w) - 1) = 0, \tag{3-1}$$

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

$$P_1 = \{w \in L : \ w \nmid p, \ E \text{ has split multiplicative reduction at } w\},$$
$$P_2 = \{w \in L : \ w \nmid p, \ E \text{ has good reduction at } w, \ E(L_w) \text{ has a point of order } p\}.$$

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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, Section 2])

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

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

REMARK 3.1. Henceforth, the sets P_1, P_2 will denote sets of primes in L (rather than L_{cyc}). By our assumption that $L \cap \mathbb{Q}_{\text{cyc}} = \mathbb{Q}$, 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. However, 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 3.2. *Let $E_{/\mathbb{Q}}$ be a rank 0 elliptic curve with good ordinary reduction at $p \ge 5$ 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 $\mathbb{Q}_{\text{cyc}}$ such that Equation (3-1) holds. Then, $\mu_p(E/L) = \lambda_p(E/L) = 0$. This implies in particular that $\text{rank}_{\mathbb{Z}}(E(L_n)) = 0$ for all $n \ge 0$.*

The conditions imposed in Proposition 3.2 will be required throughout this section. Therefore, we make the following definition.

DEFINITION 3.3. 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 Equation (3-1) holds. We begin by recalling the following well-known result.

PROPOSITION 3.4. *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 that 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]. □

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])

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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

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

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

DEFINITION 3.5. 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 3.3). Define *enemy primes* to be those primes that 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 3.6

(i) A prime $q \equiv 1 \pmod{p}$ that 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 behavior of q. The following lemma will play a crucial role in the subsequent discussion.

LEMMA 3.7. *Let $L/\mathbb{Q}$ be a cyclic degree-p extension disjoint from $\mathbb{Q}_{\text{cyc}}$. Then, Equation (3-1) 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

$$\sum_{w \in P_1} (e_{L/\mathbb{Q}}(w) - 1) \neq 0$$

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 $\mathbb{Q}_{\text{cyc}}$, we know that if p is ramified in $L/\mathbb{Q}$, there must be at least one other prime that is also ramified. Now,

$$\sum_{w \in P_2} (e_{L/\mathbb{Q}}(w) - 1) \neq 0$$

precisely when there exists a q ($\neq p$) satisfying *all* of the following conditions:

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

(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

$$\mathcal{F}_{(E,p)} = \mathcal{F}^{\mathrm{ord}}_{(E,p)} \cup \mathcal{F}^{\mathrm{ss}}_{(E,p)} \text{ and}$$
$$\mathcal{E}_{(E,p)} = \mathcal{E}^{\mathrm{split}}_{(E,p)} \cup \mathcal{E}^{\mathrm{ord}}_{(E,p)} \cup \mathcal{E}^{\mathrm{ss}}_{(E,p)}.$$

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

LEMMA 3.8. *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, $p \nmid \#\widetilde{E}(\mathbb{F}_q)$. □

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

$$\mathfrak{d}(\mathcal{E}_{(E,p)}) + \mathfrak{d}(\mathcal{F}_{(E,p)}) + \mathfrak{d}(\mathcal{N}_{(E,p)}) = \frac{1}{\varphi(p)} = \frac{1}{p-1}. \tag{3-2}$$

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, and hence $\mathfrak{d}(\mathcal{N}_{(E,p)}) = 0$. We henceforth disregard the primes q that are of nonsplit 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) $p \mid \#\widetilde{E}(\mathbb{F}_q)$.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 3.9. *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,*

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

PROOF. The result is well known and follows from the proof of [GFP20, Proposition 4.6]. For the convenience of the reader, we 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 3.8 that if conditions (b) and (c) are satisfied, then condition (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, that is, 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 satisfies both conditions (b) and (c) above if and only if $\bar{\rho}(\mathrm{Frob}_q)$ is contained in $\mathcal{S}$. According to Lemma 4.8, 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

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

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 suggest 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, we make the following assumption.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

HYPOTHESIS 3.10. Let $E_{/\mathbb{Q}}$ be an elliptic curve with CM and p be a fixed odd prime of good ordinary reduction. Then, $\mathfrak{d}(\mathcal{E}_{(E,p)}) = p/2(p-1)^2(p+1)$.

We can now prove the main result of this section.

THEOREM 3.11. *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 a rank 0 elliptic curve (defined over $\mathbb{Q}$) with complex multiplication and a relevant prime $p \geq 5$. Suppose further that Hypothesis 3.10 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 3.2 if we can show that there are infinitely many cyclic degree p extensions such that Equation (3-1) holds.

Observe that

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

It follows from Lemma 3.7 that Equation (3-1) 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 3.4 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. □

Note that condition (1) in Theorem 3.11, 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 and Najman.

THEOREM 3.12. *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, $E(L)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$.*

PROOF. See [GJN20, Theorem 7.2]. □

Combining Theorems 3.11 and 3.12, the following corollary is immediate.

COROLLARY 3.13. *Let (E, p) be a given pair of a 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*

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

representation at p is surjective. If $E_{/\mathbb{Q}}$ is an elliptic curve with CM, suppose that Hypothesis 3.10 holds. Then, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions of $\mathbb{Q}$ where the Mordell–Weil group does not grow.

REMARK 3.14. 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 that are contained in the cyclotomic field $\mathbb{Q}(\mu_q)$ where q is a prime of the form $1 \pmod p$. 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 3.11 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 and 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 3.13 holds unconditionally for density 1 primes if E is an elliptic curve without CM. However, 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 following two statements is true (see [Was08, Section 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 3.8 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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 3.4, 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 3.2, if $\operatorname{rank}_{\mathbb{Z}}(E_k/\mathbb{Q}) = 0$ and $\mu_p(E/\mathbb{Q}) = 0$ (for example, 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 3.15. *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 $\operatorname{Sel}_{p^\infty}(E/L_{\mathrm{cyc}}) = 0$. In particular, there are infinitely many $\mathbb{Z}/p\mathbb{Z}$-extensions such that $\operatorname{rank}_{\mathbb{Z}}(E(L)) = 0$.

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 3.16. 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 2.5 asserts that density one good ordinary primes are *relevant*. Further assume that N is divisible by at least one prime of the form $1 \pmod{p}$. The following lemma is a special case of Proposition 3.2.

LEMMA 3.17. *Keep the setting as above. If E has no prime of split multiplicative reduction, that is, $P_1 = \emptyset$, then there exists at least one degree-p cyclic extension $L/\mathbb{Q}$ such that $\lambda_p(E/L) = 0$. In particular, $\operatorname{rank}_{\mathbb{Z}}(E(L)) = 0$.*

PROOF. By Proposition 3.4, 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, $\operatorname{Sel}_{p^\infty}(E/L_{\mathrm{cyc}}) = 0$. Clearly, $\operatorname{Sel}_{p^\infty}(E/L)$ is trivial as well; this forces $\operatorname{rank}_{\mathbb{Z}}(E(L)) = 0$. □

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 that 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:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

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

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

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

$$\lim_{X\to\infty} \frac{\#\{\boldsymbol{a} \in S : \mathrm{height}(\boldsymbol{a}) < X\}}{\#\{\boldsymbol{a} \in \mathbb{Z}^5 : \mathrm{height}(\boldsymbol{a}) < X\}}. \tag{3-3}$$

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

LEMMA 3.18. *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 $(q-1)/2q^2$;*
(ii) *the proportion with good reduction at q is $(1 - 1/q)$.*

PROOF. For part (i), see [CS21, Theorem 5.1]. For part (ii), see [CS21, Proposition 2.2]. □

Henceforth, we assume that the rank of the elliptic curve and the reduction type at ℓ are independent of each other. In other words, we 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 3.18.

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 assumption we have made.

HYPOTHESIS 3.19. The reduction type of an elliptic curve at a prime q is independent of its rank.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

What we mean is that density results from Lemma 3.18 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 3.20. *Let $p \geq 5$ be a fixed odd prime. Suppose that Hypothesis 3.19 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*

$$\left(1 - \frac{1}{p}\right)\left(1 - \prod_{q \equiv 1 \pmod{p}} \left(\frac{q-1}{2q^2} + 1 - \frac{1}{q}\right)\right). \tag{3-4}$$

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 nonsplit 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 Equation (3-4) from Lemma 3.18.

From our earlier discussion, to prove the second assertion, it remains to show that Equation (3-4) 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. □

In Table 1, we compute Equation (3-4) for $3 \leq p < 50$ and $q \leq 179\,424\,673$ (that is, the first 10 million primes).

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

TABLE 1. Values for Equation (3-4).

Primes	Value for expression	Primes	Value for expression
3	0.293 282	23	0.040 462 1
5	0.189 719	29	0.030 333 1
7	0.121 798	31	0.019 883 6
11	0.086 631 6	37	0.019 738 5
13	0.064 784 1	41	0.019 329
17	0.045 347 8	43	0.016 566 4
19	0.034 282 8	47	0.014 143 9

QUESTION 3.21. Let $p \geq 5$ 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 Equation (3-1) holds.

PROPOSITION 3.22. *Let p be a fixed odd prime. Let $L/\mathbb{Q}$ be a fixed $\mathbb{Z}/p\mathbb{Z}$-extension that is tamely ramified at primes $q_1, \ldots, q_r$. The proportion of elliptic curves defined over $\mathbb{Q}$ (ordered by height) such that Equation (3-1) holds has a lower bound of*

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

PROOF. Note that for Equation (3-1) to hold, the reduction type at p does not matter. To find a lower bound, it suffices that *all* the ramified primes (that is, the q_i terms) are primes of bad reduction of nonsplit 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 3.18, 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 3.23. The above proposition is not sufficient to answer the question because given p, we are unable to compute the proportion of elliptic curves for which p is *relevant*. In particular, we do not know precisely for what proportion of elliptic curves p is 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 $\mathbb{F}_p$ (approximately $1/2\sqrt{p}$). Therefore, as p becomes large, 100% of the elliptic curves with good reduction at

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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 $\frac{1}{2}(1 - 1/2\sqrt{p})(1 - 1/p)$.

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 groups

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

This result is then applied to study a problem in arithmetic statistics which we prove in Theorem 4.9.

4.1. Here, we first prove a criterion for nontriviality 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) $Ш(E/L)[p^\infty]$ *is finite.*

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

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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

REMARK 4.2. Condition (iv) 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.

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

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

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

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 4.3. *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) $\operatorname{rank}_{\mathbb{Z}} E(L) = 0$*;*
(ii) *E has good ordinary reduction at p;*
(iii) *$Ш(E/L)[p^\infty]$ is finite.*

Then, the following assertions hold:

(a) *the Euler characteristic $\chi(L_{\mathrm{cyc}}/L, E[p^\infty])$ is an integer, further, it is a power of p;*
(b) *the Euler characteristic is given by the following formula:*

$$\chi(L_{\mathrm{cyc}}/L, E[p^\infty]) = \frac{\#Ш(E/L)[p^\infty] \times \prod_v c_v^{(p)}(E/L) \times \prod_{v|p}(\#\widetilde{E}(k_v)[p^\infty])^2}{(\#E(L)[p^\infty])^2}. \quad (4\text{-}1)$$

PROOF. Assertion (a) follows from [HKR21, Lemma 3.4 and Remark 3.5], and for assertion (b), the reader is referred to [CS00, Theorem 3.3]. □

The next result relates the Euler characteristic and Iwasawa invariants.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

PROPOSITION 4.4. *Let $E_{/L}$ be an elliptic curve satisfying the following conditions:*

(i) *E has good ordinary reduction at all primes $v|p$;*
(ii) $\operatorname{rank}_{\mathbb{Z}} E(L) = 0$*;*
(iii) *$Ш(E/L)[p^\infty]$ 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 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. □

LEMMA 4.5. *Let $E_{/\mathbb{Q}}$ be an elliptic curve that satisfies the following conditions:*

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

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

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

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

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

It follows from Proposition 4.4 that $\chi(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E[p^\infty]) = 1$. However, by Equation (4-1),

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

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

LEMMA 4.6. *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 that 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, pages 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, page 448]). According to [Sil09, page 448], 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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

the Kodaira type of $E_{/\mathbb{Q}_\ell}$ is I_m, then upon base-change to L_v, it becomes $\mathrm{I}_{me} = \mathrm{I}_{mp}$. 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 4.5, we have that

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

Assume by way of contradiction that

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

Since $\mathrm{rank}_{\mathbb{Z}} E(L) = 0$, it follows from Theorem 4.3 that the Euler characteristic $\chi(L_{\mathrm{cyc}}/L, E[p^\infty])$ is defined and given by the formula

$$\chi(L_{\mathrm{cyc}}/L, E[p^\infty]) = \frac{\#Ш(E/L)[p^\infty] \times \prod_v c_v^{(p)}(E/L) \times \prod_{v|p} (\#\widetilde{E}(k_v)[p^\infty])^2}{(\#E(L)[p^\infty])^2}. \tag{4-2}$$

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

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

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 4.4 that $\chi(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E[p^\infty]) = 1$.

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

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

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

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

By assumption, $Ш(E/L)[p^\infty] = 0$, and hence, $\#Ш(E/L)[p^\infty] = 1$. It follows from Lemma 4.6 that $\prod_{v \nmid p} c_v^{(p)}(E/L) = 1$. 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. However, 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 Equation (4-2) is 1. Theorem 4.3 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 4.4 that

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

In particular, we find that

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

However, recall that according to Kida's formula,

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

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

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

Thus, 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 $\operatorname{rank}_{\mathbb{Z}} E(L) > 0$ or $Ш(E/L)[p^\infty] \neq 0$. □

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 fix 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 $\mathbb{Q}_{\text{cyc}}$ and ramified at precisely one prime. For each prime $q \equiv 1 \pmod p$, there is exactly one such extension $L_q/\mathbb{Q}$ that is ramified at q (see Proposition 3.4). Note that L_q is contained in $\mathbb{Q}(\mu_q)$. For $X > 0$, let $\pi(X)$ be the prime counting function (that is, denote the number of primes $q \leq X$) and $\pi'(X)$ be the number of primes $q \leq X$ for which:

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

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 nonvanishing of $\operatorname{Sel}_{p^\infty}(E/L_q)$ is equivalent to at least one of the following conditions being satisfied:

(1) $\operatorname{rank}_{\mathbb{Z}} E(L_q) > 0$;
(2) $Ш(E/L_q)[p^\infty] \neq 0$.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

Thus, if the Selmer group becomes nonzero 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 4.9, 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 $q \neq p$ coprime to the conductor of E,

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

Therefore, if the Frobenius of a prime $q \nmid Np$ lies in the Chebotarev set $\mathcal{S}$, then the Selmer group becomes nonzero 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 $\limsup_{X\to\infty} \pi'(X)/\pi(X)$. Stated 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 $\mathbb{Q}$ that 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 that 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 $\bar{\rho}(\mathrm{Frob}_q)$ is $x^2 - a_q x + q$. Let $\mathcal{S}$ consist of elements $\sigma \in \mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$ such that

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

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

LEMMA 4.7. *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) $\mathrm{Frob}_q \in \mathcal{S}$.

PROOF. Since $\det\bar{\rho}(\mathrm{Frob}_q) = q$, we find that $\det\bar{\rho}(\mathrm{Frob}_q) = 1$ 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 $q + 1 - \mathrm{trace}(\bar{\rho}(\mathrm{Frob}_q)) = 0$. Since $q \equiv 1 \pmod{p}$, it follows that p divides $\#\widetilde{E}(\mathbb{F}_q)$ if and only if $\mathrm{trace}(\bar{\rho}(\mathrm{Frob}_q)) = 2$. □

LEMMA 4.8. *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 $\mathrm{GL}_2(\mathbb{F}_p)$ with trace 2 and determinant 1. These matrices are all of the form $g = \left(\begin{smallmatrix} a & b \\ c & 2-a \end{smallmatrix}\right)$, where $a(2-a) - bc = 1$. We count the number 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,

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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

THEOREM 4.9. *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) *$\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = 0$ 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) *$\operatorname{Sel}_{p^{\infty}}(E/L_q) \neq 0$;*
(ii) *either, $\operatorname{rank}_{\mathbb{Z}} E(L_q) > 0$ or $Ш(E/L_q)[p^{\infty}] \neq 0$ (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 4.7 that if $\operatorname{Frob}_q \in \mathcal{S}$, then $q \equiv 1 \pmod{p}$ and $p \mid \#E(\mathbb{F}_q)$. Note that $\Sigma_{L_q} = \{q\}$ and E has good reduction at q. Since $p \mid \#E(\mathbb{F}_q)$, it follows from Proposition 4.1 that $\operatorname{Sel}_{p^{\infty}}(E/L_q) \neq 0$. Therefore, by the Chebotarev density theorem and Lemma 4.8,

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

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 ℓ ($\neq p$) satisfying either of the following properties:

(i) ℓ is a prime of good reduction of E that 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 that is inert in $K/\mathbb{Q}$ and the Tamagawa number c_ℓ is divisible by p.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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

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

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

LEMMA 5.3. *With notation as above,*

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

PROOF. See [Mat09, Proposition 4.3]. □

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, we get the following theorem.

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

PROOF. See [Mat09, Proposition B]. □

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

QUESTION 5.5. Given an elliptic curve $E_{/\mathbb{Q}}$ and a fixed nonnegative integer n, varying over all quadratic number fields ordered by a conductor, what is the minimal conductor of a number field such that one can guarantee $Ш(E/K)[2] \geq n$?

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 Waldspurger (see [BFH90, Theorem in Section 0]) and 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

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

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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

Using the Kummer sequence, we see that

$$\begin{aligned}\operatorname{rank}_2 Ш(E/K)[2] &\geq \operatorname{rank}_2 \operatorname{Sel}_2(E/K) - \operatorname{rank}_{\mathbb{Z}}(E/K) - 2\\ &\geq k - 6 - \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})).\end{aligned}$$

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 that ramify in K. Using the proof of Matsuno as our inspiration, combined with more recent results of K. Ono, we 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 for 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

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

for 100% of the time, $\operatorname{rank}_{\mathbb{Z}}(E(K)) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$ or $\operatorname{rank}_{\mathbb{Z}}(E(K)) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})) + 1$. 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 100% of the quadratic fields K,

$$\begin{aligned}\operatorname{rank}_2 Ш(E/K)[2] &\geq \operatorname{rank}_2 \operatorname{Sel}_2(E/K) - \operatorname{rank}_{\mathbb{Z}}(E(K)) - 2\\ &\geq k - 7 - \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q})).\end{aligned} \tag{5-1}$$

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 $\operatorname{rank}_2 Ш(E/K)[2] \geq n$. Let $\mathcal{P} = \{\ell_1, \ldots, \ell_k\}$ 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 Equation (5-1), we need that

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

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 nonnegative 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.

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

To answer our question, we need to carefully pick the distinct primes $\ell_1, \ldots, \ell_k$. 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 $\ell_1 \sim \log(\omega(N)) \sim \log_{(3)}(N)$. 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 $\ell_1 \sim c \cdot \log(\omega(N))$, 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, $\ell_1 \sim \log(\omega(N))$. 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 $\ell_2 \sim \log(\omega(N) + 1)$. Continuing this process,

$$\begin{aligned} \mathfrak{f} = \prod_{i=1}^{k} \ell_i &\sim \prod_{i=1}^{k} (\log(\omega(N) + (i-1))) \\ &\sim \frac{(\log(\omega(N) - 1 + k))^{\omega(N)+2+k}}{\exp \operatorname{li}(\omega(N) - 1 + k)} \\ &\sim \frac{(\log n)^{n+c}}{\exp \operatorname{li}(n)}, \end{aligned} \tag{5-2}$$

where $\operatorname{li}(x) := \int_0^x (dt/\log t)$ 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

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

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 $A(x) = \sum_{n \le x} a(n)$,

$$\begin{aligned} &\log P(k) \\ &= \sum_{i=1}^{k} \log\log(\omega(N) - 1 + i) \\ &= k \log\log(\omega(N) - 1 + k) - \int_0^k \frac{\lfloor x \rfloor}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)}\, dx \\ &= k \log\log(\omega(N) - 1 + k) - \int_0^k \frac{x}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)}\, dx \\ &\quad + O\Big(\int_0^k \frac{dx}{(\omega(N) - 1 + x)\log(\omega(N) - 1 + x)} \Big) \end{aligned}$$

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

$$
\begin{aligned}
&= k\log\log(\omega(N)-1+k) - (\mathrm{li}(\omega(N)-1+x) - (\omega(N)-1)\log\log(\omega(N)-1+x))\big|_0^k \\
&\quad + O\Big(\int_0^k \frac{dx}{(\omega(N)-1+x)\log(\omega(N)-1+x)}\Big) \\
&= k\log\log(\omega(N)-1+k) - \mathrm{li}(\omega(N)-1+k) + (\omega(N)-1)\log\log(\omega(N)-1+k) \\
&\quad + O(\log\log(\omega(N)-1+k)) \\
&= (k+\omega(N)+1)\log\log(\omega(N)-1+k) - \mathrm{li}(\omega(N)-1+k) \\
&\quad + O(\log\log(\omega(N)-1+k)).
\end{aligned}
$$

This tells us that

$$
\begin{aligned}
P(k) &= \exp((k+\omega(N)+1)\log\log(\omega(N)-1+k) - \mathrm{li}(\omega(N)-1+k) \\
&\qquad + O(\log\log(\omega(N)-1+k))) \\
&= \frac{\exp((k+\omega(N)+1)\log\log(\omega(N)-1+k))}{\exp(\mathrm{li}(\omega(N)-1+k))}(\exp(O(\log\log(\omega(N)-1+k)))) \\
&= \frac{\exp((k+\omega(N)+1)\log\log(\omega(N)-1+k))}{\exp(\mathrm{li}(\omega(N)-1+k))}(O(\log(\omega(N)-1+k))) \\
&= \frac{\log(\omega(N)-1+k)^{k+\omega(N)+2}}{\exp(\mathrm{li}(\omega(N)-1+k))}.
\end{aligned}
$$

To obtain Equation (5-2), 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 5.6. *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 $\mathfrak{f}_K \sim (\log n)^{n+c}/\exp \mathrm{li}(n)$ such that $\mathrm{rank}_2\, Ш(E/K)[2] \geq n$. 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 $\mathrm{rank}_2\, Ш(E/K)[2] \geq n$.

For this section, we consider elliptic curves $E_{/\mathbb{Q}}$ that have no exceptional primes p, that is, no primes p such that the mod p Galois representation attached to E is nonsurjective. 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)

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

that there is a set of primes (call it S) with positive Frobenius density (that is, 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 $\mathrm{Gal}(L/\mathbb{Q})$) 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. However, 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 that 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, that is, $L = \mathbb{Q}$. 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

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

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

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

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

We have therefore proven the following result.

THEOREM 5.7. *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 $\mathfrak{f}_K \sim (\log n)^{n+c}/\exp \mathrm{li}(n)$ such that $\mathrm{rank}_2\, Ш(E/K)[2] \geq n$. Here, c is an explicit constant depending only on E.*

5.2. Arbitrarily large $Ш$ 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

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

It follows that

$$\mathrm{rank}_p\, \mathrm{Sel}_p(E/F) = \mathrm{rank}_{\mathbb{Z}}(E(F)) + \mathrm{rank}_p\, E(F)[p] + \mathrm{rank}_p\, Ш(E/F)[p]. \tag{5-3}$$

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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

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

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

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 $T_{E/L} \supseteq T_{E/F_{(n)}}$, that is, $\mathfrak{f}(F_{(n)}) \mid \mathfrak{f}(L)$. For each such L,

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

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

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

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) $\operatorname{rank}_{\mathbb{Z}}(E(L)) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$.

Thus, given n, there exists a cyclic extension $L/\mathbb{Q}$ of degree $p \geq 7$ such that Equation (5-3) becomes

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

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

We feel that the full force of the conjecture of David, Fearnley, and Kisilevsky is required. In particular, we do not see if the result of Mazur and 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 $\operatorname{rank}_{\mathbb{Z}}(E(\mathcal{L})) = \operatorname{rank}_{\mathbb{Z}}(E(\mathbb{Q}))$, 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:

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

for $3 \leq p < 50$ and $q \leq 179\,424\,673$ (that is, the first 10 million primes).

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,

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

TABLE 2. Proportion of enemy primes.

E	5	7	11	13	17	19
$p/2(p+1)(p-1)^2$	0.002 604	0.012 153	0.004 583	0.003 224	0.001 845	0.001 466
27a	0.020 833	0.013 881	–	0.003 471	–	0.001 533
36a	–	0.013 880	–	0.003 471	–	0.001 538
49a	–	–	0.004 989	–	–	–
64a	0.031 260	–	–	0.003 478	0.001 950	–
E	23	29	31	37	41	43
$p/2(p+1)(p-1)^2$	0.000 990	0.000 616	0.000 538	0.000 376	0.000 305	0.000 277
27a	–	–	0.000 551	0.000 424	–	0.000 279
36a	–	–	0.000 550	0.000 422	–	0.000 282
49a	0.001 028	0.000 638	–	0.000 423	–	0.000 282
64a	–	0.000 640	–	0.000 426	0.000 312	–

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 $p/2(p+1)(p-1)^2$ 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 are obtained from the code available here.

Acknowledgements

LB and DK thank Rahul Arora, Christopher Keyes, Debasis Kundu, Allysa Lumley, Jackson Morrow, Kumar Murty, Mohammed Sadek, and Frank Thorne for helpful discussions during the preparation of this article. LB and DK thank Henri Darmon for his continued support. This work was initiated by LB and DK during the thematic semester 'Number Theory – Cohomology in Arithmetic' at Centre de Recherches Mathématiques (CRM) in Fall 2020. LB and DK thank the CRM for the hospitality and generous support. AR thanks Ravi Ramakrishna, R. Sujatha, and Tom Weston for their support and guidance, and thanks Larry Washington for helpful conversations. We thank Henri Darmon, Chantal David, Antonio Lei, Robert Lemke Oliver, Jackson Morrow, Ross Paterson, Ravi Ramakrishna, and Larry Washington for their comments on an earlier draft of this paper. We thank the referee for the timely review and for the suggestions that led to various improvements in the exposition.

References

[Apo76] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics (Springer-Verlag, New York–Heidelberg, 1976).

[BCH+66] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa and J.-P. Serre, *Seminar on Complex Multiplication: Seminar Held at the Institute for Advanced Study, Princeton, NY, 1957–58*, Lecture Notes in Mathematics, 21 (Springer, Berlin–Heidelberg, 1966).

[BFH90] D. Bump, S. Friedberg and J. Hoffstein, 'Nonvanishing theorems for L-functions of modular forms and their derivatives', *Invent. Math.* **102** (1990), 543–618.

[Bir68] B. J. Birch, 'How the number of points of an elliptic curve over a fixed prime field varies', *J. Lond. Math. Soc. (2)* **1**(1) (1968), 57–60.

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

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

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

[BS15a] M. Bhargava and A. Shankar, 'Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves', *Ann. of Math. (2)* **181** (2015), 191–242.

[BS15b] M. Bhargava and A. Shankar, 'Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0', *Ann. of Math. (2)* **181** (2015), 587–621.

[Čes17] K. Česnavičius, '*p-Selmer growth in extensions of degree p*', *J. Lond. Math. Soc. (2)* **95**(3) (2017), 833–852.

[Coj04] A. C. Cojocaru, 'Questions about the reductions modulo primes of an elliptic curve', in: *Proceedings of the 7th Meeting of the Canadian Number Theory Association* (eds. H. Kisilevsky and E. Z. Goren) (American Mathematical Society, Providence, RI, 2004), 61–79.

[CS00] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves* (Narosa, New Delhi, India, 2000).

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

[CS21] J. E. Cremona and M. Sadek, 'Local and global densities for Weierstrass models of elliptic curves', Preprint, 2021, arXiv:2003.08454.

[DEvH+21] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow and D. Zureick-Brown, 'Sporadic cubic torsion', *Algebra Number Theory* **15**(7) (2021), 1837–1864.

[DFK07] C. David, J. Fearnley and H. Kisilevsky, 'Vanishing of L-functions of elliptic curves over number fields', in: *Ranks of Elliptic Curves and Random Matrix Theory*, London Mathematical Society Lecture Note Series, 341 (eds. J. B. Conrey, D. W. Farmer, F. Mezzadri and N. C. Snaith) (Cambridge University Press, Cambridge, 2007), 247–259.

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

[Dok07] T. Dokchitser, 'Ranks of elliptic curves in cubic extensions', *Acta Arith.* **4**(126) (2007), 357–360.

[Duk97] W. Duke, 'Elliptic curves with no exceptional primes', *Proc. Acad. Sci. Ser. 1, Math.* **325**(8) (1997), 813–818.

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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

[Gre99] R. Greenberg, 'Iwasawa theory for elliptic curves', in: *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, Lecture Notes in Mathematics, 1716 (ed. C. Viola) (Springer, Berlin–Heidelberg, 1999), 51–144.

[HKR21] J. Hatley, D. Kundu and A. Ray, 'Statistics for anticyclotomic Iwasawa invariants of elliptic curves', Preprint, 2021, arXiv:2106.01517.

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

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

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

[JKS04] D. Jeon, C. H. Kim and A. Schweizer, 'On the torsion of elliptic curves over cubic number fields', *Acta Arith.* **113** (2004), 291–301.

[JR08] J. W. Jones and D. P. Roberts, 'Number fields ramified at one prime', in: *International Algorithmic Number Theory Symposium* (eds. A. J. van der Poorten and A. Stein) (Springer, Berlin–Heidelberg, 2008), 226–239.

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

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

[Kid03] M. Kida, 'Variation of the reduction type of elliptic curves under small base change with wild ramification', *CEJOR Cent. Eur. J. Oper. Res.* **1**(4) (2003), 510–560.

[KM88] M. A. Kenku and F. Momose, 'Torsion points on elliptic curves defined over quadratic fields', *Nagoya Math. J.* **109** (1988), 125–149.

[Kol89] V. A. Kolyvagin, 'Finiteness of and for a subclass of Weil curves', *Math. USSR-Izv.* **32**(3) (1989), 523.

[KR21a] D. Kundu and A. Ray, 'Statistics for Iwasawa invariants of elliptic curves', *Trans. Amer. Math. Soc.* **374** (2021), 7945–7965; doi:10.1090/tran/8478.

[KR21b] D. Kundu and A. Ray, 'Statistics for Iwasawa invariants of elliptic curves, II', Preprint, 2021, arXiv:2106.12095.

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

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

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

[Maz77] B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* **47**(1) (1977), 33–186.

[Maz78] B. Mazur, 'Rational isogenies of prime degree', *Invent. Math.* **44**(2) (1978), 129–162.

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

[MP22] A. Morgan and R. Paterson, 'On 2-Selmer groups of twists after quadratic extension', *J. Lond. Math. Soc. (2)* **105**(2) (2022), 1110–1166.

[MR19] B. Mazur and K. Rubin, 'Arithmetic conjectures suggested by the statistical behavior of modular symbols', Preprint, 2020, arXiv:1910.12798.

[MRL18] B. Mazur, K. Rubin and M. Larsen, 'Diophantine stability', *Amer. J. Math.* **140**(3) (2018), 571–616.

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

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

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press

[NSW13] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften, 323 (Springer, Berlin–Heidelberg, 2013).
[Ono01] K. Ono, 'Nonvanishing of quadratic twists of modular *L*-functions and applications to elliptic curves', *J. reine angew. Math.* **533** (2001), 81–97.
[Poo18] B. Poonen, 'Heuristics for the arithmetic of elliptic curves', in: *Proceedings of the International Congress of Mathematicians-Rio de Janeiro*, vol. 2 (eds. B. Sirakov, P. N. de Souza and M. Viana) (World Scientific, Hackensack, NJ, 2018), 399–414.
[PPVW19] J. Park, B. Poonen, J. Voight and M. M. Wood, 'A heuristic for boundedness of ranks of elliptic curves', *J. Eur. Math. Soc. (JEMS)* **21**(9) (2019), 2859–2903.
[RS19] A. Ray and R. Sujatha, 'Euler characteristics and their congruences in the positive rank setting', *Canad. Math. Bull.* **64** (2021), 228–245.
[RS20] A. Ray and R. Sujatha, 'Euler characteristics and their congruences for multisigned Selmer groups', *Canad. J. Math.* (2023), 298–321.
[Sag20] Sage Developers. *Sage Math, the Sage Mathematics Software System (Version 9.2)*, 2020. https://www.sagemath.org.
[Ser74] J.-P. Serre, 'Divisibilité de certaines fonctions arithmétiques', *Sém. Delange-Pisot-Poitou. Théor. Nombres* **16**(1) (1974), 1–28.
[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 2009).
[ST68] J.-P. Serre and J. Tate, 'Good reduction of abelian varieties', *Ann. of Math. (2)* **88** (1968), 492–517.
[Wan15] J. Wang, 'On the torsion structure of elliptic curves over cubic number fields', PhD Thesis, 2015.
[Was97] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, 83 (Springer, New York, 1997).
[Was08] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography* (CRC Press, Boca Raton, FL, 2008).

LEA BENEISH, Department of Mathematics, University of California, Berkeley, 970 Evans Hall, Berkeley, CA 94720, USA
e-mail: leabeneish@berkeley.edu

DEBANJANA KUNDU, 222 College Street, Fields Institute, ON M5T 3J1, Canada
e-mail: dkundu@math.toronto.edu

ANWESH RAY, Centre de recherches mathématiques, Université de Montréal, Pavillon André-Aisenstadt, 2920 Chemin de la tour, Montréal (Québec) H3T 1J4, Canada
e-mail: anwesh.ray@umontreal.ca

https://doi.org/10.1017/S1446788723000034 Published online by Cambridge University Press