STATISTICS FOR IWASAWA INVARIANTS OF ELLIPTIC CURVES

DEBANJANA KUNDU AND ANWESH RAY

ABSTRACT. We study the average behaviour of the Iwasawa invariants for the Selmer groups of elliptic curves, setting out new directions in arithmetic statistics and Iwasawa theory.

1. INTRODUCTION

Iwasawa theory began as the study of class groups over infinite towers of number fields. In [17], B. Mazur initiated the study of Iwasawa theory of elliptic curves. The main object of study is the p-primary Selmer group of an elliptic curve E, taken over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Mazur conjectured that when p is a prime of good ordinary reduction, the p-primary Selmer group is cotorsion as a module over the Iwasawa algebra, denoted by Λ. This conjecture was settled by K. Kato, see [13, Theorem 17.4].

Note that the Iwasawa algebra Λ is isomorphic to the power series ring $\mathbb{Z}_p[\![T]\!]$. The algebraic structure of the Selmer group (as a Λ-module) is encoded by certain invariants which have been extensively studied. First consider the case when E has good ordinary reduction at p. By the p-adic Weierstrass Preparation Theorem, the characteristic ideal of the Pontryagin dual of the Selmer group is generated by a unique element $f_E^{(p)}(T)$, that can be expressed as a power of p times a distinguished polynomial. The μ-invariant is the power of p dividing $f_E^{(p)}(T)$ and the λ-invariant is its degree. R. Greenberg has conjectured that when the residual representation on the p-torsion subgroup of E is irreducible, then the μ-invariant of the Selmer group vanishes, see [11, Conjecture 1.11]. Further, if the p-primary part of the Tate-Shafarevich group, denoted by $\text{Ш}(E/\mathbb{Q})[p^\infty]$, is finite, then one can show that the λ-invariant is at least as large as the Mordell-Weil rank of E (see Lemma 3.3). However, this λ may indeed be strictly larger than the rank, and one of our main objectives is to determine its behaviour on average.

When E has supersingular reduction at p, the Selmer group is not Λ-cotorsion. This makes the analysis of the algebraic structure of the torsion part of the Selmer group particularly difficult. Instead, we consider the plus and minus Selmer groups introduced by S. Kobayashi in [15], which are known to be Λ-cotorsion. The Iwasawa invariants μ^+ and λ^+ (resp. μ^- and λ^-) of the plus (resp. minus) Selmer group are defined in an analogous manner. In the supersingular case as well, there is much computational evidence towards the conjecture that the μ-invariants μ^+ and μ^- vanish. Once again, under standard hypotheses on the Tate-Shafarevich group, both λ^+ and λ^- are known to be greater than or equal to the Mordell-Weil rank of E (see Lemma 3.3).

The main goal of this article is prove results about the variation of the Iwasawa invariants as the pair (E, p) varies such that E has good reduction (ordinary or supersingular) at p. More precisely, we analyze the following two separate but interrelated problems.

(1) For a fixed elliptic curve E, how do the Iwasawa invariants vary as p varies over all odd primes p at which E has good reduction?
(2) For a fixed prime p, how do the Iwasawa invariants vary as E varies over all elliptic curves (with good reduction at p)?

Greenberg studied the first question when $E_{/\mathbb{Q}}$ has rank zero and p varies over the primes of good ordinary reduction (see [11, Theorems 4.1 and 5.1]). In Theorem 3.8, we generalize this result to include the case of supersingular primes. We show that a conjecture of J. Coates and R. Sujatha on the vanishing of μ-invariants of fine Selmer groups holds for density one primes (see Corollary 3.10). Under natural assumptions, we prove similar results for higher rank elliptic curves (see Theorems 3.13 and 3.16). The results in both ordinary and supersingular cases lead us to make the following conjecture (which is proved for elliptic curves of rank zero).

Conjecture. Let $E_{/\mathbb{Q}}$ be an elliptic curve of rank r_E. For 100% of the primes p at which E has good ordinary reduction (resp. supersingular), $\mu = 0$ and $\lambda = r_E$ (resp. $\mu^+ = \mu^- = 0$ and $\lambda^+ = \lambda^- = r_E$).

The second question is at the intersection of arithmetic statistics and Iwasawa theory. The area of arithmetic statistics concerns the behaviour of number theoretic objects in families, and offers a probabilistic model that seeks to explain numerous phenomena in the statistical behaviour of Selmer groups. The investigations in this paper show that there is promise in the analysis of the average behaviour of Iwasawa invariants. The main results we prove are Theorems 4.3, 4.4 and 4.5. Our results indicate that it is reasonable to expect that for a fixed prime p, as we vary over all rank 0 elliptic curves over $\mathbb{Q}$ with good ordinary (resp. supersingular) reduction at p ordered by height, a positive proportion of them have trivial p-primary Selmer group (considered over the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$). In fact, the results suggest that the proportion of elliptic curves of rank 0 with trivial p-primary Selmer group approaches 100% as $p \to \infty$ (see Conjecture 4.7).

2. Background and Preliminaries

2.1. Let $\Gamma := \mathrm{Gal}(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \simeq \mathbb{Z}_p$. The Iwasawa algebra Λ is the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$. After fixing a topological generator γ of Γ, there is an isomorphism of rings $\Lambda \cong \mathbb{Z}_p[\![T]\!]$, by sending $\gamma - 1$ to the formal variable T.

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

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

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

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

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

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

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

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

2.2. Let E be an elliptic curve over $\mathbb{Q}$ with good reduction at p. It shall be assumed throughout that the prime p is odd. Let N denote the conductor of E and set S to denote the set of primes which divide Np. Let $\mathbb{Q}_S$ be the maximal algebraic extension of $\mathbb{Q}$ which is unramified at the primes $v \notin S$. Set $E[p^\infty]$ to be the Galois module of all p-power torsion points in $E(\overline{\mathbb{Q}})$.

First, consider the case when E has good (ordinary or supersingular) reduction at p. Let v be a prime in S. For any finite extension $L/\mathbb{Q}$ contained in $\mathbb{Q}^{\mathrm{cyc}}$, write

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

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

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

This Selmer group fits into a short exact sequence

(2.1) $$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to \mathrm{III}(E/\mathbb{Q})[p^\infty] \to 0,$$

see [5]. Here, $\mathrm{III}(E/\mathbb{Q})$ is the *Tate-Shafarevich group*

$$\mathrm{III}(E/\mathbb{Q}) := \left\{ H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E(\overline{\mathbb{Q}})) \to \prod_l H^1(\overline{\mathbb{Q}}_l/\mathbb{Q}_l, E(\overline{\mathbb{Q}}_l)) \right\}.$$

Throughout this article, we assume that $\mathrm{III}(E/\mathbb{Q})$ is finite. Now, define

$$J_v(E/\mathbb{Q}^{\mathrm{cyc}}) = \varinjlim J_v(E/L)$$

where L ranges over the number fields contained in $\mathbb{Q}^{\mathrm{cyc}}$ and the inductive limit is taken with respect to the restriction maps. Taking direct limits, the *p-primary Selmer group over $\mathbb{Q}^{\mathrm{cyc}}$* is defined as follows

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

As mentioned in the introduction, when p is a prime of good supersingular reduction, the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}^{\mathrm{cyc}})$ is not Λ-torsion. In this case, one studies the plus and minus Selmer groups which we describe below.

Let $E_{/\mathbb{Q}}$ be an elliptic curve with supersingular reduction at p. Denote by $\mathbb{Q}_n^{\mathrm{cyc}}$ the n-th layer in the cyclotomic $\mathbb{Z}_p$-extension, with $\mathbb{Q}_0^{\mathrm{cyc}} := \mathbb{Q}$. Set $\widehat{E}$ to be the formal group of E over $\mathbb{Z}_p$. Let L be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_L$, let $\widehat{E}(L)$ denote $\widehat{E}(\mathfrak{m}_L)$, where $\mathfrak{m}_L$ is the maximal ideal in L. Write $\mathfrak{p}$ for the (unique) prime above p in $\mathbb{Q}^{\mathrm{cyc}}$, and for the prime above p in every finite layer of the cyclotomic tower. Define the plus and minus norm groups as follows

$$\widehat{E}^+(\mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}}) := \left\{ P \in \widehat{E}(\mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}}) \mid \mathrm{tr}_{n/m+1}(P) \in \widehat{E}(\mathbb{Q}_{m,\mathfrak{p}}^{\mathrm{cyc}}),\ \text{for}\ 0 \le m < n\ \text{and}\ m\ \text{even} \right\},$$

$$\widehat{E}^-(\mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}}) := \left\{ P \in \widehat{E}(\mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}}) \mid \mathrm{tr}_{n/m+1}(P) \in \widehat{E}(\mathbb{Q}_{m,\mathfrak{p}}^{\mathrm{cyc}}),\ \text{for}\ 0 \le m < n\ \text{and}\ m\ \text{odd} \right\},$$

where $\mathrm{tr}_{n/m+1} : \widehat{E}(\mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}}) \to \widehat{E}(\mathbb{Q}_{m+1,\mathfrak{p}}^{\mathrm{cyc}})$ denotes the trace map with respect to the formal group law on $\widehat{E}$. The completion $\mathbb{Q}_{\mathfrak{p}}^{\mathrm{cyc}}$ is the union of completions $\bigcup_{n\ge 1} \mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}}$, and set $\widehat{E}^{\pm}(\mathbb{Q}_{\mathfrak{p}}^{\mathrm{cyc}}) := \bigcup_{n\ge 1} \widehat{E}^{\pm}(\mathbb{Q}_{n,\mathfrak{p}}^{\mathrm{cyc}})$. Define

$$J_p^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}}) := \frac{H^1(\mathbb{Q}_{\mathfrak{p}}^{\mathrm{cyc}}, E[p^\infty])}{\widehat{E}^{\pm}(\mathbb{Q}_{\mathfrak{p}}^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p},$$

where the inclusion

$$\widehat{E}^{\pm}(\mathbb{Q}_{\mathfrak{p}}^{\mathrm{cyc}}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}_{\mathfrak{p}}^{\mathrm{cyc}}, E[p^{\infty}])$$

is induced via the Kummer map. For $v \in S \setminus \{p\}$, set $J_v^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}})$ to be equal to $J_v(E/\mathbb{Q}^{\mathrm{cyc}})$. The *plus and minus Selmer groups* are defined as follows

$$\mathrm{Sel}_{p^{\infty}}^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}}) := \ker \left\{ H^1\left(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}, E[p^{\infty}]\right) \to \bigoplus_{v \in S} J_v^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}}) \right\}.$$

For each choice of sign $\ddagger \in \{+, -\}$, set $f_E^{(p),\ddagger}(T)$ to denote the characteristic element of $\mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})^{\vee}$, with $\mu_p^{\ddagger}(E)$, $\lambda_p^{\ddagger}(E)$ defined analogously.

Let E be an elliptic curve with good (ordinary or supersingular) reduction at $p \geq 5$. In order to state results in both ordinary and supersingular case at once, we set for the remainder of the article the following notation,

$$\mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}}) := \begin{cases} \mathrm{Sel}_{p^{\infty}}^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}}) & \text{if } E \text{ has supersingular reduction at } p, \text{ where } \ddagger = \pm, \\ \mathrm{Sel}_{p^{\infty}}(E/\mathbb{Q}^{\mathrm{cyc}}) & \text{if } E \text{ has ordinary reduction at } p. \end{cases}$$

2.3. Next, we introduce the fine Selmer group. Let E be an elliptic curve over $\mathbb{Q}$ and p be any odd prime. At each prime $v \in S$, set

$$\mathcal{K}_v(E/\mathbb{Q}^{\mathrm{cyc}}) := \bigoplus_{\eta | v} H^1(\mathbb{Q}_{\eta}^{\mathrm{cyc}}, E[p^{\infty}]).$$

The *p-primary fine Selmer group* of E is defined as follows

$$\mathrm{Sel}_{p^{\infty}}^0(E/\mathbb{Q}^{\mathrm{cyc}}) := \ker \left\{ H^1(\mathbb{Q}_S/\mathbb{Q}^{\mathrm{cyc}}, E[p^{\infty}]) \longrightarrow \bigoplus_{v \in S} \mathcal{K}_v(E/\mathbb{Q}^{\mathrm{cyc}}) \right\}.$$

By the result of Kato mentioned in the introduction, the Pontryagin dual of $\mathrm{Sel}_{p^{\infty}}^0(E/\mathbb{Q}^{\mathrm{cyc}})$ is known to be a cotorsion Λ-module independent of the reduction type at p. Further, it is conjectured that this fine Selmer group is a cotorsion $\mathbb{Z}_p$-module (i.e. the corresponding μ-invariant vanishes), see [6, Conjecture A].

2.4. In what follows, M will be a cofinitely generated cotorsion Λ-module. Note that $H^i(\Gamma, \mathrm{M})$ is always zero for $i \geq 2$.

Lemma 2.1. Let M be a cofinitely generated cotorsion Λ-module. Then,

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{M}^{\Gamma} = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{M}_{\Gamma}.$$

Proof. Note that $H^1(\Gamma, \mathrm{M})$ may be identified with M_{Γ} (see [18, Proposition 1.7.7]). It follows from [12, Theorem 1.1] that

$$\mathrm{corank}_{\Lambda} \mathrm{M} = \mathrm{corank}_{\mathbb{Z}_p} H^0(\Gamma, \mathrm{M}) - \mathrm{corank}_{\mathbb{Z}_p} H^1(\Gamma, \mathrm{M}).$$

Since M is assumed to be cotorsion over Λ, the result follows. $\square$

When the cohomology groups $H^0(\Gamma, \mathrm{M})$ and $H^1(\Gamma, \mathrm{M})$ are finite, the (classical) *Euler characteristic* $\chi(\Gamma, \mathrm{M})$ is defined as the alternating product

$$\chi(\Gamma, \mathrm{M}) = \prod_{i \geq 0} \left(\#H^i(\Gamma, \mathrm{M}) \right)^{(-1)^i}.$$

On the other hand, when the cohomology groups $H^i(\Gamma, M)$ are not finite, there is a generalized version denoted by $\chi_t(\Gamma, M)$. Since $H^1(\Gamma, M)$ is isomorphic to the group of coinvariants $H_0(\Gamma, M) = M_\Gamma$, there is a natural map

$$\Phi_M : M^\Gamma \to M_\Gamma$$

sending $x \in M^\Gamma$ to the residue class of x in M_Γ. We say that the *truncated Euler characteristic* is defined if the kernel and cokernel of Φ_M are finite. In this case, the $\chi_t(\Gamma, M)$ is defined to be the following quotient,

$$\chi_t(\Gamma, M) := \frac{\# \ker(\Phi_M)}{\# \operatorname{cok}(\Phi_M)}.$$

It is easy to check that when $\chi(\Gamma, M)$ is defined, so is $\chi_t(\Gamma, M)$. In fact,

$$\chi_t(\Gamma, M) = \chi(\Gamma, M).$$

Express the characteristic element $f_M^{(p)}(T)$ as a polynomial,

$$f_M^{(p)}(T) = c_0 + c_1 T + \cdots + c_d T^d.$$

Let r_M denote the order of vanishing of $f_M^{(p)}(T)$ at $T = 0$. For $a, b \in \mathbb{Q}_p$, we write $a \sim b$ if there is a unit $u \in \mathbb{Z}_p^\times$ such that $a = bu$.

Lemma 2.2 (S. Zerbes). Let M be a cofinitely generated cotorsion Λ-module. Assume that the kernel and cokernel of Φ_M are finite. Then,

(1) $r_M = \operatorname{corank}_{\mathbb{Z}_p}(M^\Gamma) = \operatorname{corank}_{\mathbb{Z}_p}(M_\Gamma)$.
(2) $c_{r_M} \neq 0$.
(3) $c_{r_M} \sim \chi_t(\Gamma, M)$.

Proof. See [36, Lemma 2.11]. $\square$

In particular, the classical Euler characteristic $\chi(\Gamma, M)$ is defined if and only if $r_M = 0$. When this happens, the constant coefficient $c_0 \sim \chi(\Gamma, M)$.

We specialize the discussion on Euler characteristics to Selmer groups of elliptic curves. Let ‡ be a choice of sign and recall the definition of $\operatorname{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}})$. When E has good ordinary reduction at p, the choice of ‡ is irrelevant. Denote by $\chi_t^\ddagger(\Gamma, E[p^\infty])$ (resp. $\chi^\ddagger(\Gamma, E[p^\infty])$) the truncated (resp. classical) Euler characteristic of the Selmer group $\operatorname{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}})$. The invariants $\mu_p^\ddagger(E)$ and $\lambda_p^\ddagger(E)$ simply refer to $\mu_p(E)$ and $\lambda_p(E)$ when E has good ordinary reduction at p. When E has good ordinary reduction at p, we shall drop the sign ‡ from the notation. It follows from Lemma 2.2 that the truncated Euler characteristic is always an integer.

3. Results for a fixed elliptic curve and varying prime

In this section, we study the variation of the classical and the truncated Euler characteristic as p varies. Fix a pair (E, p) such that

(1) p is odd.
(2) E is defined over $\mathbb{Q}$ and has good reduction at p.

We record some lemmas which are required throughout this section. Recall that when E has good ordinary reduction, $\operatorname{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}})$ simply refers to $\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}^{\mathrm{cyc}})$.

Theorem 3.1. Let $\ddagger \in \{+, -\}$ be a choice of sign. Let $E_{/\mathbb{Q}}$ be an elliptic curve with good reduction at $p > 2$. Then, there is a natural map

$$\operatorname{Sel}_{p^\infty}(E/\mathbb{Q}) \to \operatorname{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}})^\Gamma$$

with finite kernel and cokernel.

Proof. When E has good ordinary reduction at p, this follows from Mazur's control theorem, see [17] or [11, Theorem 1.2]. In the good supersingular reduction case, the result is due to Kobayashi (see [15, Theorem 9.3]). It also follows from [9, Lemma 3.9] (see also [23, Proposition 5.1]). $\square$

The following lemma gives a criterion for when the classical Euler characteristic $\chi^{\ddagger}(\Gamma, E[p^{\infty}])$ is well-defined.

Lemma 3.2. Let $\ddagger \in \{+, -\}$ be a choice of sign. Let $E_{/\mathbb{Q}}$ be an elliptic curve with good reduction at $p > 2$. The following are equivalent.
  (1) The classical Euler characteristic $\chi^{\ddagger}(\Gamma, E[p^{\infty}])$ is well-defined.
  (2) $\mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})^{\Gamma}$ is finite.
  (3) The Selmer group $\mathrm{Sel}_{p^{\infty}}(E/\mathbb{Q})$ is finite.
  (4) The Mordell-Weil group $E(\mathbb{Q})$ is finite, i.e. the Mordell-Weil rank is 0.

Proof. Recall that the Selmer group $\mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})$ is a cotorsion Λ-module. By Lemma 2.1, $\mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})^{\Gamma}$ is finite if and only if $\mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})_{\Gamma}$ is finite. This shows that (1) and (2) are equivalent.

Theorem 3.1 asserts that there is a natural map

$$\mathrm{Sel}_{p^{\infty}}(E/\mathbb{Q}) \to \mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})^{\Gamma},$$

with finite kernel and cokernel. Hence, the conditions (2) and (3) are equivalent. Recall that we have assumed $\text{Ш}(E/\mathbb{Q})$ is finite. Thus, it follows from (2.1) that conditions (3) and (4) are equivalent. $\square$

Lemma 3.3. Let $\ddagger \in \{+, -\}$ be a choice of sign. Let $E_{/\mathbb{Q}}$ be an elliptic curve with good reduction at $p > 2$. Assume that $\chi_t^{\ddagger}(\Gamma, E[p^{\infty}])$ is well-defined and $\text{Ш}(E/\mathbb{Q})[p^{\infty}]$ is finite. Let r_E denote the Mordell-Weil rank of $E(\mathbb{Q})$. Then, r_E is equal to the order of vanishing of $f_E^{(p),\ddagger}(T)$ at $T = 0$. In particular, we have that $\lambda_p^{\ddagger}(E) \geq r_E$.

Proof. Since it is assumed that $\text{Ш}(E/\mathbb{Q})[p^{\infty}]$ is finite, it follows from (2.1) that

$$r_E = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^{\infty}}(E/\mathbb{Q}).$$

By Lemma 2.2, it suffices to show that

$$r_E = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^{\infty}}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})^{\Gamma}.$$

Therefore the result follows from Theorem 3.1. $\square$

Lemma 3.4. Let M be a cofinitely generated and cotorsion Λ-module such that ϕ_{M} has finite kernel and cokernel. Let r_{M} be the order of vanishing of $f_{\mathrm{M}}^{(p)}(T)$ at $T = 0$. Then, the following are equivalent.
  (1) $\chi_t(\Gamma, \mathrm{M}) = 1$,
  (2) $\mu(\mathrm{M}) = 0$ and $\lambda(\mathrm{M}) = r_{\mathrm{M}}$.

Proof. Suppose that $\chi_t(\Gamma, \mathrm{M}) = 1$. Write $f_{\mathrm{M}}^{(p)}(T) = T^{r_{\mathrm{M}}} g_{\mathrm{M}}^{(p)}(T)$ where $g_{\mathrm{M}}^{(p)}(T) \in \Lambda$ and $g_{\mathrm{M}}(0) \neq 0$. By Lemma 2.2,

$$\left| g_{\mathrm{M}}^{(p)}(0) \right|_p^{-1} = \chi_t(\Gamma, \mathrm{M}) = 1.$$

In particular, $f_{\mathrm{M}}^{(p)}(T)$ and $g_{\mathrm{M}}^{(p)}(T)$ are distinguished polynomials. Since $g_{\mathrm{M}}^{(p)}(0)$ is a unit, it follows that $g_{\mathrm{M}}^{(p)}(T)$ is a unit. Since $g_{\mathrm{M}}^{(p)}(T)$ is a distinguished polynomial, it follows that

$$g_{\mathrm{M}}^{(p)}(T) = 1 \text{ and } f_{\mathrm{M}}^{(p)}(T) = T^{r_{\mathrm{M}}}.$$

Therefore, $\mu(\mathrm{M}) = 0$ and $\lambda(\mathrm{M}) = \deg f_M^{(p)}(T) = r_M$.

Conversely, suppose that $\mu(\mathrm{M}) = 0$ and $\lambda(\mathrm{M}) = r_\mathrm{M}$. Since $\mu(\mathrm{M}) = 0$, it follows that $f_\mathrm{M}^{(p)}(T)$ and $g_\mathrm{M}^{(p)}(T)$ are distinguished polynomials. The degree of $f_\mathrm{M}^{(p)}(T)$ is $\lambda_\mathrm{M} = r_\mathrm{M}$. It follows that $g_\mathrm{M}^{(p)}(T)$ is a constant polynomial and hence, $g_\mathrm{M}^{(p)}(T) = 1$. By Lemma 2.2,

$$\chi_t(\Gamma, \mathrm{M}) = \left| g_\mathrm{M}(0) \right|_p^{-1} = 1.$$

$\square$

Proposition 3.5. Let $\ddagger \in \{+, -\}$ be a choice of sign. Let $E_{/\mathbb{Q}}$ be an elliptic curve of Mordell-Weil rank r_E with good reduction at $p > 2$. Suppose that these additional conditions hold.

(i) The truncated Euler characteristic $\chi_t^\ddagger(\Gamma, E[p^\infty])$ is defined.
(ii) $\mathrm{III}(E/\mathbb{Q})[p^\infty]$ is finite.

Then the following statements are equivalent

(1) $\chi_t^\ddagger(\Gamma, E[p^\infty]) = 1$,
(2) $\mu_p^\ddagger(E) = 0$ and $\lambda_p^\ddagger(E) = r_E$.

Proof. Lemma 3.3 asserts that r_E is equal to the order of vanishing of $f_E^{(p),\ddagger}(T)$ at $T = 0$. The assertion follows from Lemma 3.4. $\square$

3.1. **Elliptic curves over $\mathbb{Q}$ with rank zero.** In this subsection, we study the variation of the classical Euler characteristic as p varies over primes of good reduction.

Corollary 3.6. Let E be an elliptic curve over $\mathbb{Q}$ with good reduction at $p > 2$ for which the Mordell-Weil rank of E is zero. The following are equivalent.

(1) $\chi^\ddagger(\Gamma, E[p^\infty]) = 1$,
(2) $\mu_p^\ddagger(E) = 0$ and $\lambda_p^\ddagger(E) = 0$.
(3) $\mathrm{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}})$ is finite.
(4) $\mathrm{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$.

Proof. Since E is assumed to have rank zero, the Tate-Shafarevich group $\mathrm{III}(E/\mathbb{Q})$ is finite. It follows from Lemma 3.2 that the Euler characteristic $\chi^\ddagger(\Gamma, E[p^\infty])$ is well-defined, and by Proposition 3.5 that (1) and (2) are equivalent. From the Structure Theorem of finitely generated Λ-modules, it is clear that (2) and (3) are equivalent conditions. It is known that $\mathrm{Sel}_{p^\infty}^\ddagger(E/\mathbb{Q}^{\mathrm{cyc}})$ contains no proper finite index submodules (see [11, Proposition 4.14] for the case when p is ordinary and [9, Theorem 3.14] for when p is supersingular). Hence, (3) and (4) are equivalent. $\square$

Let $E_{/\mathbb{Q}}$ be an elliptic curve. Denote by S^{bad} the finite set of primes at which E has bad reduction. Denote by S^{good} the primes at which E has good reduction (i.e., either ordinary reduction or supersingular reduction); write $S^{\mathrm{good}} = S^{\mathrm{ord}} \cup S^{\mathrm{ss}}$. When E has good reduction at a fixed prime p, we set $\widetilde{E}$ to denote the reduced curve over $\mathbb{F}_p$.

The following result was initially proved by Greenberg for good ordinary primes.

Theorem 3.7. Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})$ is finite. Let $\Sigma \subset S^{\mathrm{ord}}$ be the set of primes at which p divides $\#\widetilde{E}(\mathbb{F}_p)$. Let $\Sigma' \subset S^{\mathrm{ord}}$ be the finite set of primes p such that either

(1) $p = 2$.
(2) p divides $\#\mathrm{III}(E/\mathbb{Q})$.
(3) p divides the Tamagawa product $\prod_{l \in S^{\mathrm{bad}}} c_l(E)$.

Then for all primes $p \in S^{\mathrm{ord}} \setminus (\Sigma \cup \Sigma')$, we have that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$.

Observe that Σ' is always a finite set. However, the set of primes Σ, referred to as the set of *anomalous primes*, is known to be a set of Dirichlet density zero. The Lang-Trotter Conjecture predicts that the proportion of anomalous primes $p < X$ is $C \cdot \frac{\sqrt{X}}{\log X}$ for some constant C. It has recently been shown that all but a density zero set of elliptic curves have infinitely many anomalous primes [1, Corollary 4.3]. However, in special cases one can in fact show that $C = 0$ [24, §1.1]. By the Hasse inequality, a prime $p \geq 7$ is anomalous for an elliptic curve defined over $\mathbb{Q}$ if and only if $a_p = p + 1 - \#\widetilde{E}(\mathbb{F}_p) = 1$. When $p \geq 7$ and an elliptic curve has 2-torsion, a_p is even and hence $C = 0$. For more examples where the set Σ is finite, and detailed discussion on this subject, we refer the reader to [17, 19, 22].

Proof of Theorem 3.7. Since the Mordell-Weil rank of E is assumed to be zero, the Euler characteristic $\chi(\Gamma, E[p^\infty])$ is well-defined. The following formula for the Euler characteristic is well known (see [5, Theorem 3.3])

$$(3.1) \qquad \chi(\Gamma, E[p^\infty]) \sim \frac{\#\mathrm{III}(E/\mathbb{Q})[p^\infty] \times \left(\prod_{l \in S^{\mathrm{bad}}} c_l(E) \right) \times \left(\#\widetilde{E}(\mathbb{F}_p) \right)^2}{\left(\#E(\mathbb{Q})[p^\infty] \right)^2}.$$

Since the Euler characteristic is an integer, the result follows immediately from Corollary 3.6. $\square$

We prove a similar result for primes of supersingular reduction.

Theorem 3.8. Let E be an elliptic curve over $\mathbb{Q}$ such that $E(\mathbb{Q})$ is finite. Let $\Upsilon \subset S^{\mathrm{ss}}$ be the finite set of primes p such that either

(1) $p = 2$.
(2) p divides $\#\mathrm{III}(E/\mathbb{Q})$.
(3) p divides the Tamagawa product $\prod_{l \in S^{\mathrm{bad}}} c_l(E)$.

Then for all primes $p \in S^{\mathrm{ss}} \setminus \Upsilon$, we have that

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

Proof. Since $E(\mathbb{Q})$ is assumed to be finite, the Euler characteristic $\chi^\pm(\Gamma, E[p^\infty])$ is well-defined. Since E has supersingular reduction at p, $E[p]$ is irreducible as a $G_{\mathbb{Q}}$-module; hence, $E(\mathbb{Q})[p]$ is the trivial group. Finiteness of $E(\mathbb{Q})$ implies that $E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. Therefore

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

By [16, Theorem 5.15], we know that

$$(3.2) \qquad \chi^\pm(\Gamma, E[p^\infty]) = \#\mathrm{III}(E/\mathbb{Q})[p^\infty] \times \left(\prod_{\ell \in S^{\mathrm{bad}}} c_l(E) \right).$$

The result follows from Corollary 3.6. $\square$

Remark 3.9. It is clear that the μ and λ invariants do not change for each of the layers of the cyclotomic $\mathbb{Z}_p$-extension. Let $E_{/\mathbb{Q}}$ be a rank 0 elliptic curve and $p \in S^{\mathrm{ord}} \setminus (\Sigma \cup \Sigma')$ or $p \in S^{\mathrm{ss}} \setminus \Upsilon$. Since $\lambda_p^\ddagger(E) \geq r_E$, the Mordell-Weil rank of the elliptic curve must remain zero at each layer in the cyclotomic $\mathbb{Z}_p$-extension.

The following result gives evidence for the conjecture of Coates and Sujatha on the vanishing of the μ-invariant of fine Selmer groups. In fact, more is true.

Corollary 3.10. Let E be a rank 0 elliptic curve defined over $\mathbb{Q}$. Then, the p-primary fine Selmer group $\mathrm{Sel}_{p^\infty}^0(E/\mathbb{Q}^{\mathrm{cyc}})$ is trivial for density one primes.

Proof. Given any elliptic curve, it has good reduction at all but finitely many primes. When p is a prime of good (ordinary or supersingular) reduction, note that the p-primary fine Selmer group is a subgroup of $\mathrm{Sel}_{p^\infty}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}})$. The result is immediate from Theorems 3.7 and 3.8. $\square$

3.2. **Elliptic curves over $\mathbb{Q}$ with positive rank.** Next, we consider the case when the elliptic curve E has positive rank.

When E has good ordinary reduction at p, there is a notion of the p-adic height pairing, which is the p-adic analog of the usual height pairing, and was studied extensively in [26, 27]. This pairing is conjectured to be non-degenerate, and the p-adic regulator $R_p(E/\mathbb{Q})$ is defined to be the determinant of this pairing.

Theorem 3.11. [B. Perrin-Riou [21], P. Schneider [27, Theorem 2']] Let $E_{/\mathbb{Q}}$ be an elliptic curve of Mordell-Weil rank r_E with good ordinary reduction at p. Assume that

(1) $\mathrm{III}(E/\mathbb{Q})[p^\infty]$ is finite.
(2) the p-adic height pairing is non-degenerate, i.e., the p-adic regulator is non-zero.

Then, the order of vanishing of $f_E^{(p)}(T)$ at $T = 0$ is equal to $r_E := \mathrm{rank}\, E(\mathbb{Q})$. Express $f_E^{(p)}(T)$ as $T^{r_E} g_E^{(p)}(T)$. Then, $g_E^{(p)}(0) \neq 0$ and

$$g_E^{(p)}(0) \sim \frac{\left(\frac{R_p(E/\mathbb{Q})}{p^{r_E}}\right) \times \#\mathrm{III}(E/\mathbb{Q})[p^\infty] \times \left(\prod_{l \in S^{\mathrm{bad}}} c_l(E)\right) \times \left(\#\widetilde{E}(\mathbb{F}_p)\right)^2}{\left(\#E(\mathbb{Q})[p^\infty]\right)^2}.$$

The above theorem implies that the right hand side of the equation is an integer since the left hand side is. This result does not assume that the truncated Euler characteristic is well-defined. The statement is proven in greater generality, in fact, for abelian varieties over number fields.

Corollary 3.12. Let $E_{/\mathbb{Q}}$ be an elliptic curve of Mordell-Weil rank r_E with good ordinary reduction at p. Assume that

(1) $\mathrm{III}(E/\mathbb{Q})[p^\infty]$ is finite.
(2) the p-adic Height pairing is non-degenerate.
(3) the truncated Euler characteristic $\chi_t(\Gamma, E[p^\infty])$ is defined.

Then, we have that

$$\chi_t(\Gamma, E[p^\infty]) \sim \frac{\left(\frac{R_p(E/\mathbb{Q})}{p^{r_E}}\right) \times \#\mathrm{III}(E/\mathbb{Q})[p^\infty] \times \left(\prod_{l \in S^{\mathrm{bad}}} c_l(E)\right) \times \left(\#\widetilde{E}(\mathbb{F}_p)\right)^2}{\left(\#E(\mathbb{Q})[p^\infty]\right)^2}.$$

Proof. The assertion is a direct consequence of Theorem 3.11 and Lemma 2.2. $\square$

To analyze Iwasawa invariants on average, we shall apply Theorem 3.11. Let $E_{/\mathbb{Q}}$ be an elliptic curve. As before, we denote by S^{ord} the set of primes p at which E has good ordinary reduction. Let Σ be the set of anomalous primes and Σ' the finite set of primes for which

(1) $p = 2$,
(2) p divides $\#\mathrm{III}(E/\mathbb{Q})$.
(3) p divides the Tamagawa product $\prod_{l \in S^{\mathrm{bad}}} c_l(E)$.

Denote by v_p the p-adic valuation on $\mathbb{Q}_p$ normalized by $v_p(p) = 1$. Let $\Pi \subset S^{\mathrm{ord}}$ be the set of primes p at which $v_p(R_p(E/\mathbb{Q})) \geq r_E$. In other words, it is the set of primes for which p divides $\left(\frac{R_p(E/\mathbb{Q})}{p^{r_E}}\right)$. When $r_E = 0$, the p-adic regulator $R_p(E/\mathbb{Q}) = 1$, therefore the set Π is empty. On the other hand, the set of primes Π need not be empty when $r_E \geq 1$. The following result generalizes Theorem 3.7 and is an easy consequence of Theorem 3.11.

Theorem 3.13. Let $E_{/\mathbb{Q}}$ be an elliptic curve such that $r_E \geq 1$. Then for all primes $p \in S^{\mathrm{ord}} \setminus (\Sigma \cup \Sigma' \cup \Pi)$, we have that $f_E^{(p)}(T) = T^{r_E}$. In particular, $\mu_p(E) = 0$ and $\lambda_p(E) = r_E$.

Proof. Express the characteristic element $f_E^{(p)}(T)$ as $T^{r_E} g_E^{(p)}(T)$. Theorem 3.11 asserts that $g_E^{(p)}(0) \neq 0$ and

$$g_E^{(p)}(0) \sim \frac{\left(\frac{R_p(E/\mathbb{Q})}{p^{r_E}}\right) \times \#\text{Ш}(E/\mathbb{Q})[p^\infty] \times \left(\prod_{l \in S^{\text{bad}}} c_l(E)\right) \times \left(\#\widetilde{E}(\mathbb{F}_p)\right)^2}{\left(\#E(\mathbb{Q})[p^\infty]\right)^2}.$$

Thus, $g_E^{(p)}(0)$ is a p-adic unit for $p \in S^{\text{ord}} \setminus (\Sigma \cup \Sigma' \cup \Pi)$. Therefore, $g_E^{(p)}(T)$ is a unit in Λ. Since $f_E^{(p)}(T)$ is a product of a distinguished polynomial with a power of p, it follows that $g_E^{(p)}(T) = 1$ and $f_E^{(p)}(T) = T^{r_E}$. $\qquad\square$

While it is known that the set Σ' is finite and Σ is a density zero set of primes, the same is not known for Π. For $N \geq 1$, let $\Pi^{\leq N}$ be the set of primes $p \in \Pi$ for which $5 \leq p \leq N$. Calculations in [4] suggest that the set Π is likely to have Dirichlet density zero, at least for elliptic curves of rank 1 (see also [35]). We compute $\Pi^{\leq 1000}$ for the first 10 elliptic curves $E/\mathbb{Q}$ of rank 2 (ordered by conductor). The calculations in the following table were done on sage.

	Cremona Label	$\Pi^{\leq 1000}$		Cremona Label	$\Pi^{\leq 1000}$
1.	$389a$	$\emptyset$	6.	$643a$	$\emptyset$
2.	$433a$	$\{13\}$	7.	$655a$	$\{7, 31\}$
3.	$446d$	$\{7\}$	8.	$664a$	$\{59\}$
4.	$563a$	$\emptyset$	9.	$681c$	$\emptyset$
5.	$571b$	$\emptyset$	10.	$707a$	$\{29\}.$

Remark 3.14. For elliptic curves $E_{/\mathbb{Q}}$ with $r_E = 1$, the above theorem asserts that for primes outside a set (possibly of Dirichlet density zero), the characteristic element $f_E^{(p)}(T) = T$. Under the hypotheses that the p-adic height pairing on $E(\mathbb{Q}_n^{\text{cyc}})$ is non-degenerate for all n and that $\#\text{Ш}(E/\mathbb{Q}_n^{\text{cyc}})[p^\infty]$ is finite for all n, we know that $f_{\text{Sel}^0}^{(p)}(T) = 1$ (see [34, pp. 104-105]). Thus, in this case, the fine Selmer group $\text{Sel}_{p^\infty}^0(E/\mathbb{Q}^{\text{cyc}})$ is not only cofinitely generated as a $\mathbb{Z}_p$-module, but in fact it is finite. On the other hand, when $r_E > 1$ even though the fine Selmer group should be cofinitely generated as a $\mathbb{Z}_p$-module, it is not expected to be finite.

Next, we consider the supersingular case. Let $E_{/\mathbb{Q}}$ be an elliptic curve with good supersingular reduction at $p \geq 3$. Note that p divides $a_p := p + 1 - \#\widetilde{E}(\mathbb{F}_p)$. Hasse's bound states that $|a_p| < 2\sqrt{p}$; hence if $p \geq 5$, it forces that $a_p = 0$. However, when $p = 3$, it is indeed possible for $a_p \neq 0$. For simplicity, we shall assume that $a_p = 0$. In this setting, the Main conjectures were formulated in [15]. When $a_p = 0$, the Main conjecture has been proved in a preprint of X. Wan (see [32]). Let $\ddagger \in \{+, -\}$ be a choice of sign. Perrin Riou [20] formulated a p-adic L-function in the supersingular case, which is closely related to the plus and minus p-adic L-function defined by R. Pollack. The p-adic Birch and Swinnerton-Dyer conjecture formulated by D. Bernardi and Perrin-Riou in [2] predicts a formula for the leading term of the p-adic L-function. This conjecture is reformulated in terms of Pollack's p-adic L-functions in [31].

Let $\log_p$ be a branch of the p-adic logarithm, χ the p-adic cyclotomic character, and r_E be the Mordell-Weil rank of E. Let $\ddagger \in \{+, -\}$, and denote by $R_p^\ddagger(E/\mathbb{Q})$ the signed p-adic regulator (defined up to p-adic unit). The convention in *loc. cit.* is to choose a generator γ of the cyclotomic $\mathbb{Z}_p$ extension, and divide the regulator (defined w.r.t. the choice of γ) by $\log_p(\chi(\gamma))^{r_E}$. We are

however, not interested in the exact value of the regulator, but only the value up to a p-adic unit. Therefore, we simply work with the fraction $\left(\frac{R_p^{\ddagger}(E/\mathbb{Q})}{p^{r_E}}\right)$. Lemma 3.3 asserts that the order of vanishing of $f_E^{(p),\ddagger}(T)$ at $T = 0$ is equal to r_E. Express $f_E^{(p),\ddagger}(T)$ as a product $T^{r_E}g_E^{(p),\ddagger}(T)$. The following conjecture is equivalent to the p-adic Birch and Swinnerton-Dyer conjecture.

Conjecture 3.15. Let E be an elliptic curve with good supersingular reduction at the prime p and $\ddagger \in \{+, -\}$. Then,

$$g_E^{(p),\ddagger}(0) \sim \left(\frac{R_p^{\ddagger}(E/\mathbb{Q})}{p^{r_E}}\right) \times \#\mathrm{III}(E/\mathbb{Q})[p^{\infty}] \times \left(\prod_{l \in S^{\mathrm{bad}}} c_l(E)\right).$$

Let $\Pi^{\ddagger} \subset S^{\mathrm{ss}}$ be the set of primes p at which $v_p(R_p^{\ddagger}(E/\mathbb{Q})) \geq r_E$. In other words, it is the set of primes for which p divides $\left(\frac{R_p^{\ddagger}(E/\mathbb{Q})}{p^{r_E}}\right)$. The following result is proved using the same strategy as that of Theorem 3.13, so we skip the proof.

Theorem 3.16. Assume that Conjecture 3.15 holds. Let $E_{/\mathbb{Q}}$ be an elliptic curve with Mordell-Weil rank $r_E \geq 1$. Let p be a prime at which E has good supersingular reduction. Then for all primes $p \in S^{\mathrm{ss}} \setminus (\Sigma \cup \Sigma' \cup \Pi^{\ddagger})$, we have that $f_E^{(p),\ddagger}(T) = T^{r_E}$. In particular, $\mu_p^{\ddagger}(E) = 0$ and $\lambda_p^{\ddagger}(E) = r_E$.

It seems reasonable to make the following conjecture.

Conjecture 3.17. Let $E_{/\mathbb{Q}}$ be an elliptic curve of rank r_E with good (ordinary or supersingular) reduction at p. For 100% of the primes, $\mu_p^{\ddagger}(E) = 0$ and $\lambda_p^{\ddagger}(E) = r_E$.

Remark 3.18. Let $E_{/\mathbb{Q}}$ be an elliptic curve with $r_E \geq 1$. If p is a prime at which the p-adic regulator has valuation equal to p^{r_E}, the same argument as Remark 3.9 shows that the rank of the elliptic curve remains unchanged in every layer of the cyclotomic $\mathbb{Z}_p$-extension.

4. Results for a fixed prime and varying elliptic curve

In this section, we fix a prime $p \geq 5$ and study the variation of Iwasawa invariants as E ranges over all elliptic curves of rank zero with good reduction at p. Recall that any elliptic curve E over $\mathbb{Q}$ admits a unique Weierstrass equation

$$(4.1) \qquad\qquad E : y^2 = x^3 + Ax + B$$

where A, B are integers and $\gcd(A^3, B^2)$ is not divisible by any twelfth power. Since $p \geq 5$, such an equation is minimal. We order elliptic curves by height and expect that similar results shall hold when they are ordered by conductor or discriminant. Recall that the *height of E* satisfying the minimal equation (4.1) is given by $H(E) := \max\left(|A|^3, |B|^2\right)$.

Let $\mathcal{E}$ be the set of isomorphism classes of all elliptic curves over $\mathbb{Q}$. Let $\mathcal{J}$ be the set of elliptic curves E over $\mathbb{Q}$ satisfying the following two properties

   (1) E has rank zero,
   (2) E has good reduction (ordinary or supersingular) at p.

The set $\mathcal{J}$ is the (disjoint) union of two sets $\mathcal{J}^{\mathrm{ord}}$ and $\mathcal{J}^{\mathrm{ss}}$, consisting of rank 0 elliptic curves with ordinary and supersingular reduction at p, respectively. For $X > 0$, write $\mathcal{E}(X)$ for the set of isomorphism classes of elliptic curves over $\mathbb{Q}$ of height $< X$. If $\mathcal{S}$ is a subset of $\mathcal{E}$, set $\mathcal{S}(X) = \mathcal{S} \cap \mathcal{E}(X)$. It is conjectured that when ordered by height, discriminant or conductor, half

of the elliptic curves over $\mathbb{Q}$ have rank 0 (see for example [10, Conjecture B] or [14, p. 15]). If $E \in \mathcal{J}$ has good ordinary reduction at p, then the Euler characteristic formula (3.1) states that

(4.2)
$$\chi(\Gamma, E[p^\infty]) \sim \frac{\#\text{III}(E/\mathbb{Q})[p^\infty] \times \left(\prod_l c_l(E)\right) \times \left(\#\widetilde{E}(\mathbb{F}_p)\right)^2}{\#\left(E(\mathbb{Q})[p^\infty]\right)^2}.$$

Note that in the above equation, $\#E(\mathbb{Q})[p^\infty] = 1$ if $p \geq 11$. On the other hand, if $E \in \mathcal{J}$ has good supersingular reduction at p, then by (3.2), we have that

(4.3)
$$\chi^\pm(\Gamma, E[p^\infty]) \sim \#\text{III}(E/\mathbb{Q})[p^\infty] \times \left(\prod_l c_l(E)\right).$$

Denote by $c_l^{(p)}(E)$ the p-part of $c_l(E)$, given by $c_l^{(p)}(E) := p^{v_p(c_l(E))}$. The key observation in this section is that to analyze the variation of the Euler characteristic (and hence μ and λ-invariants) of elliptic curves, it suffices to study the average behaviour of the following quantities for fixed p and varying $E \in \mathcal{J}$,

(1) $s_p(E) := \#\text{III}(E/\mathbb{Q})[p^\infty]$,
(2) $\tau_p(E) := \prod_l c_l^{(p)}(E)$,
(3) $\delta_p(E) := \#\left(\widetilde{E}(\mathbb{F}_p)[p]\right)$.

Definition 4.1. Let $\mathcal{E}_1(X)$, $\mathcal{E}_2(X)$, and $\mathcal{E}_3(X)$ be the subset of elliptic curves in $\mathcal{E}(X)$ for which p divides $s_p(E)$, $\tau_p(E)$ and $\delta_p(E)$ respectively.

Note that no assumptions are made on the rank of elliptic curves in $\mathcal{E}(X)$ or $\mathcal{E}_i(X)$. On the other hand, for elliptic curves $E \in \mathcal{J}$, the rank is zero.

The primary goal is to obtain upper bounds for

$$\mathfrak{d}_p^{(i)} := \limsup_{X \to \infty} \frac{\#\mathcal{E}_i(X)}{\#\mathcal{E}(X)}$$

for $i = 2, 3$ (with no constraints on the rank of the elliptic curves).

In [8], C. Delauney gave heuristics for the average number of elliptic curves with $s_p(E) \neq 1$. These heuristics are stated in terms of elliptic curves ordered by conductor. However, they indicate that $\mathfrak{d}_p^{(1)}$ goes to 0 as $p \to \infty$ rather fast. Since there is still not much known about this particular question, we are unable to make further clarifications about the behaviour of $\mathfrak{d}_p^{(1)}$. However, we expect that the analysis of this part of the formula is the most difficult.

Let $\kappa = (a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ be such that the discriminant $\Delta(\kappa) := 4a^3 + 27b^2$ is nonzero. The elliptic curve $E_\kappa : y^2 = x^3 + ax + b$ defined over $\mathbb{F}_p$ is smooth. Let $d(p)$ be the number of pairs $\kappa = (a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ such that

(1) $\Delta(\kappa) \neq 0$.
(2) $E_\kappa : y^2 = x^3 + ax + b$ has a point over $\mathbb{F}_p$ of order p.

For the primes p in the range $5 \leq p < 500$, computations on sage show that $d(p) \leq 1$ and $d(p) = 1$ for $p \in \{5, 7, 61\}$. We remark that $d(p)$ is closely related to the Kronecker class number of $1 - 4p$ (see [28, p. 184]). The estimate (4.4) follows from the method of M. Sadek [25], or the results of J. Cremona and Sadek, see [7].

Theorem 4.2. Let $p \geq 5$ be a fixed prime number. Then

(4.4)
$$\mathfrak{d}_p^{(2)} \leq \sum_{l \neq p} \frac{(l-1)^2}{l^{p+2}},$$

where the sum is taken over prime numbers $l \neq p$, and

$$(4.5) \qquad \mathfrak{d}_p^{(3)} \leq \zeta(10) \cdot \frac{d(p)}{p^2}.$$

We provide a proof of (4.4) in Theorem 4.11 and of (4.5) in Theorem 4.14. Note that $\zeta(10) = \frac{\pi^{10}}{93555}$ is approximately equal to 1.001. This quantity arises since the proportion of Weierstrass equations ordered by height which are minimal is $\frac{1}{\zeta(10)}$ (see [7]). To avoid confusion, we state the results for good ordinary and good supersingular elliptic curves separately. First, we state the result for elliptic curves with good ordinary reduction at p.

Theorem 4.3. Let $p \geq 5$ be a fixed prime number. Let $\mathcal{Z}^{\mathrm{ord}}$ denote the set of rank 0 elliptic curves E with good ordinary reduction at p for which the following equivalent conditions are satisfied

   (1) $\chi(\Gamma, E[p^\infty]) = 1$,
   (2) $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$.

Then,

$$\limsup_{X \to \infty} \frac{\#\mathcal{Z}^{\mathrm{ord}}(X)}{\#\mathcal{E}(X)} \geq \limsup_{X \to \infty} \frac{\#\mathcal{J}^{\mathrm{ord}}(X)}{\#\mathcal{E}(X)} - \mathfrak{d}_p^{(1)} - \sum_{l \neq p} \frac{(l-1)^2}{l^{p+2}} - \zeta(10) \cdot \frac{d(p)}{p^2}.$$

Proof. It follows from Corollary 3.6 that $\chi(\Gamma, E[p^\infty]) = 1$ and $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}^{\mathrm{cyc}})$ are equivalent. By the Euler characteristic formula (4.2),

$$\limsup_{X \to \infty} \frac{\#\mathcal{Z}^{\mathrm{ord}}(X)}{\#\mathcal{E}(X)} \geq \limsup_{X \to \infty} \frac{\#\mathcal{J}^{\mathrm{ord}}(X)}{\#\mathcal{E}(X)} - \mathfrak{d}_p^{(1)} - \mathfrak{d}_p^{(2)} - \mathfrak{d}_p^{(3)}.$$

The result follows from Theorem 4.2. $\qquad\qquad\square$

Next, we prove an analogous result in the case when E varies over elliptic curves with good supersingular reduction at p.

Theorem 4.4. Let $p \geq 5$ be a fixed prime number. Let $\mathcal{Z}^{\mathrm{ss}}$ be the rank 0 elliptic curves E with good supersingular reduction at p, for which the following equivalent conditions are satisfied

   (1) $\chi^{\pm}(\Gamma, E[p^\infty]) = 1$
   (2) $\mathrm{Sel}_{p^\infty}^{\pm}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$.

Then,

$$\limsup_{X \to \infty} \frac{\#\mathcal{Z}^{\mathrm{ss}}(X)}{\#\mathcal{E}(X)} \geq \limsup_{X \to \infty} \frac{\#\mathcal{J}^{\mathrm{ss}}(X)}{\#\mathcal{E}(X)} - \mathfrak{d}_p^{(1)} - \sum_{l \neq p} \frac{(l-1)^2}{l^{p+2}}.$$

Proof. The proof is identical to that of Theorem 4.3. It is a direct consequence of Corollary 3.6, Theorem 4.2, and the Euler characteristic formula (4.3). $\qquad\qquad\square$

We prove a result which applies for all elliptic curves with good reduction.

Theorem 4.5. Let $p \geq 5$ be a fixed prime number. Let $\mathcal{Z}$ be the set of rank 0 elliptic curves E with good reduction at p, for which $\mathrm{Sel}_{p^\infty}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$. Then,

$$\limsup_{X \to \infty} \frac{\#\mathcal{Z}(X)}{\#\mathcal{E}(X)} \geq \limsup_{X \to \infty} \frac{\#\mathcal{J}(X)}{\#\mathcal{E}(X)} - \mathfrak{d}_p^{(1)} - \sum_{l \neq p} \frac{(l-1)^2}{l^{p+2}} - \zeta(10) \cdot \frac{d(p)}{p^2}.$$

Proof. Let $\mathcal{Y} \subset \mathcal{E}$ consist of the elliptic curves E for which $s_p(E)\tau_p(E)\delta_p(E) \neq 1$. It follows from the Euler characteristic formulas (4.2) and (4.3) that $\mathcal{Z}$ is contained in $\mathcal{E} \setminus \mathcal{Y}$. By Theorem 4.3 that

$$\limsup_{X \to \infty} \frac{\#\mathcal{Y}(X)}{\#\mathcal{E}(X)} \leq \mathfrak{d}_p^{(1)} + \sum_{l \neq p} \frac{(l-1)^2}{l^{p+2}} + \zeta(10) \cdot \frac{d(p)}{p^2}$$

and the result follows. □

Remark 4.6. On average, the proportion of elliptic curves over $\mathbb{Z}_p$ with good reduction at p (ordered by height) is $(1 - \frac{1}{p})$, see [7]. Also, it is expected that $1/2$ the elliptic curves have rank 1 when ordered by height. Therefore, it is reasonable to expect that

$$\limsup_{X \to \infty} \frac{\#\mathcal{J}(X)}{\#\mathcal{E}(X)} = \frac{1}{2}\left(1 - \frac{1}{p}\right).$$

Heuristics of Delauney suggest that $\mathfrak{d}_p^{(1)}$ should approach zero quite rapidly as $p \to \infty$. The result indicates that the proportion of elliptic curves for which the Selmer group is zero is > 0 and the proportion approaches $1/2$ as $p \to \infty$.

We are led to make the following conjecture.

Conjecture 4.7. Let p be a fixed prime. Denote by $\mathcal{J}_p$ the set of rank 0 elliptic curves with good reduction at p, and by $\mathcal{Z}_p$ the subset of elliptic curves for which $\mathrm{Sel}_{p^\infty}^{\ddagger}(E/\mathbb{Q}^{\mathrm{cyc}}) = 0$. Then,

$$\liminf_{p \to \infty}\left(\limsup_{X \to \infty} \frac{\mathcal{Z}_p(X)}{\mathcal{J}_p(X)}\right) = 1.$$

Remark 4.8. In the rank one case, such an analysis is difficult. This is because of the term arising from the p-adic regulator in the formula for the truncated Euler characteristic. At the time of writing, the authors are not aware of any results or heuristics for the average behaviour of the p-adic valuation of $R_p(E/\mathbb{Q})$ as E ranges over all elliptic curves of rank 1 with good ordinary reduction at p.

Theorem 4.2 is proved in the remainder of the section.

4.1. **Average results on Tamagawa numbers.** Let $p \geq 5$ be a fixed prime, and l be a prime different from p. In this section, we estimate the proportion of elliptic curves $E/\mathbb{Q}$ up to height X with Kodaira type I_p at l. These estimates are well known, but we include them for the sake of completeness, see [25, 7]. Recall that when the Kodaira symbol at the prime l is I_p, the Tamagawa number c_l is divisible by p [30, p. 448]. Let $\mathcal{E}(X)$ be the set of isomorphism classes of all elliptic curves over $\mathbb{Q}$ with height $\leq X$. This is in one-to-one correspondence with the set

$$\left\{(A, B) \in \mathbb{Z} \times \mathbb{Z} : \begin{array}{c} |A| \leq \sqrt[3]{X}, |B| \leq \sqrt{X} \\ 4A^3 + 27B^2 \neq 0 \\ \text{for all primes } q \text{ if } q^4|A, \text{then } q^6 \nmid B \end{array}\right\}.$$

Lemma 4.9 (A. Brumer)**.** With notation as above,

$$\#\mathcal{E}(X) = \frac{4X^{5/6}}{\zeta(10)} + O\left(\sqrt{X}\right).$$

Proof. See [3, Lemma 4.3]. □

Consider the set $\mathcal{E}_l^{I_p}(X)$, i.e. the set of elliptic curves over $\mathbb{Q}$ with bad reduction at l, height $\leq X$, and Kodaira type I_p. The Kodaira symbol forces the bad reduction to be of multiplicative type. It follows from Tate's algorithm that this set is in one-to-one correspondence with

$$(4.6) \qquad \left\{(A, B) \in \mathbb{Z} \times \mathbb{Z} : \begin{array}{c} |A| \leq \sqrt[3]{X}, |B| \leq \sqrt{X} \\ l \nmid A, \ l \nmid B, \ l^p \parallel 4A^3 + 27B^3 \\ (A, B) \neq (0,0) \in \mathbb{Z}/q^4 \times \mathbb{Z}/q^6 \text{ for any prime } q \end{array}\right\}.$$

We include both upper and lower bounds, however, we only apply upper bounds in our analysis. The following calculations have been done in the preprint [25, Lemma 4.1]. We clarify the arguments and include them here for completeness.

Lemma 4.10 (Sadek). Let $X > 0$ and l_i be the i-th prime. Let $k > 0$ be the largest positive integer such that $L_k = \prod_{i=1}^{k} l_i \le \sqrt[12]{X}$. Then,

$$4l^p(l-1)^2 \prod_{i=1}^{k}(l_i^{10}-1)\left(\left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}L_k^4}\right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}L_k^6}\right\rfloor - \frac{X^{5/6}}{9l^{2p+2}L_k^{10}l_k^9}\right) \le \#\mathcal{E}_l^{I_p}(X)$$

$$\le 4l^p(l-1)^2 \prod_{i=1}^{k}(l_i^{10}-1)\left(\left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}L_k^4}\right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}L_k^6}\right\rfloor + \frac{\sqrt[3]{X}}{3l^{p+1}L_k^4 l_k^3} + \frac{\sqrt{X}}{5l^{p+1}L_k^6 l_k^5}\right).$$

Proof. To obtain the estimate on the size of the set $\mathcal{E}_l^{I_p}(X)$, we use the description of the set in (4.6). Observe that $l^{p+1} \nmid 4A^3 + 27B^2$, hence the condition $4A^3 + 27B^2 \neq 0$ is inherent in the definition of $\mathcal{E}_l^{I_p}(X)$.

Consider the congruence equation $4A^3 + 27B^2 \equiv 0 \pmod{l}$. It has $l - 1$ non-singular solutions, which lift to $l^{p-1}(l-1)$ solutions modulo l^p (see for example [33, §3.4.1]). Note that the description of the set in (4.6) says that $l \nmid A$ and $l \nmid B$; thereby allowing us to ignore the point $(0, 0)$.

In view of (4.6), we are interested in solutions modulo l^p that fail to satisfy the congruence equation modulo l^{p+1}. Since the $l - 1$ non-singular solutions lift to $l^{p-1}(l-1)$ solutions modulo l^p and $l^p(l-1)$ solutions modulo l^{p+1}, it follows that the number of pairs $(A, B) \in \mathbb{Z}/l^{p+1} \times \mathbb{Z}/l^{p+1}$ such that

(1) $(A, B) \not\equiv (0, 0) \mod l$,
(2) $4A^3 + 27B^2 \equiv 0 \mod l^p$,
(3) $4A^3 + 27B^2 \not\equiv 0 \mod l^{p+1}$,

is equal to

$$l^2 \cdot (l^{p-1}(l-1)) - l^p(l-1) = l^p(l-1)^2.$$

Therefore, $\mathcal{E}_l^{I_p}(X)$ has $l^p(l-1)^2$ pairs of residue classes in $\mathbb{Z}/l^{p+1} \times \mathbb{Z}/l^{p+1}$. Next, we need to count the number of lifts of each such pair under the additional condition that $(A, B) \neq (0, 0) \in \mathbb{Z}/l_i^4 \times \mathbb{Z}/l_i^6$ for each prime l_i. Note that the number of pairs (A, B) satisfying this additional condition is $(l_i^{10} - 1)$.

It follows that the number of pairs (A, B) in the box $[-\sqrt[3]{X}, \sqrt[3]{X}] \times [-\sqrt{X}, \sqrt{X}]$ such that $(A, B) \neq (0, 0) \in \mathbb{Z}/l^{p+1} \times \mathbb{Z}/l^{p+1}$, $(A, B) \neq (0, 0) \in \mathbb{Z}/l_i^4 \times \mathbb{Z}/l_i^6$ and $4A^3 + 27B^2 \equiv 0 \mod l^p$ is

$$4l^p(l-1)^2 \prod_{i=1}^{k}\left(l_i^{10}-1\right)\left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}L_k^4}\right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}L_k^6}\right\rfloor.$$

Our estimate so far might include pairs (A, B) such that it is $(0, 0) \in \mathbb{Z}/q^4 \times \mathbb{Z}/q^6$ when $l_k < q \le \sqrt[12]{X}$. So, we must exclude the integral pairs which reduce to $(0, 0) \in \mathbb{Z}/q^4 \times \mathbb{Z}/q^6$ for $l_k < q \le \sqrt[12]{X}$. Therefore, we need to remove

$$4l^p(l-1)^2 \prod_{i=1}^{k}\left(l_i^{10}-1\right)\sum_{l_k < q \le \sqrt[12]{X}}\left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}q^4 L_k^4}\right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}q^6 L_k^6}\right\rfloor$$

many pairs from our count. Putting this together, we get

$$\#\mathcal{E}_l^{I_p}(X) = 4l^p(l-1)^2 \prod_{i=1}^{k}\left(l_i^{10}-1\right)\left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}L_k^4}\right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}L_k^6}\right\rfloor$$

$$- 4l^p(l-1)^2 \prod_{i=1}^{k}\left(l_i^{10}-1\right)\sum_{l_k < q \le \sqrt[12]{X}}\left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}q^4 L_k^4}\right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}q^6 L_k^6}\right\rfloor.$$

15

To obtain the expression as in the statement of the lemma, we will need to manipulate the following term

$$\sum_{l_k < q \leq \sqrt[12]{X}} \left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}q^4 L_k^4} \right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}q^6 L_k^6} \right\rfloor.$$

First we consider its upper bound.

$$\sum_{l_k < q \leq \sqrt[12]{X}} \left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}q^4 L_k^4} \right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}q^6 L_k^6} \right\rfloor \leq \frac{X^{5/6}}{l^{2(p+1)} L_k^{10}} \sum_{l_k < q \leq \sqrt[12]{X}} 1/q^{10}$$

$$\leq \frac{X^{5/6}}{l^{2(p+1)} L_k^{10}} \int_{l_k}^{\infty} 1/x^{10} dx$$

$$\leq \frac{X^{5/6}}{9 l^{2(p+1)} l_k^9 L_k^{10}}.$$

Now for the lower bound, observe that

$$\sum_{l_k < q \leq \sqrt[12]{X}} \left\lfloor \frac{\sqrt[3]{X}}{l^{p+1}q^4 L_k^4} \right\rfloor \left\lfloor \frac{\sqrt{X}}{l^{p+1}q^6 L_k^6} \right\rfloor \geq \sum_{l_k < q \leq \sqrt[12]{X}} \left(\frac{\sqrt[3]{X}}{l^{p+1}q^4 L_k^4} - 1 \right) \left(\frac{\sqrt{X}}{l^{p+1}q^6 L_k^6} - 1 \right)$$

$$\geq -\frac{\sqrt[3]{X}}{l^{p+1} L_k^4} \sum_{l_k < q \leq \sqrt[12]{X}} 1/q^4 - \frac{\sqrt{X}}{l^{p+1} L_k^6} \sum_{l_k < q \leq \sqrt[12]{X}} 1/q^6$$

$$\geq -\frac{\sqrt[3]{X}}{3 l^{p+1} L_k^4 l_k^3} - \frac{\sqrt{X}}{5 l^{p+1} L_k^6 l_k^5}.$$

The result is now immediate. $\qquad\square$

The following result follows from the previous lemmas in this section.

Theorem 4.11. With notation as above,

$$\limsup_{X \to \infty} \frac{\#\mathcal{E}_l^{I_p}(X)}{\#\mathcal{E}(X)} \leq \frac{(l-1)^2}{l^{p+2}}.$$

Proof. The result follows from using the upper bound of $\mathcal{E}_l^{I_p}(X)$ and Lemma 4.9. $\qquad\square$

Remark 4.12. When the elliptic curves are ordered by conductor (rather than height), the same bounds have been obtained in [29, Theorem 1.6].

4.2. **Average results on anomalous primes.** We fix a prime $p \geq 5$. Let $\mathcal{W}$ consist of tuples $(A, B) \in \mathbb{Z} \times \mathbb{Z}$, where (A, B) is identified with the (minimal) Weierstrass equation

$$y^2 = x^3 + Ax + B.$$

Denote by $\mathcal{W}(X)$ the set of Weierstrass equations for which the height is $\leq X$. Note that $\mathcal{E}(X)$ is a subset of $\mathcal{W}(X)$ such that

(4.7)
$$\lim_{X \to \infty} \frac{\#\mathcal{E}(X)}{\#\mathcal{W}(X)} = \frac{1}{\zeta(10)}$$

(see [7]). Thus 99.9% of Weierstrass equations are globally minimal.

Let $\kappa = (a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ with $\Delta(\kappa) \neq 0$. Let E_κ be the elliptic curve defined by the Weierstrass equation

$$E_\kappa : y^2 = x^3 + ax + b.$$

Note that κ is not uniquely determined by E_κ.

16

Lemma 4.13. Let κ be a pair and $\mathcal{W}_\kappa(X) \subset \mathcal{W}(X)$ be the subset of Weierstrass equations $y^2 = x^3 + Ax + B$ such that the pair (A, B) reduces to κ. Then,

$$\limsup_{X \to \infty} \frac{\#\mathcal{W}_\kappa(X)}{\#\mathcal{E}(X)} \leq \frac{\zeta(10)}{p^2}.$$

Proof. Observe that $\mathcal{W}_{(0,0)}$ is the lattice in $\mathbb{Z} \times \mathbb{Z}$ with lattice basis $(p, 0)$ and $(0, p)$. Since $\mathcal{W}_\kappa$ is simply a translation of $\mathcal{W}_{(0,0)}$, it follows that

$$\lim_{X \to \infty} \frac{\#\mathcal{W}_\kappa(X)}{\#\mathcal{W}(X)} = \frac{1}{p^2}.$$

The result follows from (4.7). $\qquad\square$

Denote by $\mathfrak{S}$ the set of pairs $\kappa = (a, b) \in \mathbb{F}_p \times \mathbb{F}_p$ such that E_κ contains a point of order p over $\mathbb{F}_p$. Recall that $d(p) := \#\mathfrak{S}$. Let $\mathcal{W}'(X) \subset \mathcal{W}(X)$ be the set of Weierstrass equations $y^2 = x^3 + Ax + B$ which reduce to E_κ for some $\kappa \in \mathfrak{S}$.

Theorem 4.14. We have that $\mathfrak{d}_p^{(3)} \leq \zeta(10) \cdot \frac{d(p)}{p^2}$.

Proof. It follows from Lemma 4.13 that

$$\limsup_{X \to \infty} \frac{\#\mathcal{W}'(X)}{\#\mathcal{E}(X)} \leq \zeta(10) \cdot \frac{d(p)}{p^2}.$$

Recall that $\mathcal{E}_3(X) \subseteq \mathcal{W}'(X)$. The result follows. $\qquad\square$

Acknowledgments

References

[1] L. Babinkostova, J. C. Bahr, Y. H. Kim, E. Neyman, and G. K. Taylor. Anomalous primes and the elliptic Korselt criterion. *J. Number Theory*, 201:108–123, 2019.

[2] D. Bernardi and B. Perrin-Riou. *p*-adic variant of the Birch and Swinnerton-Dyer conjecture (the supersingular case). *Proceedings of the Académie des sciences. Séry 1, Mathématics*, 317(3):227–232, 1993.

[3] A. Brumer. The average rank of elliptic curves I. *Invent. Math.*, 109(1):445–472, 1992.

[4] J. Coates and G. McConnell. Iwasawa theory of modular elliptic curves of analytic rank at most 1. *J. London Math. Soc.*, 50(2):243–264, 1994.

[5] J. Coates and R. Sujatha. *Galois cohomology of elliptic curves*. Narosa, 2000.

[6] J. Coates and R. Sujatha. Fine Selmer groups of elliptic curves over *p*-adic Lie extensions. *Math. Annalen*, 331(4):809–839, 2005.

[7] J. Cremona and M. Sadek. Local and global densities for Weierstrass models of elliptic curves. *arXiv preprint arXiv:2003.08454*, 2020.

[8] C. Delaunay. Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. *Experimental Mathematics*, 10(2):191–196, 2001.

[9] B. Du Kim. The plus/minus Selmer groups for supersingular primes. *J. Australian Math. Soc.*, 95(2):189–200, 2013.

[10] D. Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number Theory Carbondale 1979*, pages 108–118. Springer, 1979.

[11] R. Greenberg. *Arithmetic Theory of Elliptic Curves: Lectures given at the 3rd Session of the Centro Internazionale Matematico Estivo (CIME) held in Cetaro, Italy, July 12-19, 1997*. Springer, 1999.

[12] S. Howson. Euler characteristics as invariants of Iwasawa modules. *Proc. London Math. Soc.*, 85(3):634–658, 2002.

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

[14] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45. American Mathematical Soc., 1999.

[15] S. Kobayashi. Iwasawa theory for elliptic curves at supersingular primes. *Invent. Math.*, 152(1):1–36, 2003.

[16] A. Lei and R. Sujatha. On Selmer groups in the supersingular reduction case. *Tokyo Journal of Mathematics*, 43(2):455–479, 2020.

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

[18] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*, volume 323. Springer, 2013.

[19] L. D. Olson. Hasse invariants and anomalous primes for elliptic curves with complex multiplication. *J. Number Theory*, 8(4):397–414, 1976.

[20] B. Perrin-Riou. Fonctions *L*, *p*-adiques d'une courbe elliptique et points rationnels. In *Annales de l'institut Fourier*, volume 43, pages 945–995, 1993.

[21] B. Perrin-Riou. Théorie d'Iwasawa des représentations *p*-adiques sur un corps local. *Invent. Math.*, 115(1):81–149, 1994.

[22] H. Qin. Anomalous primes of the elliptic curve $E_D : y^2 = x^3 + D$. *Proc. London Math. Soc.*, 112(2):415–453, 03 2016.

[23] A. Ray and R. Sujatha. Euler characteristics and their congruences for multi-signed Selmer groups. *arXiv preprint arXiv:2011.05387*, 2020.

[24] P. C. Ridgdill. *On the frequency of finitely anomalous elliptic curves*. PhD thesis, University of Massachusetts Amherst, 2010.

[25] M. Sadek. Counting elliptic curves with bad reduction over a prescribed set of primes. *arXiv preprint arXiv:1704.02056*, 2017.

[26] P. Schneider. p-adic height pairings I. *Invent. Math.*, 69(3):401–409, 1982.

[27] P. Schneider. p-adic height pairings II. *Invent. Math.*, 79(2):329–374, 1985.

[28] R. Schoof. Nonsingular plane cubic curves over finite fields. *Journal of combinatorial theory, Series A*, 46(2):183–211, 1987.

[29] A. N. Shankar, A. Shankar, and X. Wang. Families of elliptic curves ordered by conductor. *Compos. Math.*, to appear.

[30] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[31] F. Sprung. A formulation of *p*-adic versions of the Birch and Swinnerton-Dyer conjectures in the supersingular case. *Research in Number Theory*, 1(1):1–13, 2015.

[32] X. Wan. Iwasawa main conjecture for supersingular elliptic curves and BSD conjecture. *arXiv preprint arXiv:1411.6352*, 2014.

[33] M. Watkins. Some heuristics about elliptic curves. *Experimental Mathematics*, 17(1):105–125, 2008.

[34] C. Wuthrich. *The fine Selmer group and height pairings*. PhD thesis, University of Cambridge, 2004.

[35] C. Wuthrich. On *p*-adic heights in families of elliptic curves. *J. London Math. Soc.*, 70(1):23–40, 2004.

[36] S. L. Zerbes. Generalised Euler characteristics of Selmer groups. *Proc. London Math. Soc.*, 98(3):775–796, 2009.

Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada.
Email address: dkundu@math.ubc.ca

Department of Mathematics, University of British Columbia, Vancouver BC, V6T 1Z2, Canada.
Email address: anweshray@math.ubc.ca