# COTORSION OF ANTI-CYCLOTOMIC SELMER GROUPS ON AVERAGE

Abstract. For an elliptic curve, we study how many Selmer groups are cotorsion over the anti-cyclotomic $\mathbb{Z}_p$-extension as one varies the prime $p$ or the quadratic imaginary field in question.

## 1. Introduction

Let $\mathsf{E}$ be an elliptic curve define over $\mathbb{Q}$ and let $\mathbb{Q}(\sqrt{d})$ be an imaginary quadratic field. Much of the arithmetic of $\mathbb{Q}(\sqrt{d})$-rational points of $\mathsf{E}$ is contained in the behaviour of points of $\mathsf{E}$ up the anti-cyclotomic $\mathbb{Z}_p$-tower $\mathbb{Q}(\sqrt{d})_{\mathrm{ac}}$ of $\mathbb{Q}(\sqrt{d})$ for a prime $p$ of good reduction.

The goal of this paper is to count the proportion of anti-cyclotomic Selmer groups whose behaviour we understand. There are two different cases to be considered. The first is the *indefinite case*, in which the number of bad primes of $\mathsf{E}$ that are inert in $\mathbb{Q}(\sqrt{d})$ is even. This condition is also known as the (generalized) Heegner hypothesis, and should allow for many rational points on the elliptic curve. Indeed, M. Bertolini [Ber95] and M. Longo–S. Vigni [LV19] show in various scenarios that the appropriate anti-cyclotomic Selmer groups have corank 1 over the anti-cyclotomic Iwasawa algebra.

The second one is the *definite case* and was studied by R. Pollack and T. Weston in [PW11], and in their joint work with C. Kim [KPW17]. Here, the number of bad inert primes is odd, preventing the existence of Heegner points. Consequently, there should be few rational points. Their work confirms this and shows that under various hypotheses, the anti-cyclotomic Selmer group is cotorsion.

While the hypotheses employed in works concerning the first (indefinite) case are mild from a statistical point of view, the ones employed in the second (definite) case (i.e. [BD05, KPW17, PW11]) cut down the proportion of provably corank 0 Selmer groups, and we are interested in counting what this proportion is. To this end, there are known results in some cases: For a fixed pair $(\mathsf{E}_{/\mathbb{Q}}, p)$ where $p$ is ordinary, [HKR21] gave a lower bound in this definite case for the proportion of imaginary quadratic fields of the form $\mathbb{Q}(\sqrt{-\ell})$ with $\ell$ a prime for which the Selmer groups are known to be cotorsion. Our paper generalizes [HKR21] in two ways:

(1) We include all imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ in the count.
(2) We remove the ordinarity hypothesis by including supersingular primes for which $a_p = 0$.

The main result of our paper measures from a statistical point of view how mild the assumptions in [KPW17] and [PW11] are. A bit more precisely, it asserts that the proportion of such imaginary quadratic fields is halved (i.e. multiplied by $\frac{1}{2}$) for each prime of bad reduction that is *split* that would violate the key hypothesis of [KPW17] *were it inert*. Instead of overwhelming the reader with precise statements, we give a flavor via an example. (For the technically savvy reader: they are Theorems 4.5 and 4.13, addressing the supersingular and the ordinary cases separately.)

The elliptic curve 497a1 with Weierstrass equation $y^2+xy = x^3+x^2+25x-14$ has bad reduction at 7 and 71. At the prime 5, this elliptic curve attains good supersingular reduction. Our theorem then says that the proportion of cotorsion anti-cyclotomic Selmer groups as one varies the quadratic imaginary field is at least

$$\frac{1}{4} \times \frac{5 \times 7 \times 71}{6 \times 8 \times 72} = 0.1797598\cdots .$$

When randomly choosing imaginary quadratic fields, $p$ should split half of the time and we should land in the definite case half of the time. This accounts for the factor of $\frac{1}{4} = \frac{1}{2} \times \frac{1}{2}$. The other factor occurs because we count fields with discriminant coprime to $p$ and conductor of the elliptic curve.

---

2010 *Mathematics Subject Classification.* 11G05, 11R23 (primary); 11R45 (secondary).

*Key words and phrases.* Iwasawa theory, Selmer groups, elliptic curves, anti-cyclotomic, supersingular primes.

If instead of the assumptions in [PW11], we relied on [BD05][1], the lower bound would be

$$\frac{1}{8} \times \frac{5 \times 7 \times 71}{6 \times 8 \times 72} = 0.0898799 \cdots ,$$

i.e. our theorem shows that the work of [PW11] doubled the desired proportion!

We achieve the lower bound by counting the proportion of such imaginary quadratic fields that satisfy several hypotheses imposed in [KPW17], which we call *choired*. *'Cho'* indicates we are in the definite case, while *'ired'* indicates a ramification hypothesis. More precisely, *'Choired'* stands for: **C**onductor shouldn't satisfy **H**eegner hypothesis, so has an **O**dd number of factors. Furthermore, **I**nert primes **R**amify only under **E**xtra **D**ifficulty imposed by (Kim–)Pollack–Weston.

Three steps are needed to perform the count.

First, in Lemma 4.8 we encode imaginary quadratic fields with the same splitting type at the bad primes of $\mathsf{E}$ into something that is easier to count. We achieve this by working with the discriminants of the fields modulo the conductor of $\mathsf{E}$ (denoted by $N_{\mathsf{E}}$) and modulo the prime $p$, showing that each family of such fields corresponds to a proportion of $\frac{1}{2^{r+1}}$ of the possible residue classes, where $r$ is the number of bad primes.

The second step is to estimate the proportion of imaginary quadratic fields with discriminant coprime to $pN_{\mathsf{E}}$ (Proposition 4.9). To do this, we sum appropriate estimates due to K. Prachar and P. Humphries over the residue classes in question from the first step.

In the final step, we break up the choired fields into a disjoint union of families of imaginary quadratic fields with prescribed splitting type as in step 1. Then using the counting estimates in the previous two steps and a combinatorial count for this disjoint union, we arrive at our estimate.

*Organization*: Including this introduction, the article has four sections. Section 2 is preliminary in nature. We introduce the definition of the key objects and also introduce the criterion of Pollack–Weston in this section. Sections 3 and 4 are devoted to studying this criterion on average. Section 3 is a warm-up to the main result: we show that for a fixed a pair $(\mathsf{E}_{/\mathbb{Q}}, \mathbb{Q}(\sqrt{d}))$, the Selmer groups are cotorsion for all $p$ of good reduction larger than an explicit constant. See Theorem 3.2 for the precise statement. We then develop the methods to prove our main result in Section 4, following the three steps described above.

*Outlook*: If we fix the pair $\left(p, \mathbb{Q}(\sqrt{d})\right)$ and vary the elliptic curve (ordered by height or conductor) with good reduction at $p$, it seems to be significantly more difficult to estimate for what proportion of elliptic curves the appropriate Selmer groups are $\Lambda$-cotorsion. We will investigate aspects of this question in future projects.

## Acknowledgements

We thank Manjul Bhargava, Allysa Lumley, V. Kumar Murty, Artane Siad, Joseph Silverman, and Andrew Sutherland for stimulating and helpful discussions, and Ming-Lun Hsieh, Chan-Ho Kim, Robert Pollack, and Tom Weston for answering our questions related to [KPW17, PW11], and Noam Elkies for answering a question related to [Elk87]. We also thank Stefano Vigni for clarifying the papers [Ber95, LV19] and Melanie Matchett Wood for answering a question related to counting imaginary quadratic fields.

## 2. Preliminaries

Let $p > 3$ be a prime and $K = \mathbb{Q}(\sqrt{d})$ an imaginary quadratic field. Denote by $K_{\mathrm{ac}}$ the anti-cyclotomic $\mathbb{Z}_p$-extension of $K$. For $n \geq 0$, the *$n$-th layer* is the unique number field $K_n$ such that $K \subseteq K_n \subset K_{\mathrm{ac}}$ and $[K_n : K] = p^n$. Note that $K_n$ is Galois over $\mathbb{Q}$ and its Galois group $\mathrm{Gal}(K_n/\mathbb{Q})$ is (isomorphic to) the dihedral group of order $2p^n$.

[1] [PW11, Remark 4.2] compares the different assumptions in more detail.

Denote by $\Gamma$ the Galois group $\mathrm{Gal}(K_{\mathrm{ac}}/K)$ and pick a topological generator $\gamma \in \Gamma$. The *Iwasawa algebra* $\Lambda$ is the completed group algebra $\mathbb{Z}_p[\![\Gamma]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma/\Gamma^{p^n}]$. Fix an isomorphism of rings $\Lambda \simeq \mathbb{Z}_p[\![T]\!]$ by sending $\gamma - 1$ to the formal variable $T$.

2.1. Let $\mathsf{E}_{/\mathbb{Q}}$ be an elliptic curve with good reduction at $p$ and of conductor $N_{\mathsf{E}}$ so that the discriminant of $K = \mathbb{Q}(\sqrt{d})$ is coprime to $pN_{\mathsf{E}}$. The main objects of study in this paper are the *minimal Selmer groups* defined in [PW11, Section 3.1]. For the convenience of the reader, we work with a less technical but equivalent definition of these $p$-primary Selmer groups than that of [PW11][2].

Choose a finite set of primes $S$ containing the primes $v|p$ in $K$, the archimedean primes, and the primes at which $\mathsf{E}$ has bad reduction. For any finite extension $L/K$, write $S(L)$ to denote the set of primes $w$ of $L$ such that $w$ lies above a prime $v \in S$.

For ease of notation, define

$$J_v(\mathsf{E}/L) = \prod_{w|v} H^1\left(L_w, \mathsf{E}[p^\infty]\right) / \left(\mathsf{E}(L_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right),$$

where the product is over all primes $w$ of $L$ lying above $v$. Following R. Greenberg [Gre89, p. 107] (see also [Gre99, p. 20]), the *$p$-primary Selmer group over $L$* is defined as follows

$$\mathrm{Sel}_{p^\infty}(\mathsf{E}/L) := \ker\left\{H^1\left(L, \mathsf{E}[p^\infty]\right) \longrightarrow \bigoplus_v J_v(\mathsf{E}/L)\right\}.$$

It is also possible to define the *$p$-primary Selmer group* by using a smaller Galois group,

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

The fact that these two definitions agree follows from [Mil06, Proposition 6.5 or Corollary 6.6]. For a detailed discussion, we refer the reader to [CS00, Section 1.7 (Cassels-Poitou-Tate sequence)]. Next, set $J_v(\mathsf{E}/K_{\mathrm{ac}})$ to be the direct limit

$$J_v(\mathsf{E}/K_{\mathrm{ac}}) := \varinjlim_L J_v(\mathsf{E}/L),$$

where $L$ ranges over all number fields contained in $K_{\mathrm{ac}}$. Taking direct limits, the *$p$-primary Selmer group over $K_{\mathrm{ac}}$* can be defined as follows

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

As explained earlier, over $K_{\mathrm{ac}}$ as well, we have an equivalent definition of the Selmer group,

$$\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{ac}}) := \ker\left\{H^1\left(K_{\mathrm{ac}}, \mathsf{E}[p^\infty]\right) \longrightarrow \bigoplus_{v} J_v(\mathsf{E}/K_{\mathrm{ac}})\right\}.$$

Note that the map above is a map of $\Lambda$-modules. A $\Lambda$-module $M$ is said to be *cofinitely generated* (resp. *cotorsion*) if its Pontryagin dual $M^\vee := \mathrm{Hom}_{\mathbb{Z}_p}\left(M, \mathbb{Q}_p/\mathbb{Z}_p\right)$ is finitely generated (resp. torsion) as a $\Lambda$-module. A standard application of Nakayama's lemma shows that $\mathrm{Sel}_{p^\infty}(E/K_{\mathrm{ac}})$ is cofinitely generated. However, this Selmer group *need not be* $\Lambda$-cotorsion.

[2]For the equivalence of the definitions in the setting of this paper, we refer the reader to [PW11, Appendix A]. The two sentence summary of their discussion is that Selmer groups are defined via a collection of local conditions, which the authors call *Selmer structures*. While these Selmer structures may be different at $K_n$, they become the same as one takes the limit and works with $K_{ac}$.

2.2. Let $\mathsf{E}_{/\mathbb{Q}}$ be an elliptic curve with supersingular reduction at $p > 3$. Set $\widehat{\mathsf{E}}$ to be the formal group of $\mathsf{E}$ over $\mathbb{Z}_p$. Let $L$ be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_L$ and let $\widehat{\mathsf{E}}(L)$ denote $\widehat{\mathsf{E}}(\mathfrak{m}_L)$, where $\mathfrak{m}_L$ is the maximal ideal in $L$. Let $v$ be a prime above $p$ in $K_n$. Following S. Kobayashi [Kob03], we define the plus (and minus) norm groups as follows

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

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

where $\mathrm{tr}_{n/m+1} : \widehat{\mathsf{E}}(K_{n,v}) \to \widehat{\mathsf{E}}(K_{m+1,v})$ is the trace map with respect to the formal group law on $\widehat{\mathsf{E}}$. Define the *plus (resp. minus) Selmer group* at the $n$-th layer of the $\mathbb{Z}_p$-extension as follows

$$0 \to \mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_n) \to \mathrm{Sel}_{p^\infty}(\mathsf{E}/K_n) \to \prod_{v|p} \frac{H^1\left(K_{n,v}, \mathsf{E}[p^\infty]\right)}{\widehat{\mathsf{E}}^{\pm}(K_{n,v}) \otimes \mathbb{Q}_p/\mathbb{Z}_p}$$

in view of $\left(\widehat{\mathsf{E}}(L_v)^{\pm} \otimes \mathbb{Q}_p/\mathbb{Z}_p\right) \subset \left(\mathsf{E}(L_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p\right)$. The plus (resp. minus) Selmer groups over $K_{\mathrm{ac}}$ are defined by taking direct limits, i.e.,

$$\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}}) := \varinjlim_n \mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_n).$$

2.3. Let $M$ be a finitely generated $\Lambda$-module and $M^\vee$ denote its Pontryagin dual. The *Structure Theorem for* $\Lambda$*-modules* (see [Was97, Theorem 13.12]) asserts that $M$ is pseudo-isomorphic to a finite direct sum of cyclic $\Lambda$-modules, i.e., there is a map of $\Lambda$-modules

$$M \longrightarrow \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{\mu_i})\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T))\right)$$

with finite kernel and cokernel. Here, $\mu_i > 0$, and $f_j(T)$ are distinguished polynomials (monic polynomials with non-leading coefficients divisible by $p$). The $\mu$-invariant of $M$ is defined as the power of $p$ in $f_M(T) := p^{\sum_i \mu_i} \prod_j f_j(T)$. More precisely,

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

*Remark* 2.1. We are interested in the $\Lambda$-modules $\mathrm{Sel}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$ (or $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$) when they are $\Lambda$-cotorsion, see [PW11, Theorem 1.3]. We write $\mu(\mathsf{E}/K_{\mathrm{ac}})$ (or $\mu^{\pm}(\mathsf{E}/K_{\mathrm{ac}})$) for the $\mu$-invariant of the appropriate Selmer group.

2.4. Keeping the notation introduced earlier, write $N_{\mathsf{E}} = N^+_{\mathsf{E}} N^-_{\mathsf{E}}$ where $N^+_{\mathsf{E}}$ is the product of the bad reduction primes that are split in $K$ and $N^-_{\mathsf{E}}$ is the product of the bad reduction inert primes. The following hypothesis guarantees the cotorsionness of the above remark in a large number of cases. It was introduced in [PW11] (see [KPW17, Assumption 1.1 and Remark 1.4] for correction).

**Hypothesis choired.** *For a prime $p > 3$, this hypothesis is the following list of conditions:*
(*1*) $\overline{\rho}_{\mathsf{E},p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ *is surjective.*
(*2*) *If $q$ is a prime with $q|N^-_{\mathsf{E}}$ and $q \equiv \pm 1 \pmod p$, then $\overline{\rho}_{\mathsf{E},p}$ is ramified at $q$.*
(*3*) *$N^-_{\mathsf{E}}$ is square-free and the number of primes dividing $N^-_{\mathsf{E}}$ is odd.*
(*4*) $a_p \not\equiv \pm 1 \pmod p$.

*Remark* 2.2. In [KPW17] and [PW11], various subsets of the above hypotheses are named 'CR' – CR stands for 'controlled ramification' [Kim22]. We make a few clarifying remarks. In [PW11], Condition (4) had been omitted. Also, the results in *loc. cit.* implicitly assumed that $\overline{\rho}_{\mathsf{E},p}$ is ramified at all primes dividing $N^+_{\mathsf{E}}$. This latter assumption of $N^+$-minimality can now be removed by a level-lowering trick introduced in [KPW17], see Section 1.2 in *loc. cit.* for details.

Finally, we recall the main theorems of interest in [PW11, KPW17].

**Theorem 2.3** ([PW11, Theorem 1.3] and [KPW17, Theorem 2.2])**.** *Let $\mathsf{E}$ be an elliptic curve with good reduction at a prime $p > 3$ and conductor $N_{\mathsf{E}}$ so that Hypothesis choired holds.*

*(1) When $a_p = 0$, let $K$ be an imaginary quadratic field so that the discriminant of $K$ is coprime to $pN_{\mathsf{E}}$ and $p$ splits in $K$ into two primes that are totally ramified in $K_{\mathrm{ac}}/K$. Then $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})^\vee$ is $\Lambda$-torsion with $\mu^{\pm}(\mathsf{E}/K_{ac}) = 0$.*

*(2) When $a_p \notin \{\pm 1, 0\}$, let $K$ be an imaginary quadratic field so that the discriminant of $K$ is coprime to $pN_{\mathsf{E}}$. Then $\mathrm{Sel}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})^\vee$ is $\Lambda$-torsion with $\mu(\mathsf{E}/K_{ac}) = 0$.*

## 3. Average results: Varying over supersingular primes

In this short warm-up section, we study what happens when one fixes a pair $(\mathsf{E}_{/\mathbb{Q}}, K)$ and varies $p$. The main theorem shows that the Selmer groups $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$ or $\mathrm{Sel}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$ are $\Lambda$-cotorsion 100% of the time, and in fact as soon as $p$ is sufficiently large. We do this by proving that Hypothesis choired holds for appropriately large primes, so that the aforementioned work of Pollack–Weston guarantees the desired $\Lambda$-torsionness and also guarantees the vanishing of the $\mu$-invariant(s). Note that we require *no* hypothesis on the Mordell–Weil rank of the elliptic curve over $\mathbb{Q}$ (or $K$).

The results of Pollack–Weston require that $K$ is an imaginary quadratic field of discriminant coprime to $pN_{\mathsf{E}}$. In the supersingular reduction case, it is also required that $p$ splits in $K$ and that the primes above $p$ are totally ramified in $K_{\mathrm{ac}}/K$.

*Remark* 3.1. If $p$ does not divide the class number of $K$, denoted by $h_K$, then the primes above $p$ in $K$ are totally ramified in the anti-cyclotomic $\mathbb{Z}_p$-extension, see [Bri07, p. 2131 last paragraph].

**Theorem 3.2.** *Fix a pair $(\mathsf{E}_{/\mathbb{Q}}, K)$, where $K$ is an imaginary quadratic field as above and $\mathsf{E}_{/\mathbb{Q}}$ is an elliptic curve without complex multiplication so that $N^-_{\mathsf{E}}$ is a product of an odd number of distinct primes. Let $p > 68N_{\mathsf{E}}(1 + \log\log N_{\mathsf{E}})^{1/2}$ be a prime of good reduction.*

*(1) If $a_p = 0$, $p$ splits in $K$ and $p \nmid h_K$, then the $p$-primary signed Selmer groups $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$ are $\Lambda$-cotorsion with $\mu^{\pm}(\mathsf{E}/K_{\mathrm{ac}}) = 0$.*

*(2) If $a_p \not\equiv 0, \pm 1 \pmod{p}$ and $p$ is unramified in $K$, then the $p$-primary Selmer group $\mathrm{Sel}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$ is $\Lambda$-cotorsion with $\mu(\mathsf{E}/K_{\mathrm{ac}}) = 0$.*

*Proof.* We check for which primes the four criteria appearing in Hypothesis choired hold. The last two always hold by assumption. The first two are satisfied for $p > 68N_{\mathsf{E}}(1 + \log\log N_{\mathsf{E}})^{1/2}$:

(i) $\overline{\rho}_{\mathsf{E},p}$ is surjective:
Serre's Open Image Theorem (see for example [Ser71]) asserts that for a fixed elliptic curve $\mathsf{E}$ without complex multiplication there exists a positive constant $C_{\mathsf{E}}$ such that for $p > C_{\mathsf{E}}$ the mod-$p$ representation is surjective. The bound $C_{\mathsf{E}} \leq 68N_{\mathsf{E}}(1+\log\log N_{\mathsf{E}})^{1/2}$ is due to A. Kraus [Kra95]. Hence, this condition is satisfied as soon as $p > 68N_{\mathsf{E}}(1 + \log\log N_{\mathsf{E}})^{1/2}$.

(ii) If $q|N^-_{\mathsf{E}}$ and $q \equiv \pm 1 \pmod{p}$, then $\overline{\rho}_{\mathsf{E},p}$ is ramified at $q$:
For any of the finitely many primes $q$ dividing $N^-_{\mathsf{E}}$, the condition $q \equiv \pm 1 \pmod{p}$ is never satisfied for $p \gg 0$, e.g. $p > 68N^-_{\mathsf{E}}$. In particular, this condition is vacuous for all good reduction primes $p > 68N(1 + \log\log N)^{1/2}$.

We thus conclude that Hypothesis choired is satisfied for all sufficiently large $p$ in either case.

To complete the proof we apply [PW11, Theorems 1.1 and 1.3]. Note that in (1), Remark 3.1 ensures that $p$ is totally ramified in $K_{\mathrm{ac}}/K$. This allows using the said results from *loc. cit.* □

*Remark* 3.3. (1) A. Cojocaru has obtained bounds similar to that of Kraus in [Coj05, Theorem 2]. Thus, our theorem may be improved by replacing Kraus's bound $68N_{\mathsf{E}}(1 + \log\log N_{\mathsf{E}})^{1/2}$ by Cojocaru's $\frac{4\sqrt{6}}{3}N_{\mathsf{E}}\prod_{p|N_{\mathsf{E}}}\left(1 + \frac{1}{p}\right)^{\frac{1}{2}}$ whenever it is smaller.

(2) It is conjectured that $C_{\mathsf{E}} = 37$, see [Ser81, p. 399]. Consequently, the Selmer group $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$ (resp. $\mathrm{Sel}_{p^\infty}(\mathsf{E}/K_{\mathrm{ac}})$) would be $\Lambda$-cotorsion as soon as $p > \max\{N_{\mathsf{E}}^- + 1, 37, h_K\}$ (resp. $p > \max\{N_{\mathsf{E}}^- + 1, 37\}$) and $p$ splits (resp. is unramified) in $K$.

(3) Elkies proved that given $\mathsf{E}_{/\mathbb{Q}}$, there are infinitely many primes at which it has supersingular reduction [Elk87, Theorem 1]. By the Chebotarev density theorem, half of the primes split in $K$. A priori it is not obvious that given a pair $(\mathsf{E}_{/\mathbb{Q}}, K)$ there are infinitely many primes of supersingular reduction of $\mathsf{E}$ which split in $K$. It is possible to find non-CM elliptic curves over $\mathbb{Q}$ for which only finitely many supersingular primes split in a given *imaginary quadratic* field. For example (see [Wal10, p. 1]) the supersingular primes of $X_1(15)$, given by the equation
$$Y^2 + XY + Y = X^3 + X^2,$$
satisfy the property that $p \equiv 3 \pmod 4$[3]. However, such primes do not split in $K = \mathbb{Q}(i)$. In [Wal10, Section 4.1], it is explained that in any real (resp. imaginary) quadratic field $K$, there is a bias *in favour of* (resp. *against*) the occurrence of supersingular primes that split in the field. However, the averaging results in *loc. cit.* suggest that if $\mathsf{E}$ is a non-CM elliptic curve picked *at random* then there is a positive proportion of supersingular primes which split in $K$.

## 4. Average results: Varying the imaginary quadratic field

Fix an elliptic curve $\mathsf{E}_{/\mathbb{Q}}$ without complex multiplication of square-free conductor $N_{\mathsf{E}}$ and a prime $p > 3$ of good reduction with $a_p \not\equiv \pm 1 \pmod p$. In this section, we count for what proportion of imaginary quadratic fields the associated Selmer groups are $\Lambda$-cotorsion with $\mu$-invariant equal to 0. We prove the theorem separately when $p$ is a prime of supersingular or ordinary reduction.

4.1. **The supersingular case.** In this section, we assume $a_p = 0$. Varying over *imaginary quadratic* fields $\mathbb{Q}(\sqrt{d})$ we estimate how often $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/\mathbb{Q}(\sqrt{d})_{\mathrm{ac}})$ is $\Lambda$-cotorsion with $\mu^{\pm}(\mathsf{E}/\mathbb{Q}(\sqrt{d})_{\mathrm{ac}}) = 0$. To this end, we estimate for what proportion of *imaginary quadratic* fields the following properties hold:

(1) $\gcd\left(pN_{\mathsf{E}}, \left|D_{\mathbb{Q}(\sqrt{d})}\right|\right) = 1$,
(2) Hypothesis choired is satisfied by the triple $(\mathsf{E}_{/\mathbb{Q}}, \mathbb{Q}(\sqrt{d})_{\mathrm{ac}}, p)$, *and*
(3) $p$ splits in $\mathbb{Q}(\sqrt{d})$.
(4) $p$ does not divide the class number of $\mathbb{Q}(\sqrt{d})$.

As for the last property, the *Cohen–Lenstra heuristics* predict that among all imaginary quadratic fields, the proportion for which $p$ *divides* the class number is [BM19], [CL84, Section 9.I]
$$c_p = \frac{6}{\pi^2}\left(1 - \prod_{j=1}^{\infty}\left(1 - \frac{1}{p^j}\right)\right). \tag{4.1}$$
We remind the readers that this constant is expected to be *positive*. A result of K. Horie and Y. Onishi (see [HO88]) establishes that there are infinitely many imaginary quadratic number fields such that $p$ *does not* divide the class number. In [KO99], W. Kohnen and K. Ono have obtained lower bound asymptotics but we are still quite far from establishing the Cohen–Lenstra heuristics.

**Definition 4.1.** *Let $\mathcal{S}$ be a subset of imaginary quadratic fields. Define the* density of $\mathcal{S}$ *as*
$$\delta(\mathcal{S}) := \lim_{x\to\infty} \frac{\#\left\{\mathbb{Q}(\sqrt{d}) : \left|D_{\mathbb{Q}(\sqrt{d})}\right| < x \text{ and } \mathbb{Q}(\sqrt{d}) \in \mathcal{S}\right\}}{\#\left\{\mathbb{Q}(\sqrt{d}) : d < 0, \left|D_{\mathbb{Q}(\sqrt{d})}\right| < x\right\}}.$$

[3]Note that not all primes of the form $p \equiv 3 \pmod 4$ are supersingular.

**Definition 4.2.** *Given a pair $(\mathsf{E}_{/\mathbb{Q}}, p)$ of an elliptic curve $\mathsf{E}$ of conductor $N_{\mathsf{E}}$ and a prime $p$ of good reduction, define $Q^{-}(choired, p+)$ as the following set*

$$\left\{\mathbb{Q}(\sqrt{d}) : d<0,\ \gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, pN_{\mathsf{E}}\right)=1,\ p \text{ splits in } \mathbb{Q}(\sqrt{d}),\ \text{Hypothesis choired holds for } (\mathsf{E}_{/\mathbb{Q}}, \mathbb{Q}(\sqrt{d}), p)\right\}.$$

**Definition 4.3.** *Given an elliptic curve $\mathsf{E}_{/\mathbb{Q}}$ of conductor $N_{\mathsf{E}}$ and a prime $p$, define $k$ to be the number of bad primes $q|N_{\mathsf{E}}$ that satisfy both of the following:*
*(1)* $q \equiv \pm 1 \pmod{p}$,
*(2)* $\bar{\rho}_{\mathsf{E},p}$ *is unramified at* $q$.

*Remark* 4.4. In words, $k$ counts the number of bad primes $q$ that would defy the key assumption of [KPW17] if $q$ were inert in the quadratic imaginary field to be chosen. Of course, since we are working under their assumption, the primes in Definition 4.3 must split – they are 'kounterexamples,' i.e. fake counterexamples to the key assumption of [KPW17], hence the choice of the letter $k$.

**Theorem 4.5.** *Fix a pair $(\mathsf{E}_{/\mathbb{Q}}, p)$ so that*
*(1) $\mathsf{E}_{/\mathbb{Q}}$ is an elliptic curve with square-free conductor $N_{\mathsf{E}} = \prod_{i=1}^{r} q_i$, and*
*(2) $p>3$ is a prime at which $\mathsf{E}$ has good supersingular reduction, $\bar{\rho}_{\mathsf{E},p}$ is surjective, and $k<r$.*
*Then*

$$\delta\left(Q^{-}(\text{choired}, p+)\right) = \frac{pN_{\mathsf{E}}}{2^{k+2}(p+1)\prod_{q_i|N_{\mathsf{E}}}(q_i+1)}.$$

*Let $c_p^*$ denote the proportion of imaginary quadratic fields in $Q^{-}(\text{choired}, p+)$ with $p$ dividing the class number. The proportion of imaginary quadratic fields with $\gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, pN_{\mathsf{E}}\right)=1$, the prime $p$ splits in $\mathbb{Q}(\sqrt{d})$, and $\mathrm{Sel}^{\pm}_{p^\infty}(\mathsf{E}/\mathbb{Q}(\sqrt{d})_{\mathrm{ac}})$ is $\Lambda$-cotorsion with $\mu^{\pm}$-invariant equal to zero is* at least

$$\frac{pN_{\mathsf{E}}}{2^{k+2}(p+1)\prod_{q_i|N_{\mathsf{E}}}(q_i+1)} \cdot (1-c_p^*).$$

First, we introduce some notation.

**Definition 4.6.** *Define $\Pi_p(N_{\mathsf{E}})$ to be the set of prime divisors of $N_{\mathsf{E}}$ together with $p$, i.e.,*

$$\Pi_p(N_{\mathsf{E}}) = \{p, q_1, \dots, q_r\}.$$

*Choose the indices so that $q_i$ with $i \leq k$ are the primes that satisfy the conditions of Definition 4.3. This choice allows keeping track of primes that potentially violate condition (2) in Hypothesis choired.*

**Definition 4.7.** *For any partition $\Pi = \Pi^{-} \sqcup \Pi^{+}$ of $\Pi_p(N_{\mathsf{E}})$ into two disjoint parts, define*

$$Q^{-}(\Pi) := \left\{\mathbb{Q}(\sqrt{d}) : d<0,\ \gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, pN_{\mathsf{E}}\right)=1,\ \text{primes in } \Pi^{-} \text{ are inert in } \mathbb{Q}(\sqrt{d}),\right.$$
$$\left.\text{and primes in } \Pi^{+} \text{ split in } \mathbb{Q}(\sqrt{d})\right\}.$$

*Denote by $\delta_{\Pi}$ the density of $Q^{-}(\Pi)$, i.e. $\delta_{\Pi} := \delta\left(Q^{-}(\Pi)\right)$.*

**Lemma 4.8.** *Pick a partition $\Pi = \Pi^{-} \sqcup \Pi^{+}$ of $\Pi_p(N_{\mathsf{E}})$ into two disjoint parts.*
*(1) When $2 \nmid N_{\mathsf{E}}$, there exists a subset $\mathfrak{r}_{\Pi}$ of $(\mathbb{Z}/pN_{\mathsf{E}}\mathbb{Z})^*$ of size $\frac{\varphi(pN_{\mathsf{E}})}{2^{r+1}}$ so that*

$$\mathbb{Q}(\sqrt{d}) \in Q^{-}(\Pi) \iff D_{\mathbb{Q}(\sqrt{d})} \mod pN_{\mathsf{E}} \in \mathfrak{r}_{\Pi}.$$

*(2) When $2 \mid N_{\mathsf{E}}$, there exists a subset $\mathfrak{r}_{\Pi}$ of $(\mathbb{Z}/4pN_{\mathsf{E}}\mathbb{Z})^*$ of size $\frac{\varphi(pN_{\mathsf{E}})}{2^{r}}$ so that*

$$\mathbb{Q}(\sqrt{d}) \in Q^{-}(\Pi) \iff D_{\mathbb{Q}(\sqrt{d})} \mod 4pN_{\mathsf{E}} \in \mathfrak{r}_{\Pi}.$$

*In either case, $Q^-(\Pi)$ corresponds to $\frac{1}{2^{r+1}}$ of the possible residue classes for discriminants of quadratic imaginary fields coprime to $pN_{\mathsf{E}}$.*

*Proof.* From [Cox13, Proposition 5.16], we have that $\mathbb{Q}(\sqrt{d}) \in Q^-(\Pi)$ if and only if for all $q \in \Pi^-$, the Kronecker symbol $\left(\frac{D_{\mathbb{Q}(\sqrt{d})}}{q}\right) = -1$ and for all $q \in \Pi^+$, the Kronecker symbol $\left(\frac{D_{\mathbb{Q}(\sqrt{d})}}{q}\right) = +1$.

We first handle the case $2 \nmid N_{\mathsf{E}}$. For $q \in \Pi_p(N_{\mathsf{E}})$, denote by $\mathfrak{r}_\Pi^q \subset (\mathbb{Z}/q\mathbb{Z})^*$ the set of quadratic non-residues. Note that for an odd prime $q$ we have that $\#\mathfrak{r}_\Pi^q = \frac{q-1}{2}$, since half the elements of $(\mathbb{Z}/q\mathbb{Z})^*$ are squares. Define

$$\mathfrak{r}_\Pi := \prod_{q \in \Pi_p(N_{\mathsf{E}})} \mathfrak{r}_\Pi^q \subset \prod_{q \in \Pi_p(N_{\mathsf{E}})} (\mathbb{Z}/q\mathbb{Z})^* \cong (\mathbb{Z}/pN_{\mathsf{E}}\mathbb{Z})^*.$$

Thus, $\mathbb{Q}(\sqrt{d}) \in Q^-(\Pi)$ if and only if $D_{\mathbb{Q}(\sqrt{d})} \mod pN_{\mathsf{E}} \in \mathfrak{r}_\Pi$, as claimed. It also follows that

$$\#\mathfrak{r}_\Pi = \frac{(p-1)}{2} \prod_{i=1}^{r} \frac{q_i - 1}{2} = \frac{\varphi(pN_{\mathsf{E}})}{2^{r+1}}.$$

To handle the case $2 \mid N_{\mathsf{E}}$, set

$$\mathfrak{r}_\Pi^2 := \{1\} \in \left(\mathbb{Z}/8\mathbb{Z}\right)^*$$

Note that by definition of the Kronecker symbol, $D_{\mathbb{Q}(\sqrt{d})} \mod 8 \in \{1\} \subset \left(\mathbb{Z}/8\mathbb{Z}\right)^*$ if and only if $\left(\frac{D_{\mathbb{Q}(\sqrt{d})}}{2}\right) = 1$. We can then proceed analogously to the case when $N_{\mathsf{E}}$ was odd, working with

$$\mathfrak{r}_\Pi = \prod_{q \in \Pi_p(N_{\mathsf{E}})} \mathfrak{r}_\Pi^q \subset \left(\mathbb{Z}/8\mathbb{Z}\right)^* \times \prod_{\text{odd } q \in \Pi_p(N_{\mathsf{E}})} (\mathbb{Z}/q\mathbb{Z})^* \cong (\mathbb{Z}/4pN_{\mathsf{E}}\mathbb{Z})^*.$$

For the last assertion, note that when $N_{\mathsf{E}}$ is odd, $D_{\mathbb{Q}(\sqrt{d})}$ can reduce to any element in $(\mathbb{Z}/pN_{\mathsf{E}}\mathbb{Z})^*$, while for $N_{\mathsf{E}}$ even, the reduction in the $(\mathbb{Z}/8\mathbb{Z})^*$ part lies in $\{1, 5\}$ as 2 does not ramify by assumption. □

**Proposition 4.9.** *Let $M$ be any square-free integer. Define*

$$Q^-(x, D \perp M) := \left\{\mathbb{Q}(\sqrt{d}) \text{ imaginary}: \left|D_{\mathbb{Q}(\sqrt{d})}\right| < x \text{ and } \gcd\left(D_{\mathbb{Q}(\sqrt{d})}, M\right) = 1\right\}.$$

*Then asymptotically,*

$$\lim_{x\to\infty} \#Q^-(x, D \perp M) \sim \frac{1}{2} \frac{x}{\zeta(2)} \frac{M}{\prod_{q|M}(q+1)}$$

*Proof.* A result of Prachar [Pra58, formula 1] (see [Hum17] for two proofs by Humphries) says that

$$\lim_{x\to\infty} \#\left\{n \text{ square-free}: \ 0 < n < x, \ n \equiv a \pmod{b}, \ \gcd(b, a) = 1\right\} \sim \frac{x}{\zeta(2)} \frac{1}{b} \prod_{q|b} \left(1 - \frac{1}{q^2}\right)^{-1},$$

where $a$ and $b$ are integers, and the $q$'s are primes.
We first handle the case $2 \nmid M$.
Put $b = 4M$. Then there are $\prod_{q|M}(q-1)$ congruence classes $a \pmod{b}$ with $\gcd(a, 4M) = 1$ and

$a \equiv 1 \mod 4$, over which we sum the above Prachar–Humphries estimate. Therefore,

$$\begin{aligned}
&\lim_{x\to\infty} \#\left\{n \text{ square-free}: \quad n \equiv 1 \pmod 4,\ 0 < n < x,\ \gcd(n, M) = 1\right\} \\
(*)\qquad &\sim \prod_{q|M}(q-1) \times \frac{x}{\zeta(2)}\frac{1}{4M}\prod_{q|4M}\left(1-\frac{1}{q^2}\right)^{-1} \\
&= \prod_{q|M}(q-1) \times \frac{x}{\zeta(2)}\frac{1}{4M}\frac{4}{3}\prod_{q|M}\frac{q^2}{q^2-1} \\
&= \frac{x}{\zeta(2)}\frac{1}{3}\frac{M}{\prod_{q|M}(q+1)}.
\end{aligned}$$

The same estimate works for the congruence class $n \equiv 3 \pmod 4$. To handle the congruence class $n \equiv 2 \pmod 4$, note that $n \equiv 2 \pmod 4$ with $(n, M) = 1$ is square-free if and only if $\frac{n}{2}$ is. But $\frac{n}{2}$ can be $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$, so by using the above argument,

$$\begin{aligned}
&\lim_{x\to\infty} \#\left\{n \text{ square-free}: \quad n \equiv 2 \pmod 4,\ 0 < n < x,\ \gcd(n, M) = 1\right\} \\
&= \lim_{x\to\infty} \#\left\{n \text{ square-free}: \quad n \equiv 1 \text{ or } 3 \pmod 4,\ 0 < n < \frac{x}{2},\ \gcd(n, M) = 1\right\} \\
&\sim 2 \times \frac{x/2}{\zeta(2)}\frac{1}{3}\frac{M}{\prod_{q|M}(q+1)}.
\end{aligned}$$

Since we are assuming that $2 \nmid M$, note that $\gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, M\right) = 1 \iff \gcd(|d|, M) = 1$. Hence, we are interested in the following estimate:

$$\begin{aligned}
(**)\qquad &\lim_{x\to\infty} \#\left\{d \text{ square-free}:\ d < 0,\ \left|D_{\mathbb{Q}(\sqrt{d})}\right| < x,\ \gcd(|d|, M) = 1\right\} \\
&= \lim_{x\to\infty} \#\left\{d \text{ square-free}:\ d < 0,\ |d| < x,\ \gcd(|d|, M) = 1,\ d \equiv 1 \pmod 4\right\} \cup \\
&\quad \lim_{x\to\infty} \#\left\{d \text{ square-free}:\ d < 0,\ |d| < \frac{x}{4},\ \gcd(|d|, M) = 1,\ d \equiv 2,3 \pmod 4\right\} \\
&\sim \left(\frac{1}{3}\frac{x}{\zeta(2)} + \frac{1}{3}\frac{x/4}{\zeta(2)} + \frac{1}{3}\frac{x/4}{\zeta(2)}\right)\left(\frac{M}{\prod_{q|M}(q+1)}\right) = \frac{1}{2}\frac{x}{\zeta(2)}\frac{M}{\prod_{q|M}(q+1)}.
\end{aligned}$$

The case $2|M$ is a bit easier.
The simplification appears when decomposing (**) into $\pmod 4$ congruence classes. Since $2 \mid M$, note that $\gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, M\right) = 1$ implies $d \equiv 1 \pmod 4$. Thus,

$$\begin{aligned}
&\lim_{x\to\infty} \#\left\{\mathbb{Q}(\sqrt{d}):\ d < 0,\ \left|D_{\mathbb{Q}(\sqrt{d})}\right| < x,\ \gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, M\right) = 1\right\} \\
&= \lim_{x\to\infty} \#\left\{d \text{ square-free}:\ d \equiv 1 \pmod 4,\ -x < d < 0,\ \gcd(|d|, M) = 1\right\} \\
&\sim \frac{1}{2}\frac{x}{\zeta(2)}\left(\frac{M}{\prod_{q|M}(q+1)}\right).
\end{aligned}$$

The reason for the different result in the Prachar–Humphries estimate (a factor of $\frac{1}{2}$ instead of $\frac{1}{3}$) is the following. The integer $b = 2M$ is a multiple of 4, so there are again $\prod_{q|M}(q-1)$ congruence classes $a \pmod b$ with $(a, M) = 1$ and $a \equiv 1 \pmod 4$.

Summing the Prachar–Humphries estimate over these classes,

(1) the term $\frac{1}{4M}$ in the equation (*) is replaced by $\frac{1}{2M}$, and

(2) the term $\frac{4}{3}$ in the line below disappears, since in the product $\prod_{q|M} \frac{q^2}{q^2-1}$, one of the primes $q = 2$ by assumption.

This accounts for a total scaling by a factor of $2 \times \frac{3}{4}$.

The same argument also applies when $a \equiv 1 \pmod 4$ is replaced by $a \equiv 3 \pmod 4$. □

*Remark* 4.10. (1) It is well known that (see for example, [CDO02, Corollary 1.3][4])

$$\lim_{x\to\infty} \# \left\{ \mathbb{Q}(\sqrt{d}) \text{ imaginary quadratic} : \left| D_{\mathbb{Q}(\sqrt{d})} \right| < x \right\} \sim \frac{1}{2} \frac{x}{\zeta(2)}.$$

In *loc. cit.*, one finds an extra factor of $\frac{1}{2^{r_2}}$, but $r_2 = 0$ since $\mathbb{Q}$ has signature (1,0).

(2) Proposition 4.9 says that for each prime $q$ with respect to which the coprimality condition is imposed on the discriminant, the proportion of imaginary quadratic fields reduces by a factor of $\frac{q}{q+1}$.

We are now in a position to prove Theorem 4.5.

*Proof of Theorem 4.5.* For Hypothesis choired to be satisfied, we need

- $N_{\mathsf{E}}^-$ is a product of an odd number of primes *and*
- none of the primes $q_i$ for $i \le k$ divide $N_{\mathsf{E}}^-$.

Let $\mathcal{N}$ be the collection of all candidate subsets of the prime divisors of $N_{\mathsf{E}}^-$. In other words, let $\mathcal{N}$ be the collection of all subsets $\Pi^- \subseteq \{q_{k+1}, \dots, q_r\}$ for which $\#\Pi^-$ is odd. Each such $\Pi^-$ determines a partition $\Pi = \Pi^- \sqcup \Pi^+$ of $\Pi_p(N_{\mathsf{E}})$ so that $p \in \Pi^+$. Then

$$Q^-(\mathit{choired},\, p+) = \bigsqcup_{\Pi \text{ so that } \Pi^- \in \mathcal{N}} Q^-(\Pi).$$

Lemma 4.8 asserts that $Q^-(\Pi)$ corresponds to $\frac{1}{2^{r+1}}$ of the possible residue classes of discriminants coprime to $pN_{\mathsf{E}}$. Setting $M = pN_{\mathsf{E}}$, Proposition 4.9 tells us that the proportion of those imaginary quadratic fields with discriminant coprime to $pN_{\mathsf{E}}$ among all quadratic imaginary fields is given by

$$\mathfrak{d} := \frac{pN_{\mathsf{E}}}{(p+1)\prod_{q_i|N_{\mathsf{E}}}(q_i+1)},$$

so that

$$\delta_\Pi = \frac{1}{2^{r+1}}\mathfrak{d} = \frac{pN_{\mathsf{E}}}{2^{r+1}(p+1)\prod_{q_i|N_{\mathsf{E}}}(q_i+1)},$$

Since $\#\mathcal{N} = 2^{r-k-1}$ [Sob13, Exercise 1.1.13],

$$\delta\left(Q^-(\mathit{choired},\, p+)\right) = \#\mathcal{N} \cdot \delta_\Pi.$$

This proves our first assertion.

For the final assertion regarding the $\Lambda$-cotorsionness and triviality of the $\mu$-invariants, we need the two primes above $p$ to be *totally ramified* in $\mathbb{Q}(\sqrt{d})_{\mathrm{ac}}/\mathbb{Q}(\sqrt{d})$. A sufficient condition for this is the (additional) hypothesis that $p$ does not divide the class number of $\mathbb{Q}(\sqrt{d})$, which gives the factor of $1 - c_p^*$ in the final assertion. □

*Remark* 4.11. The relationship between $c_p$ and $c_p^*$ is not immediate to the authors, e.g. should they be equal? We think it would be worthwhile to investigate this question in greater depth.

[4]This count is slightly different from the one in [Bha07] where all fields are weighted by $1/\#\,\mathrm{Aut}$.

4.2. **The ordinary case.** We now prove an analogue of Theorem 4.5 when $(\mathsf{E}_{/\mathbb{Q}}, p)$ is a fixed pair as before but $p$ is a prime of good *ordinary* reduction of $\mathsf{E}$. We begin with the following definition:

**Definition 4.12.** *Given a pair $(\mathsf{E}_{/\mathbb{Q}}, p)$ of an elliptic curve $\mathsf{E}$ of square-free conductor $N_{\mathsf{E}}$ and a prime $p$ of good ordinary reduction, define $Q^{-}(\text{choired}, p\pm)$ – or less precisely $Q^{-}(\text{choired})$ – as the following set*

$$\left\{\mathbb{Q}(\sqrt{d}) : d<0,\ \gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, pN_{\mathsf{E}}\right)=1,\ \textit{Hypothesis choired holds for } (\mathsf{E}_{/\mathbb{Q}}, \mathbb{Q}(\sqrt{d}), p),\right\}.$$

Unlike in the supersingular case, here we count imaginary quadratic fields where $p$ is either inert or $p$ splits. This is because, as pointed out in Section 2.4, Pollack–Weston have shown that for any triple $(\mathsf{E}_{/\mathbb{Q}}, \mathbb{Q}(\sqrt{d}), p)$ with $\mathbb{Q}(\sqrt{d}) \in Q^{-}(\text{choired}, p\pm)$, the associated Selmer group is $\Lambda$-cotorsion with $\mu(\mathsf{E}/\mathbb{Q}(\sqrt{d})_{\text{ac}})=0$. In particular, there are no restrictions imposed on the splitting of $p$ in the imaginary quadratic field or on the class number of the said field. We write

$$Q^{-}(\text{choired}, p\pm) = Q^{-}(\text{choired}, p+) \sqcup Q^{-}(\text{choired}, p-). \tag{4.2}$$

Here, $p+$ (resp. $p-$) indicates quadratic fields in $Q^{-}(\text{choired}, p\pm)$ with the additional property that $p$ splits (resp. remains inert), cf. Definition 4.2.

**Theorem 4.13.** *Fix a pair $(\mathsf{E}_{/\mathbb{Q}}, p)$ so that*

*(1) $p$ is a prime of good ordinary reduction of $\mathsf{E}$.*
*(2) $\mathsf{E}_{/\mathbb{Q}}$ is an elliptic curve with square-free conductor $N_{\mathsf{E}} = \prod_{i=1}^{r} q_i$, and*
*(3) $p>3$ is a prime at which $\mathsf{E}$ has good reduction, $a_p \not\equiv 1 \pmod{p}$, $\overline{\rho}_{\mathsf{E},p}$ is surjective, and $k<r$.*

*Then the proportion of imaginary quadratic fields with $\gcd\left(\left|D_{\mathbb{Q}(\sqrt{d})}\right|, pN_{\mathsf{E}}\right)=1$ and $\mathrm{Sel}_{p^\infty}(\mathsf{E}/\mathbb{Q}(\sqrt{d})_{\text{ac}})$ $\Lambda$-cotorsion with $\mu$-invariant equal to zero is at least*

$$\delta\left(Q^{-}(\textit{choired}, p\pm)\right) = \frac{pN_{\mathsf{E}}}{2^{k+1}(p+1)\prod_{q_i \mid N_{\mathsf{E}}}(q_i+1)}.$$

*Proof.* For Hypothesis choired to be satisfied, we need

- $N_{\mathsf{E}}^{-}$ is a product of an odd number of primes *and*
- none of the primes $q_i$ for $i \leq k$ divide $N_{\mathsf{E}}^{-}$.
- $a_p \not\equiv \pm 1 \mod p$.

However, the third condition involving the Fourier coefficients does not depend on the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. In other words, this condition does not alter the count of $Q^{-}(\text{choired}, p\pm)$. Hence, for each subset the calculations go through verbatim from the previous section.

Let $\mathcal{N}$ be the collection of all $\Pi^{-} \subseteq \{q_{k+1}, \dots, q_r\}$ for which $\#\Pi^{-}$ is odd. Analogously to the supersingular case, to each such $\Pi^{-}$ we associate a partition of $\Pi$ of $\Pi_p(N_{\mathsf{E}}) = \{p, q_1, \dots, q_r\}$ by

$$\Pi = \begin{cases} \Pi^{-} \sqcup \Pi^{+}, & \text{letting } p \in \Pi^{+} \text{ if } p \text{ splits in } \mathbb{Q}(\sqrt{d}) \\ \left(\Pi^{-} \sqcup \{p\}\right) \sqcup \Pi^{+}, & \text{letting } p \notin \Pi^{+} \text{ if } p \text{ is inert in } \mathbb{Q}(\sqrt{d}). \end{cases}$$

The proof then proceeds analogously to the proof of Theorem 4.5, noting that adding $p$ to the collection of prescribed inert primes doesn't change the argument. Thus,

$$\delta\left(Q^{-}(\text{choired}, p+)\right) = \delta\left(Q^{-}(\text{choired}, p-)\right) = \frac{pN_{\mathsf{E}}}{2^{k+2}(p+1)\prod_{q_i \mid N_{\mathsf{E}}}(q_i+1)}.$$

This completes the proof of the theorem. ∎

## References


[BD05] Massimo Bertolini and Henri Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Ann. Math. (2005), 1–64.

[Ber95] Massimo Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compos. Math. **99** (1995), no. 2, 153–182.

[Bha07] Manjul Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants*, Int. Math. Res. Not. IMRN **2007** (2007), no. 9.

[BM19] Ajit Bhand and M. Ram Murty, *Class numbers of quadratic fields*, Hardy-Ramanujan J. **42** (2019), 17–25. MR 4221215

[Bri07] David Brink, *Prime decomposition in the anti-cyclotomic extension*, Math. Comput. **76** (2007), no. 260, 2127–2138.

[CDO02] Henri Cohen, F Diaz Y Diaz, and Michel Olivier, *On the density of discriminants of cyclic extensions of prime degree*, J. reine angew. Math. **2002** (2002), no. 550, 169–209.

[CL84] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62. MR 756082

[Coj05] Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canadian Math. Bull. **48** (2005), no. 1, 16–31, Appendix by Ernst Kani.

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, second ed., Pure and Applied Mathematics (Hoboken), John Wiley & Sons, Inc., Hoboken, NJ, 2013, Fermat, class field theory, and complex multiplication. MR 3236783

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

[Elk87] Noam D Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$*, Invent. math. **89** (1987), no. 3, 561–567.

[Gre89] Ralph Greenberg, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137.

[Gre99] R Greenberg, *Introduction to Iwasawa theory for elliptic curves. Arithmetic algebraic geometry (Park City, UT, 1999)*, IAS/Park City Math. Ser **9** (1999), 407–464.

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

[HO88] Kuniaki Horie and Yoshihiro Onishi, *The existence of certain infinite families of imaginary quadratic fields*, J. Reine Angew. Math. (1988).

[Hum17] Peter Humphries, *The density of square-free integers satisfying a congruence relation*, Mathematics Stack Exchange, 2017, URL:https://math.stackexchange.com/q/2093697 (version: 2017-01-12).

[Kim22] Chan-Ho Kim, *personal communication*.

[KO99] Winfried Kohnen and Ken Ono, *Indivisibility of class numbers of imaginary quadratic fields and orders of Tate–Shafarevich groups of elliptic curves with complex multiplication*, Invent. math. **135** (1999), no. 2, 387–398.

[Kob03] Shinichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. math. **152** (2003), no. 1, 1–36.

[KPW17] Chan-Ho Kim, Robert Pollack, and Tom Weston, *On the freeness of anticyclotomic Selmer groups of modular forms*, Int. J. Number Theory **13** (2017), no. 06, 1443–1455.

[Kra95] Alain Kraus, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 9, 1143–1146. MR 1360773

[LV19] Matteo Longo and Stefano Vigni, *Plus/minus Heegner points and Iwasawa theory of elliptic curves at supersingular primes*, Boll. Unione Mat. Ital. **12** (2019), no. 3, 315–347. MR 3989744

[Mil06] James S Milne, *Arithmetic duality theorems*, second ed., BookSurge, LLC, 2006.

[Pra58] Karl Prachar, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*, Monatsh. Math. **62** (1958), 173–176. MR 92806

[PW11] Robert Pollack and Tom Weston, *On anticyclotomic $\mu$-invariants of modular forms*, Compos. Math. **147** (2011), no. 5, 1353–1381.

[Ser71] Jean-Pierre Serre, *Galois properties of finite order points of elliptic curves*, Invent. Math. **15** (1971), no. 4, 259–331.

[Ser81] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401. MR 644559

[Sob13] Pablo Soberón, *Problem-solving methods in combinatorics: An approach to olympiad problems*, Springer Basel, 2013.

[Wal10] Nahid Walji, *Supersingular distribution on average for congruence classes of primes*, Acta Arith. **142** (2010), no. 4, 387–400.

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