Elliptic Curves Over Galois Number Fields

by

Ross Jarratt Paterson

A thesis submitted in fulfilment of the requirements
for the degree of

Doctor of Philosophy

at the

School of Mathematics & Statistics
College of Science & Engineering
University of Glasgow

September 2022

To my family

Abstract

This thesis is concerned with the statistical behaviour of elliptic curves over extension fields. That is, if $K/\mathbb{Q}$ is a finite extension, we study the arithmetic of E/K as E ranges in natural families of elliptic curves *defined over* $\mathbb{Q}$. We study the statistical properties of the action of the group $\mathrm{Aut}(K)$ on $E(K)$ and on the p-Selmer groups $\mathrm{Sel}_p(E/K)$ where p is a prime number.

We construct special generalised Selmer groups, and show that these are related to certain representation-theoretic invariants of $\mathrm{Sel}_p(E/K)$. The sizes of these groups are related to the cokernels of the norm maps over the completions of K, which we go on to compute in several cases. In the statistical component of this thesis, we study quadratic twist families of elliptic curves and the family of 'all elliptic curves'.

For quadratic twist families we consider the behaviour over quadratic extensions. Using methods similar to those of Heath-Brown [HB93, HB94] and of Fouvry–Klüners [FK07], we determine the complete distribution of the 2-Selmer groups as Galois modules. This also allows us to determine representation-theoretic properties for the Mordell–Weil groups of 100% of twists.

For the family of all elliptic curves over $\mathbb{Q}$, we consider the behaviour with respect to a general finite Galois extension K/F. Writing $G = \mathrm{Gal}(K/F)$, our first main result is that the difference in dimension between $\mathrm{Sel}_p(E/K)^G$ and $\mathrm{Sel}_p(E/F)$ has bounded average in this family. Using this we are able, with additional assumptions on K/F and p, to bound the average dimension of $\mathrm{Sel}_p(E/K)$ and so the average rank of the Mordell–Weil group $E(K)$. Our methods also allow us to bound how often certain $\mathbb{Z}[G]$-lattices occur as summands of $E(K)$, with additional assumptions on F. We refine our results in the setting where $K/\mathbb{Q}$ is multiquadratic and $p = 2$, and prove strong upper and lower bounds for the average dimension of the 2-Selmer group.

Contents

List of Tables

Acknowledgements

First and foremost, I would like to express my deep gratitude to my supervisor, Alex Bartel: for suggesting the problem that started me on this journey; for the abundance of advice, encouragement, and support, that he has given me; and for the community spirit that he has fostered in the Number Theory group during my time here.

I am very grateful to Adam Morgan for a fruitful first collaboration which acted as a port during the storm of the early pandemic in 2020, as well as a plethora of fascinating and helpful conversations. I would also like to thank Peter Koymans, Carlo Pagano, and Efthymios Sofos for helpful conversations directing me toward using the Redei symbol in proving Theorem 1.2.5. I am also grateful to my examiners, Vladimir Dokchitser and Efthymios Sofos, for their patient reading of this thesis and insightful comments on its presentation and contents.

I wish to thank my fellow PhD students, who made the office such a vibrant place and made Zoom lunches an excellent distraction from the end of the world (as we knew it). Among them, I am particularly grateful to Dave, James, Jamie, Jay, Kellan, Mikel, Niall, Okke, Sarah, and Vitalijs.

This work would not have been possible without the support of my family. In particular I thank my wife, Rebecca, for being such a positive and inspiring force in my life. Throughout my life I have been offered boundless encouragement to pursue mathematical joy, from my parents, brother, and my grandparents, and I am immensely grateful to them for this.

Throughout this work I was supported by a PhD scholarship from the Carnegie Trust for the Universities of Scotland. I am grateful to the Carnegie Trust: not just for the generous financial support they have provided, but for their compassionate and transparent communications during the pandemic.

Author's declaration

I declare that, except where explicit reference is made to the contribution of others, this dissertation is the result of my own work and has not been submitted for any other degree at the University of Glasgow or any other institution.

Chapter 1

Introduction

This thesis sits at the intersection of arithmetic statistics, arithmetic geometry and representation theory. In its modern form, arithmetic statistics began with work of Henri Cohen and Hendrik W. Lenstra Jr. [CL84] in the early 1980's on statistical properties of class groups of quadratic number fields. Their work, in turn, was motivated by investigations of Gauss some 200 years earlier. The basic philosophy of the area is to study arithmetic objects in natural families, instead of individually, and determine statistical results for properties of interest. Meanwhile, in arithmetic geometry, elliptic curves present some of the most difficult and longest standing challenges in modern number theory.

In this thesis we study elliptic curves defined over the rational numbers in natural families, and determine statistical results on their behaviour over higher number fields. The results will describe representation-theoretic properties of their Mordell–Weil groups and p-Selmer groups as Galois modules.

§ 1.1 | Context

In this thesis we will be concerned with quadratic twist families of elliptic curves, and the family of 'all elliptic curves'. This section will recall some results from the literature regarding these families when we look at their behaviour over the rational numbers, in order to give context to our results in the thesis.

§ 1.1.1 | Quadratic Twist Families

Quadratic twist families of elliptic curves are amongst the first for which statistical results were proved.

Definition 1.1.1. Let $E : y^2 = f(x)$ be an elliptic curve defined over $\mathbb{Q}$, and d be a squarefree integer. Then the quadratic twist of E by d is the elliptic curve

$$E_d : dy^2 = f(x).$$

Note that this curve becomes isomorphic to E over $\mathbb{Q}(\sqrt{d})$.

The quadratic twist family associated to an elliptic curve is then the collection of quadratic twists, indexed by squarefree integers d. This family comes with a natural

ordering: we consider all E_d for $|d|$ at most some positive real number X, estimate statistical quantities of interest for this finite set of twists, and then take a limit as $X \to \infty$.

In the 1990's Heath-Brown [HB93, HB94] gave some initial results on the quadratic twists of the congruent number curve. He obtained the distribution of $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/\mathbb{Q})$ as d varies in the set of odd squarefree integers. Heath-Brown's results were then extended by Kane [Kan13], building on earlier work of Swinnerton-Dyer [SD08]. The main outcome was the following.

Theorem 1.1.2 ([Kan13, Theorem 3 and discussion following])**.** *Write $\alpha_0 = \alpha_1 = 0$, and for $n \geq 0$*

$$\alpha_{n+2} = \frac{2^n}{\prod_{j=1}^{n}(2^j - 1)\prod_{j=0}^{\infty}(1 + 2^{-j})}.$$

Let $E/\mathbb{Q}$ be an elliptic curve with full 2-torsion and no cyclic 4-isogeny defined over $\mathbb{Q}$. Then for each $r \geq 0$

$$\lim_{X\to\infty} \frac{\#\left\{|d| \leq X \ : \ \substack{d \text{ squarefree,} \\ \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/\mathbb{Q})=r,}\right\}}{\#\left\{|d| \leq X \ : \ d \text{ squarefree}\right\}} = \alpha_r.$$

Remark 1.1.3. This shows that for more than 99.9% of twists E_d of such a curve E, we have $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/\mathbb{Q}) \leq 6$.

In general, the statistical behaviour of 2-Selmer groups in quadratic twist families depends on the structure of the 2-torsion. Below we summarise some of the main results for other quadratic twist families.

(A) If $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) = 0$ then the works of Heath-Brown, Swinnerton-Dyer and Kane mentioned above determine the distribution of the 2-Selmer group as in Theorem 1.1.2, so long as E has no cyclic 4-isogeny;

(B) If $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ then Klagsbrun–Lemke Oliver [KLO16] showed that for each fixed integer $z \geq 0$, a proportion of at least 50% of twists E_d satisfy $\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/\mathbb{Q}) \geq z$. There are similar results for a slightly less general setting proved earlier by Xiong–Zaharescu [XZ08].

(C) If $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$ then Klagsbrun–Mazur–Rubin [KMR14] determine the distribution of $\dim \mathrm{Sel}_2(E_d/\mathbb{Q})$, albeit with respect to a different ordering on the twists from the natural one we have discussed above.

Remark 1.1.4. There is also the very recent work of Smith, [Smi17, Smi22], which determines the distribution of 2^∞-Selmer groups in each of the twist families above, all ordered in the natural way, as well as some other cases. This work is still very recent, but is a huge step forward.

In this thesis we consider the family in (A), and study the 2-Selmer groups over quadratic extensions. The results will, however, be closer in nature to the outcome in

(B). There is an analogy explaining why this is the case, but we will not discuss it in this thesis and instead direct the reader to our paper [MP22] for this.

§ 1.1.2 | The Family of All Elliptic Curves

We also study the family of 'all elliptic curves'. For the duration of this thesis, we introduce the following notation.

Notation 1.1.5. Let

$$\mathcal{E} := \left\{(A,B) \in \mathbb{Z}^2 : \begin{smallmatrix}\gcd(A^3,B^2) \text{ is } 12^{\text{th}}\text{-power free,}\\ 4A^3+27B^2\neq 0\end{smallmatrix}\right\}.$$

This set parametrises elliptic curves via the identification $(A,B) \leftrightarrow E_{A,B} : y^2 = x^3 + Ax + B$. It is well known, see e.g. [Sil09, III.1], that every elliptic curve defined over the rational numbers is isomorphic to a unique curve parametrised by $\mathcal{E}$. The natural ordering on $\mathcal{E}$ is induced by the height: for $(A,B) \in \mathcal{E}$, the height of $E_{A,B}$ is defined to be $\max\left\{|A|^3, B^2\right\}$. For every positive real number X, we write $\mathcal{E}(X)$ for the finite subset of $\mathcal{E}$ of curves which have height at most X. There is also the naïve height, defined to be $\max\left\{4|A|^3, 27B^2\right\}$, and we similarly define $\mathcal{E}'(X)$ to be the set of curves in $\mathcal{E}$ with naïve height at most X.

Very little was known about statistics for the family $\mathcal{E}$ until the groundbreaking results of Bhargava–Shankar. In a series of papers from 2010–2013 they established the following result.

Theorem 1.1.6 ([BS15a, BS15b, BS13])**.** *Let $p \in \{2,3,5\}$, then*

$$\lim_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}'(X)} \#\mathrm{Sel}_p(E_{A,B}/\mathbb{Q})}{\#\mathcal{E}'(X)} = p+1$$

In fact their results are stronger: they can replace $\mathcal{E}$ with any 'large family'. This more general class of families includes those defined by finitely many congruence conditions on the set $\mathcal{E}$ or indeed even some which are defined by infinitely many such conditions – see Definition 7.4.7 for the definition. Initially the main corollary of interest from the above result was that this shows that the average of $\mathrm{rk}E(\mathbb{Q})$ is finite.

Corollary 1.1.7 ([BS13, Theorem 3])**.** *The average rank of elliptic curves is finite. In fact,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \mathrm{rk}E_{A,B}(\mathbb{Q})}{\#\mathcal{E}(X)} < 0.885.$$

Shortly after, even preceding the final paper in the series of Bhargava–Shankar, a heuristic of Poonen–Rains emerged which seeks to explain these averages conceptually. In words: they note that the p-Selmer group is naturally an intersection of maximal isotropic subgroups of an infinite dimensional quadratic $\mathbb{F}_p$-space, and so model it as such. One of the predictions arising from their model is the following.

Conjecture 1 ([PR12, Conjecture 1.1(b)])**.** *Fix a prime number p. The average of $\#\mathrm{Sel}_p(E_{A,B}/\mathbb{Q})$, as $(A,B) \in \mathcal{E}$ varies is $p+1$.*

The heuristic of Poonen–Rains agrees with the averages found by Bhargava–Shankar in the cases $p = 2, 3, 5$. Moreover, the prediction obtained from their heuristic for the second moment of $\#\mathrm{Sel}_2(E/\mathbb{Q})$ agrees with recent work of Bhargava–Shankar–Swaminathan [BSS21]. These are all of the known statistical quantities related to the heuristics and so, to date, the Poonen–Rains heuristics are uncontested.

In light of the 'large family' generality in which Theorem 1.1.6 holds, we expect the average in Conjecture 1 to hold for any family of $E/\mathbb{Q}$ defined by a fixed finite number of congruence conditions. We mark this as a hypothesis for later use below.

Hypothesis 1. *Let $\tilde{\mathcal{E}} \subseteq \mathcal{E}$ be a subset defined by finitely many congruence conditions, and for every positive real number X write $\tilde{\mathcal{E}}(X) = \mathcal{E}(X) \cap \tilde{\mathcal{E}}$. For each prime number p, the average of $\#\mathrm{Sel}_p(E_{A,B}/\mathbb{Q})$ for $(A, B) \in \tilde{\mathcal{E}}(X)$ goes to $p + 1$ as $X \to \infty$.*

One of the main directions of this thesis is estimating analogous quantities to those in Theorem 1.1.6, though in general our methods describe the dimension of the p-Selmer group rather than its size, over extension fields. One input for our theorems will be Theorem 1.1.6, and so in particular we can use the extension of the Poonen–Rains heuristics in Hypothesis 1 to extend our results beyond the restricted setting in which they can be proved at present. See §1.5.3 for more on this.

§ 1.2 | Main Results: Quadratic Twist Families

We now outline our main results for the family of quadratic twists of such E. This is joint work with Adam Morgan [MP22]. We will be concerned with the statistical behaviour of the groups $\mathrm{Sel}_2(E_d/K)$, for a fixed elliptic curve $E/\mathbb{Q}$ with full 2-torsion, as d varies in the set of squarefree integers.

The statistical work described here can be found in Part II (Chapter 4), with the algebraic inputs being recalled at the start from Chapter 2.

§ 1.2.1 | Erdős–Kac for 2-Selmer

Our first result, strongly reminiscent of the Erdős–Kac theorem [EK40], shows that $\dim \mathrm{Sel}_2(E_d/K)$ is normally distributed with mean $\log\log|d|$ and variance $2\log\log|d|$.

Theorem 1.2.1 (Corollary 4.3.5)**.** *Let $E/\mathbb{Q}$ be an elliptic curve such that $E[2] \subseteq E(\mathbb{Q})$, and $K/\mathbb{Q}$ be a quadratic extension. For every $z \in \mathbb{R}$ we have*

$$\lim_{X\to\infty} \frac{\#\left\{|d| \le X \text{ squarefree } : \frac{\dim \mathrm{Sel}_2(E_d/K) - \log\log|d|}{\sqrt{2\log\log|d|}} \le z\right\}}{\#\left\{|d| \le X \text{ squarefree }\right\}} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-t^2/2} dt.$$

One immediate consequence is that, for any fixed real number z, the proportion of $|d| \le X$ for which $\dim \mathrm{Sel}_2(E_d/K)$ is smaller than z tends to 0 as X tends to infinity. We present this as Corollary 4.2.12. By contrast recall that, if we assume that E has no cyclic 4-isogeny defined over $\mathbb{Q}$, for any fixed integer $n \ge 2$ Theorem 1.1.2 shows

that a positive proportion of twists E_d have $\dim \mathrm{Sel}_2(E_d/\mathbb{Q})$ equal to n. Thus Theorem 1.2.1 shows that the groups $\mathrm{Sel}_2(E_d/K)$ exhibit significantly different behaviour to the corresponding groups over $\mathbb{Q}$.

As a consequence of this discrepancy, we are able to show that, at least when E has no cyclic 4-isogeny defined over $\mathbb{Q}$, Theorem 1.2.1 remains true when $\dim \mathrm{Sel}_2(E_d/K)$ is replaced by $\dim Ш(E_d/K)[2]$ in the statement. We present this alternative perspective as Corollary 4.3.6.

§ 1.2.2 | Structural Results for 100% of Twists

The growth of the 2-Selmer group when passing from $\mathbb{Q}$ to a quadratic extension is explained by the Selmer structures in Chapter 2. For each twist $E_d/\mathbb{Q}$, roughly speaking, we identify a quotient of the invariant subgroup $\mathrm{Sel}_2(E_d/K)^{\mathrm{Gal}(K/\mathbb{Q})}$ whose dimension is controlled by purely local invariants. This is analogous to the situation for class groups of quadratic fields where the dimension of the 2-torsion of the (narrow) class group admits an explicit description via genus theory. In this setting, the definition of this quotient appears in work of Kramer [Kra81].

In order to prove Theorem 1.2.1 we study, as d varies, the discrepancy between the 'systematic' part of the 2-Selmer group $\mathrm{Sel}_2(E_d/K)$ alluded to above, and the full 2-Selmer group. Ultimately, Theorem 1.2.1 is a consequence of the following result, giving a precise description of the full 2-Selmer group for 100% of twists.

Theorem 1.2.2 (Corollary 4.3.4)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with $E[2] \subseteq E(\mathbb{Q})$, and let $K/\mathbb{Q}$ be a quadratic extension. For* 100% *of squarefree d ordered by absolute value, the* $\mathrm{Gal}(K/\mathbb{Q})$*-action on* $\mathrm{Sel}_2(E_d/K)$ *is trivial, and we have*

$$\dim \mathrm{Sel}_2(E_d/K) = -2 + \sum_{v \text{ place of } \mathbb{Q}} \dim E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E_d(K_w). \tag{1.1}$$

Here, in each summand, w is a choice of place extending v and $N_{K_w/\mathbb{Q}_v}$ is the norm map.

Remark 1.2.3. In §4.2 we study the behaviour of the right hand side of (1.1). Even when E does not have all its 2-torsion defined over $\mathbb{Q}$, we are still able to use this to gain partial control of the Selmer groups $\mathrm{Sel}_2(E_d/K)$ as d varies. In particular, provided that $\mathbb{Q}(E[2]) \cap K = \mathbb{Q}$ we show in Corollary 4.2.12 that for any fixed real number z, the dimension of $\mathrm{Sel}_2(E_d/K)$ exceeds z for 100% of twists d.

Since the group $E_d(K)/2E_d(K)$ sits inside $\mathrm{Sel}_2(E_d/K)$, we can deduce some consequences for Mordell–Weil groups from the above results. Specifically, for an elliptic curve $E/\mathbb{Q}$ and squarefree integer d, define the Mordell–Weil lattice

$$\Lambda(E_d/\mathbb{Q}) := E_d(\mathbb{Q})/E_d(\mathbb{Q})_{\mathrm{tors}}.$$

For a quadratic extension $K/\mathbb{Q}$, write $\Lambda(E_d/\mathbb{Q})^{\chi_K}$ for the $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module with underlying abelian group $\Lambda(E_d/\mathbb{Q})$ on which the generator of $\mathrm{Gal}(K/\mathbb{Q})$ acts as mul-

tiplication by -1. We have the following result, giving a complete description of the Galois module structure of $E_d(K)$ for 100% of d.

Theorem 1.2.4 (Corollary 4.3.10)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with $E[2] \subseteq E(\mathbb{Q})$, and $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ be a quadratic extension. Then for 100% of squarefree d ordered by absolute value, we have an isomorphism of $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-modules*

$$E_d(K) \cong (\mathbb{Z}/2\mathbb{Z})^2 \ \oplus \ \Lambda(E_d/\mathbb{Q}) \ \oplus \ \Lambda(E_{d\theta}/\mathbb{Q})^{\chi_K}, \tag{1.2}$$

where here $(\mathbb{Z}/2\mathbb{Z})^2$ carries trivial $\mathrm{Gal}(K/\mathbb{Q})$-action, and $\Lambda(E_{d\theta}/\mathbb{Q})^{\chi_K}$ is the Galois module defined above.

§ 1.2.3 | Prime twists of the congruent number curve

It is natural to ask if the description in Theorem 1.2.2 simply holds for *all* d. This is, however, not the case: we provide infinitely many examples where the Galois action is nontrivial in §4.6. Specifically, take E to be the congruent number curve:

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

Further, we restrict to the setting where $K = \mathbb{Q}(\sqrt{\theta})$ is an imaginary quadratic extension of class number 1 in which 2 is inert. Alternatively put, we can assume $\theta \in \{-3, -11, -19, -43, -67, -163\}$. For a prime number p, via the classification of $\mathbb{F}_2[G]$-modules ([Alp86, page 24], see also Lemma 2.2.12), we can define non-negative integers $e_1(E_p/K)$ and $e_2(E_p/K)$ such that we have an $\mathbb{F}_2[G]$-module isomorphism

$$\mathrm{Sel}_2(E_p/K) \cong \mathbb{F}_2^{e_1(E_p/K)} \oplus \mathbb{F}_2[\mathrm{Gal}(K/\mathbb{Q})]^{e_2(E_p/K)}.$$

Theorem 1.2.5 (Theorem 4.6.7)**.** *Let $E/\mathbb{Q}$ be the congruent number curve, and $K/\mathbb{Q}$ be an imaginary quadratic field with class number 1 in which 2 is inert. Then for each pair $(e_1, e_2) \in \mathbb{Z}^2_{\geq 0}$, the natural density of prime numbers p for which $e_1(E_p/K) = e_1$ and $e_2(E_p/K) = e_2$ is as follows:*

$$\lim_{X\to\infty} \frac{\#\left\{p \leq X \text{ prime } : \begin{smallmatrix} e_1(E_p/K)=e_1 \text{ and} \\ e_2(E_p/K)=e_2 \end{smallmatrix}\right\}}{\#\{p \leq X \text{ prime}\}} = \begin{cases} 9/16 & \text{if } (e_1, e_2) = (4, 0), \\ 1/16 & \text{if } (e_1, e_2) = (2, 2), \\ 4/16 & \text{if } (e_1, e_2) = (2, 1), \\ 2/16 & \text{if } (e_1, e_2) = (2, 0), \\ 0 & \text{else.} \end{cases}$$

In particular, the proportion of prime twists of the congruent number curve for which the $\mathrm{Gal}(K/\mathbb{Q})$-action on $\mathrm{Sel}_2(E_p/K)$ is non-trivial is equal to 5/16.

§ 1.3 | Main Results: All Elliptic Curves over Galois Extensions

We now outline the main results in this thesis for the family of all elliptic curves, in the sense defined in Notation 1.1.5. More precisely, for a fixed finite Galois extension of a number field K/F and prime number p we study the behaviour of $\mathrm{Sel}_p(E/K)$ as a $\mathbb{Z}[\mathrm{Gal}(K/F)]$-module, as $E/\mathbb{Q}$ varies according to height. These results are contained in a preprint of the author [Pat21]. The main algebraic and geometric work can be found in this thesis in Part I, and the statistical results are then proved in Part III Chapter 5.

§ 1.3.1 | Average Ranks

Our first main result is the first known generalisation of Corollary 1.1.7 to average ranks over extension fields. Firstly: by a multiquadratic number field, we will always mean a finite Galois extension $F/\mathbb{Q}$ with $\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$ for some $r > 0$; and for a prime number p we say that a Galois field extension K/F is a p-extension if $\mathrm{Gal}(K/F)$ is a finite p-group.

Theorem 1.3.1. *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum\limits_{(A,B)\in\mathcal{E}(X)} \mathrm{rk}E_{A,B}(K)}{\#\mathcal{E}(X)} \ll [K:\mathbb{Q}]\omega(\Delta_K)$$

where the implied constant is absolute. Moreover, assuming Hypothesis 1 the same conclusion holds (uniformly) over all prime numbers p.

Indeed we prove an explicit version of this result, see

Remark 1.3.2. There are stronger bounds in the case that $K/\mathbb{Q}$ is multiquadratic. These are obtained from the results of Bhargava and Shankar by computing the average size of the 5–Selmer group of the Weil restrictions of our $E/\mathbb{Q}$ from K (see Proposition 5.2.14).

Remark 1.3.3. The growth of our bound compares nicely with Iwasawa–theoretic considerations in $\mathbb{Z}_p$–towers above F, as we discuss in §1.3.6.

§ 1.3.2 | The Explicit Bound

The explicit version of the bound in depends on certain constants $C_p(K/F)$, which we will now introduce.

Definition 1.3.4. For each prime number p and finite Galois extension of number fields K/F,

$$C_p(K/F) := 2\omega_F(6p\Delta_K) + [F:\mathbb{Q}] + \delta_2(p)r_1(F) + 2\sum_{\substack{\ell \text{ prime} \\ \ell\nmid 6p\Delta_K}} \omega_F(\ell)\frac{2\ell^8-\ell^7-1}{\ell^{10}-1},$$

where: $\delta_2(p) = 1$ if $p = 2$ and $\delta_2(p) = 0$ otherwise; for an integer n, $\omega_F(n)$ is the number of prime ideals of F which divide the ideal generated by n over the integers of F; $r_1(F)$ is the number of real embeddings of F; and Δ_K is the discriminant of K.

Note that the asymptotic behaviour of $C_p(K/F)$ is estimated by

$$C_p(K/F) \ll [F : \mathbb{Q}]\omega(\Delta_K)$$

with absolute implied constant. We prove the following explicit version of Theorem 1.3.5.

Theorem 1.3.5. *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \mathrm{rk}E_{A,B}(K)}{\#\mathcal{E}(X)} \leq \begin{cases} [K : F]C_2(K/F) + [K : \mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3^{7/2}}{2^{8/3}}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ [K : F]\left(C_p(K/F) + \left(\frac{27}{4}\right)^{5/6}\frac{p+1}{p}[F : \mathbb{Q}]\right) & \text{else,} \end{cases}$$

Moreover, assuming Hypothesis 1 the same conclusion holds if p is any prime number.

Example 1.3.6. *Theorem 1.3.5 implies that there are infinitely S_3 number fields K for which*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \mathrm{rk}E_{A,B}(K)}{\#\mathcal{E}(X)} < 65. \tag{1.3}$$

Indeed, for each prime number ℓ take K_ℓ to be the splitting field of $X^3 - \ell$. These are cubic extensions of their shared quadratic subfield $F = \mathbb{Q}(\zeta_3)$, so we compute that if $\ell \equiv 2 \mod 3$ then $C_3(K_\ell/F) \leq 8.44$; thus (1.3) holds with $K = K_\ell$.

Remark 1.3.7. Although we can often obtain uniform bounds for average ranks over infinitely many extensions with Galois group isomorphic to some fixed G, we cannot use these methods to obtain a bound which works for a positive proportion of such extensions. Indeed, any sensible ordering of such extensions would see the number of ramified primes grow, which in turn causes our bound to grow.

§ 1.3.3 | Galois Descent

Theorem 1.3.5 is proved by studying the statistical behaviour of the Galois fixed space inside Selmer groups. For a finite Galois extension of number fields K/F and prime number p, we study the failure of Galois descent from K to F for p-Selmer groups of elliptic curves $E/\mathbb{Q}$. That is, we examine the difference

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K)^G - \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F), \tag{1.4}$$

where $G = \mathrm{Gal}(K/F)$. This difference between the fixed space and the Selmer group over the base field comes in two flavours: “good” and “bad” characteristic.

In the case that $p \nmid \#G$ this difference is 0: the finite cohomology groups $H^i(K/F, E(K)[p])$ and their local analogues are trivial, so the inflation–restriction exact sequence yields an isomorphism $\mathrm{Sel}_p(E/F) \cong \mathrm{Sel}_p(E/K)^G$ (see also §5.2 for a more geometric explanation). In other words, Galois descent holds in the "good characteristic" case.

The interesting case, that of so-called "bad characteristic", is when $p \mid \#G$. In fact, in this case, Galois descent can fail to an arbitrary extent. Indeed, if $E/\mathbb{Q}$ is an elliptic curve with $E[2] \subseteq E(\mathbb{Q})$ and $K/\mathbb{Q}$ is a quadratic extension: for the fixed space, our work with Morgan [MP22], specifically Theorems 1.2.1 and 1.2.2, shows that for every fixed positive real number z, 100% of quadratic twists E_d of E have

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/K)^G = \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/K) > z;$$

however by Remark 1.1.3 more than 99.9% of quadratic twists E_d of E have

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E_d/\mathbb{Q}) \leq 6.$$

In this latter proportion of twists, the difference (1.4) must be arbitrarily large.

The core statistical result in Chapter 5 shows that, despite this, in the family $\mathcal{E}$ the failure of Galois descent is not typically large.

Theorem 1.3.8 (Theorem 5.3.8)**.** *Let p be a prime number, F be a number field and K/F be a finite Galois extension. Writing $G = \mathrm{Gal}(K/F)$, we have that*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{A,B}/K)^G - \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)} \leq C_p(K/F),$$

where $C_p(K/F)$ is the constant of Definition 1.3.4.

§ 1.3.4 | Selmer Ranks

In the case of a Galois p-extension, the p-Selmer group is a *modular* representation of the Galois group. Appealing to the theory of such, we use Theorem 1.3.8 to bound the average dimension of the full Selmer group, not just the Galois fixed space.

Theorem 1.3.9 (Corollary 5.4.2)**.** *Let $p \in \{2, 3, 5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{A,B}/K)}{\#\mathcal{E}(X)}$$
$$\leq \begin{cases} [K:F]C_2(K/F) + [K:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3^{7/2}}{2^{8/3}}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ [K:F]\left(C_p(K/F) + \left(\frac{27}{4}\right)^{5/6} \frac{p+1}{p}[F:\mathbb{Q}]\right) & \text{else,} \end{cases}$$

where $C_p(K/F)$ and $C_p(F/\mathbb{Q})$ are the constants of Definition 1.3.4. Moreover, assuming Hypothesis 1 the same conclusion holds if p is any prime number.

It is from this result, and the usual inclusion $E(K)/pE(K) \subseteq \mathrm{Sel}_p(E/K)$, that we obtain Theorem 1.3.5.

Example 1.3.10. *The bounds obtained in Theorem 1.3.9 are often much larger than the bound in Corollary 1.1.7. Let $K/\mathbb{Q}$ be the splitting field of $x^{10}-35x^6+130x^4+160$, so that the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to D_{10} the dihedral group of order 10. In this case, $F=\mathbb{Q}(\sqrt{-10})$ is a multiquadratic field contained in K, and K/F is a degree 5 extension, so we apply Theorem 1.3.9 with $p=5$. We can compute that $C_5(K/F)\leq 8.36$, so the average dimension of 5-Selmer groups over K of elliptic curves over $\mathbb{Q}$ is less than 101.*

§ 1.3.5 | Mordell–Weil Lattices

We deduce some representation–theoretic information about Mordell-Weil lattices from Theorem 1.3.8. For each elliptic curve $E/\mathbb{Q}$ and each number field K, we write $\Lambda(E/K)$ for the Mordell–Weil lattice:

$$\Lambda(E/K) = E(K)/E(K)_{\mathrm{tors}}.$$

For a finite Galois extension K/F, writing $G=\mathrm{Gal}(K/F)$, $\Lambda(E/K)$ is a $\mathbb{Z}$-free $\mathbb{Z}[G]$-module. We refer to such modules as $\mathbb{Z}[G]$-lattices. In Definition 5.5.2 we define the multiplicity of a $\mathbb{Z}[G]$-lattice Λ in $\Lambda(E/K)$ to be the largest integer $e=e_\Lambda(K/F;E)$ such that Λ^e is isomorphic to a direct summand of $\Lambda(E/K)$. We prove a bound for the average of this multiplicity in certain cases.

Theorem 1.3.11 (Corollary 5.5.8)**.** *Let $p\in\{2,3,5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a finite Galois extension. Writing $G=\mathrm{Gal}(K/F)$, for every $\mathbb{Z}[G]$-lattice Λ such that $\dim_{\mathbb{F}_p}(\Lambda/p\Lambda)^G\geq 1$,*

$$\limsup_{X\to\infty}\frac{\sum_{(A,B)\in\mathcal{E}(X)} e_\Lambda(K/F;E_{A,B})}{\#\mathcal{E}(X)} \leq \frac{1}{\dim_{\mathbb{F}_p}(\Lambda/p\Lambda)^G}\cdot\begin{cases} C_2(K/F)+[F:\mathbb{Q}]\left(C_2(F/\mathbb{Q})+\frac{3^{7/2}}{2^{8/3}}\right) & \text{if } p=2 \text{ and } F\neq\mathbb{Q},\\ C_p(K/F)+\left(\frac{27}{4}\right)^{5/6}\frac{p+1}{p}[F:\mathbb{Q}] & \text{else,}\end{cases}$$

where $C_p(K/F)$ and $C_p(F/\mathbb{Q})$ are the constants of Definition 1.3.4. Moreover, assuming Hypothesis 1 the same conclusion holds if p is any prime number.

Remark 1.3.12. For example, if G is a p-group then, by the orbit stabiliser theorem, for every $\mathbb{Z}[G]$-lattice Λ we have $\dim_{\mathbb{F}_p}(\Lambda/p\Lambda)^G\geq 1$. Of course, in this case these multiplicities can already be shown to be have bounded average by applying Theorem 1.3.5.

The following example, which is generalised in §5.5.3, demonstrates that Theorem 1.3.11 is not just a formal consequence of Theorem 1.3.5.

Example 1.3.13. *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G\cong\mathbb{F}_5\rtimes\mathbb{F}_5^\times$, for example the Galois closure of $\mathbb{Q}(\sqrt[5]{2})$.*

Let $\mathfrak{p} \triangleleft \mathbb{Z}[\zeta_5]$ be the prime ideal lying over 5 in the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_5)$, upon which a choice of generator of $\mathbb{F}_5$ acts by multiplication by ζ_5 and $\mathbb{F}_5^\times$ acts as $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$. It is elementary to check that the actions above induce the structure of a $\mathbb{Z}[G]$–lattice on $\mathfrak{p}$. The action of every non-trivial normal subgroup $N \leq G$ is without fixed points, so we cannot obtain bounds on the average multiplicity of $\mathfrak{p}$ in Mordell–Weil lattices by passing to lower Galois extensions and applying Theorem 1.3.5. *Since $\dim_{\mathbb{F}_5}(\mathfrak{p}/5\mathfrak{p})^G = 1$, we can, however, apply Theorem 1.3.11.*

Our method does not allow us to bound the multiplicity of the lattice $\mathbb{Z}[\zeta_5]$ with the analogous action of G: this lattice has no G-fixed space, so for every prime number p we have that

$$(\mathbb{Z}[\zeta_5]/p\mathbb{Z}[\zeta_5])^G \cong H^1(G, \mathbb{Z}[\zeta_5])[p],$$

and one can easily compute that $H^1(G, \mathbb{Z}[\zeta_5]) = 0$. In particular, Theorem 1.3.11 does not allow us to bound the average multiplicity of $\mathbb{Q}(\zeta_5)$ as an irreducible subrepresentation inside of $E(K) \otimes \mathbb{Q}$.

§ 1.3.6 | Comparison to Iwasawa Theory

In Iwasawa theory, the growth of ranks of elliptic curves over $\mathbb{Z}_p$-towers of number fields is studied; we now discuss our results in that context. For the duration of this subsection, we fix a prime number p. If $p \geq 7$ then we also assume Hypothesis 1.

The cyclotomic $\mathbb{Z}_p$–extension of a number field F is the unique subfield $F_{\mathrm{cyc}} \subseteq \bigcup_{n\geq 1} F(\zeta_{p^n})$ such that $\mathrm{Gal}(F_{\mathrm{cyc}}/F) \cong \mathbb{Z}_p$. If $F = \mathbb{Q}$ then this is the only $\mathbb{Z}_p$-extension by the Kronecker–Weber theorem. If $F/\mathbb{Q}$ is imaginary quadratic then the anticyclotomic $\mathbb{Z}_p$-extension of F is the (unique) $\mathbb{Z}_p$-extension of F for which every intermediate extension is dihedral over $\mathbb{Q}$.

Average Rank Growth

We obtain asymptotic bounds for average rank growth in $\mathbb{Z}_p$–extensions of $\mathbb{Q}$ and of multiquadratic fields.

Corollary 1.3.14. *Let F be $\mathbb{Q}$ or a multiquadratic number field, and let F_∞/F be a $\mathbb{Z}_p$–extension. For each integer $n \geq 1$, let F_n be the intermediate field $F \subseteq F_n \subseteq F_\infty$ such that $\mathrm{Gal}(F_n/F) \cong \mathbb{Z}/p^n\mathbb{Z}$. Then for every integer $n \geq 1$*

$$\limsup_{X\to\infty} \frac{\sum\limits_{(A,B)\in\mathcal{E}(X)} \mathrm{rk} E_{A,B}(F_n)}{\#\mathcal{E}(X)} \ll_F p^n,$$

where the implied constant is explicit and depends only on the choice of F.

Remark 1.3.15. Here we can ignore the $\omega_{\mathbb{Q}}(\Delta_{F_n})$ factors since F_n/F can only ramify at primes above p (see e.g. [Was97b, Proposition 13.2]).

Cyclotomic $\mathbb{Z}_p$-Towers

A well known result of Kato and Rohrlich shows that the Mordell–Weil rank of an elliptic curve is bounded in the cyclotomic $\mathbb{Z}_p$-extensions of abelian number fields.

Theorem 1.3.16 ([Kat04, Roh84], see also [Gre01, Theorem 1.4])**.** *For each elliptic curve $E/\mathbb{Q}$, and abelian number field F, there is an integer $C_{E,F_{\mathrm{cyc}}/F}$ such that for all subfields $K \subseteq F_{\mathrm{cyc}}$ we have*

$$\mathrm{rk}(E(K)) \leq C_{E,F_{\mathrm{cyc}}/F}.$$

Currently there is no reason to expect $C_{E,F_{\mathrm{cyc}}/F}$ to be uniformly bounded across all $E/\mathbb{Q}$ – there is substantial debate regarding whether even $\mathrm{rk}E(\mathbb{Q})$ is uniformly bounded (see [PPVW19, §3]). If F is $\mathbb{Q}$ or multiquadratic then our result in Corollary 1.3.14 suggests that these $C_{E,F_\infty/F}$ must not grow too quickly with the height of E. For example, it cannot be the case that the curves of height at most X typically have C_E of order $\exp(X)$ and attain this maximum rank at low levels of the tower F_{cyc}/F.

Anticyclotomic $\mathbb{Z}_p$-Towers

We now consider the anticyclotomic extension of imaginary quadratic fields. The growth number proposition [Maz84, §18] shows that if $E/\mathbb{Q}$ has good ordinary reduction at p, and the special fibre of the Néron model of E is geometrically connected at each place where the extension F_∞/F splits infinitely often, then for each intermediate field F_n (as in Corollary 1.3.14), we must have

$$\mathrm{rk}_p(E/F_n) = a(E, F_\infty/F)p^n + O(1),$$

where the implied constant and leading term $a(E, F_\infty/F)$ are independent of n, and $\mathrm{rk}_p(E/F_n)$ is the p^∞-Selmer rank of E/F_n. Note that, subject to finiteness of the Shafarevich–Tate group, we expect the p^∞-Selmer rank to be precisely the rank of $E(F_n)$. The growth number conjecture of Mazur ([Maz84, §18 Growth Number Conjecture]) predicts that (for $E/\mathbb{Q}$ as in the growth number proposition):

$$a(E, F_\infty/F) = \begin{cases} 0 & \text{if } w_E = 1, \\ 1 & \text{if } w_E = -1 \text{ and } E \text{ does not have CM by } F, \\ 2 & \text{if } w_E = -1 \text{ and } E \text{ has CM by } F. \end{cases}$$

The condition $w_E = -1$ is conjectured to hold for 50% of $E/\mathbb{Q}$, and is known to hold for at least 27.5% of $E/\mathbb{Q}$ by [BS13, Theorem 6]. The additional stipulations coming from the growth number proposition are expected to also hold for a positive proportion of curves, and 100% of $E/\mathbb{Q}$ do not have CM [Duk97]. In particular it is expected that $a(E, F_\infty/F) = 1$ for a positive proportion of $E/\mathbb{Q}$, and so we should expect from this conjecture and finiteness of the Shafarevich–Tate group that *at least*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \mathrm{rk}E_{A,B}(F_n)}{\#\mathcal{E}(X)} \gg p^n.$$

Corollary 1.3.14 shows that this is not just a lower bound but is the worst possible asymptotic behaviour to be expected on average.

§ 1.4 | Main Results: All Elliptic Curves over Multiquadratic Extensions

In the setting of multiquadratic extensions $K/\mathbb{Q}$ we are able to do substantially better than the general setting described in §1.3. Indeed, we are able to obtain stronger upper bounds for the average dimension, with comparably strong lower bounds on the average dimension of the 2-Selmer group. This work will appear in a future article of the author.

§ 1.4.1 | Bounds for Selmer Groups

Our results for 2-Selmer groups over multiquadratic extensions takes some notation to set up.

Definition 1.4.1. Define the functions FS^+ and S^+ from the set of multiquadratic extensions to $\mathbb{R}_{\geq 0}$ by

$$\mathrm{FS}^+(K) := \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}} \dim \mathrm{Sel}_2(E_{A,B}/K)^{\mathrm{Gal}(K/\mathbb{Q})}}{\#\mathcal{E}(X)},$$
$$S^+(K) := \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}} \dim \mathrm{Sel}_2(E_{A,B}/K)}{\#\mathcal{E}(X)},$$

and similarly let $\mathrm{FS}^-(K)$ and $S^-(K)$ be the liminfs for the above ratios. If $\mathrm{FS}^+(K) = \mathrm{FS}^-(K)$ then we denote the resulting value by $\mathrm{FS}(K)$, and similarly for $S(K)$.

We obtain strong upper and lower bounds for $\mathrm{FS}^+(K)$ and $\mathrm{FS}^-(K)$ respectively, which then give the following interesting corollary.

Theorem 1.4.2 (Theorem 6.5.6 and Corollary 6.5.8)**.** *Let $K/\mathbb{Q}$ be a multiquadratic extension. Then*

$$\sum_{\substack{v\in\Omega_\mathbb{Q}\\ v\nmid 6}} \mathcal{G}_K(v) \leq \mathrm{FS}^-(K) \leq \mathrm{FS}^+(K) \leq \sum_{v\in\Omega_\mathbb{Q}} \mathcal{G}_K(v) + \left(\frac{27}{4}\right)^{5/6} \left(4 \prod_{\substack{v\in\Omega_\mathbb{Q}\\ v\nmid 6}} L_v(\mathscr{C}(K))\right),$$

where $\Omega_\mathbb{Q}$ is the set of places of $\mathbb{Q}$, the function $\mathcal{G}_K$ is defined in Definition 1.4.5, and similarly the factors $L_v(\mathscr{C}(K))$ are defined in Definition 6.5.3.

Further, assuming that $\mathcal{K}$ is a set of multiquadratic fields K in which 2 and 3 are totally split and $\mathrm{FS}(K)$ exists, for each of the $K \in \mathcal{K}$

$$\mathrm{FS}(K) = \sum_{v\in\Omega_\mathbb{Q}} \mathcal{G}_K(v) + O\left(\left(\frac{46}{48}\right)^{\omega(\Delta_K)}\right),$$

where the implied constant is independent of K.

We are, in fact, able to similarly obtain upper and lower bounds for $S^+(K)$ and $S^-(K)$ respectively, though these are not as tight and do not give asymptotics as in

Theorem 1.4.2. See Corollary 6.5.7. Restricting to quadratic fields we can do better, firstly we can obtain a result on the Galois action on these Selmer groups in a similar vein to what we prove for quadratic twists in Theorem 1.2.2.

Corollary 1.4.3 (Corollary 6.5.9)**.** *For each squarefree integer d,*

$$\limsup_{X\to\infty} \frac{\#\left\{(A,B)\in\mathcal{E}(X) \ : \ \substack{\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) \text{ acts nontrivially} \\ \text{on } \mathrm{Sel}_2(E_{A,B}/\mathbb{Q}(\sqrt{d}))}\right\}}{\#\mathcal{E}(X)} \ll \left(\frac{46}{48}\right)^{\omega(d)},$$

with constant independent of d.

Note that, unlike in quadratic twist families, we are unable to obtain that the Galois action is trivial for 100% of curves! Indeed, as we will discuss in §1.4.3, computational evidence suggests this action may be nontrivial for a positive proportion of elliptic curves in $\mathcal{E}$. We also obtain strong upper and lower bounds for the average dimension of the 2-Selmer groups of elliptic curves over quadratic extension fields.

Theorem 1.4.4 (Theorem 6.5.11)**.** *Let d be a squarefree integer. Then if we write $K=\mathbb{Q}(\sqrt{d})$,*

$$\sum_{\substack{v\in\Omega_{\mathbb{Q}}\\ v\nmid 6}} \mathcal{G}_K(v) \le S^-(\mathbb{Q}(\sqrt{d})) \le S^+(\mathbb{Q}(\sqrt{d})) \le \sum_{v\in\Omega_{\mathbb{Q}}} \mathcal{G}_K(v) + \left(\frac{27}{4}\right)^{5/6} \left(8\prod_{\substack{v\in\Omega_{\mathbb{Q}}\\ v\nmid 6}} L_v(\mathscr{C}(K))\right).$$

where the function $\mathcal{G}_K$ is defined in Definition 1.4.5, and similarly the factors $L_v(\mathscr{C}(K))$ are defined in Definition 6.5.3. Moreover, assuming that $S(d)$ exists then we have for all $d\equiv 1 \mod 24$

$$S(d) = \sum_{v\in\Omega_{\mathbb{Q}}} \mathcal{G}_K(v) + O\left(\left(\frac{46}{48}\right)^{\omega(d)}\right).$$

§ 1.4.2 | The Constants and Asymptotic Behaviour

The function $\mathcal{G}_K$, for a multiquadratic field K, plays an important role above and so we should now define it and discuss the associated asymptotic behaviour briefly.

Definition 1.4.5 (Definition 6.5.1)**.** For each multiquadratic extension $K/\mathbb{Q}$, define the function

$$\mathcal{G}_K : \Omega_{\mathbb{Q}} \to \mathbb{R}$$

as follows. We map each prime number $\ell\ge 5$ to

$$\mathcal{G}_K(\ell) = \begin{cases} \frac{\ell(\ell^5+1)(\ell-1)(5\ell^3+2\ell^2+3)}{6(\ell^{10}-1)} & \text{if } K/\mathbb{Q} \text{ is ramified and quadratic at } \ell, \\ \frac{\ell(\ell-1)(3\ell^7+3\ell^6+3\ell^5+\ell^4+2\ell^3+\ell^2+3\ell+3)}{3(\ell+1)(\ell^{10}-1)} & \text{if } K/\mathbb{Q} \text{ is unramified and quadratic at } \ell, \\ \frac{\ell(\ell^5+1)(10\ell^5+4\ell^4-7\ell^3+5\ell^2-12)}{12(\ell^{10}-1)(\ell+1)} & \text{if } K/\mathbb{Q} \text{ is biquadratic at } \ell, \\ 0 & \text{if } K/\mathbb{Q} \text{ is totally split at } \ell. \end{cases}$$

For the remaining finite primes we define

$$\mathcal{G}_K(2) = \begin{cases} 0 & \text{if } K/\mathbb{Q} \text{ is totally split at 2,} \\ 2^{2+[K_2:\mathbb{Q}_2]} & \text{else;} \end{cases} \qquad \mathcal{G}_K(3) = \begin{cases} 0 & \text{if } K/\mathbb{Q} \text{ is totally split at 3,} \\ 4 & \text{else.} \end{cases}$$

We then send the infinite place to

$$G_K(\infty) = \begin{cases} \frac{7}{10\sqrt{27}} & \text{if } K \text{ is imaginary,} \\ 0 & \text{else.} \end{cases}$$

In particular we note that the sum $\sum_{v\in\Omega_\mathbb{Q}} \mathcal{G}_K(v)$ converges and has size around $\omega(\Delta_K)$. Indeed for each prime number $\ell \geq 5$

$$\mathcal{G}_K(\ell) \approx \begin{cases} 1 & \text{if } K/\mathbb{Q} \text{ is ramified at } \ell; \\ 1/p^2 & \text{if } K/\mathbb{Q} \text{ is unramified at } \ell. \end{cases}$$

Thus in the asymptotics, for example in Theorem 1.4.4 we get that $S(d)$ behaves asymptotically like $\omega(d)$ as $d \equiv 1 \mod 24$ varies. This compares well with genus theory for quadratic fields. Similarly, in Theorem 1.4.2, $\mathrm{FS}(K)$ behaves asymptotically in K like $\omega(\Delta_K)$ among the multiquadratic fields where 2 and 3 are totally split.

§ 1.4.3 | Limitations & Expectations

What's Wrong with 2 and 3?

The bounds in Theorems 1.4.2 and 1.4.4 are tightest when 2 and 3 are split in the associated (multi)quadratic field. When this condition is not met, the lower bound ignores their contributions and their contribution to the upper bound is far larger than for other primes. In fact the terms $\mathcal{G}_K(2)$ and $\mathcal{G}_K(3)$ are coarse approximations – it should be possible to replace them with terms of a similar shape to the other $\mathcal{G}_K(\ell)$ (for $\ell \geq 5$ prime), and then remove the $v \nmid 6$ condition from the lower bound. We now outline what would be needed to do this.

For $\ell \geq 5$ prime, the rational number $\mathcal{G}_K(\ell)$ is the average (over all $E/\mathbb{Q}$) of the local norm index $E(\mathbb{Q}_\ell)/N_{K_\ell/\mathbb{Q}_\ell}E(K_\ell)$ where K_ℓ is the completion of K at a choice of place above ℓ. The 'correct' term to have for $\mathcal{G}_K(2)$ and $\mathcal{G}_K(3)$ would be this average for those primes. For every prime number ℓ, the local norm index can be understood in terms of ratios of Tamagawa numbers, with an additional 'stretch factor' occurring at $\ell = 2$ (see [KT82]). In order to do obtain the average, one would need to do a detailed analysis of the outcomes of Tate's algorithm [Sil94] for an elliptic curve of the form $y^2 = x^3 + Ax + B$ locally at 2 and 3, as well as account for the behaviour of the 'stretch factor' at 2.

Nontriviality of the Galois Action

As we mention above, Corollary 1.4.3 shows that, for a typical quadratic field K, at most a very small proportion of elliptic curves $E/\mathbb{Q}$ have nontrivial $G = \mathrm{Gal}(K/\mathbb{Q})$

action on $\mathrm{Sel}_2(E/K)$. One then wonders: is this proportion positive or zero?

For every finite dimensional $\mathbb{F}_2[G]$-module M, there is a unique pair $(e_1, e_2) \in \mathbb{Z}^2_{\geq 0}$ such that

$$M \cong \mathbb{F}_2^{e_1} \oplus \mathbb{F}_2[G]^{e_2}, \tag{1.5}$$

where $\mathbb{F}_2$ is the one-dimensional module (upon which G acts trivially) [Alp86, page 24]. Writing $\sigma \in G$ for the nontrivial element, note that the norm element, $N_{K/\mathbb{Q}} = 1 + \sigma \in \mathbb{Z}[G]$, acts on M with image of dimension e_2. Thus the dimension of the image of $N_{K/\mathbb{Q}}$ gives a measurement for how nontrivially G acts on M.

We prove Theorem 1.2.2 (and many of our results, see §1.5) by using a local approximation of the norm on the 2-Selmer group for each $E/\mathbb{Q}$, which we call the corestriction Selmer group and denote by $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$. In a sense, this group contains the image $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$. In Chapter 4 we show that the average size of the corestriction Selmer group when E varies in quadratic twist families is 0, which gives that 100% of twists have trivial Galois action in Theorem 1.2.2 by the above. However, in Chapter 7, we find the average size of the corestriction Selmer group is positive in the family of all elliptic curves.

In principal the norms from the Selmer group could still be trivial for 100% of E, matching the situation for quadratic twists. However, computational experiments (see Appendix B) seem to suggest that the image of the norms may have a positive probability of being nontrivial as they seem to behave similarly to the corestriction Selmer groups. This would mean that the Galois action can be nontrivial a positive proportion of the time.

§ 1.5 | An Impressionistic Sketch of the Thesis

The thesis is divided into three parts: the first contains the general algebraic framework used to prove our results; the second is where the statistical work for quadratic twist families occurs; and the third is where the statistical work for the family of all elliptic curves occurs. The material in Chapter 4 is joint work with Adam Morgan, as are any dependencies from Chapter 2 which are clearly marked therein. The rest of Chapter 2, and indeed the rest of Part I, along with Part III, consists of original work of the author unless otherwise stated. Below is a diagram indicating the order of reading in the thesis.

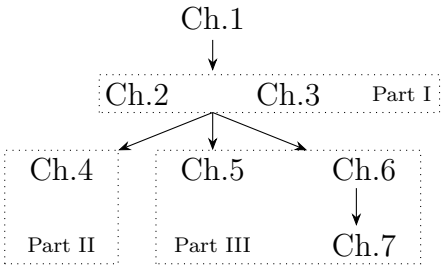


Figure 1.1: Chapter dependency diagram

There is a consistent algebraic approach underpinning the different statistical results that we obtain in this thesis. In this section we will give a sketch of the arguments in this thesis, and for the sake of exposition we will occasionally be imprecise. Wherever the reader sees the symbol $\sim$ they should take this to mean that the mathematical statement it is embedded in uses some poetic license. For the duration of this section, let K/F be a finite Galois extension of number fields with Galois group $G = \mathrm{Gal}(K/F)$, and p be a prime number.

§ 1.5.1 | Part I

In Part I, Chapter 2 we construct 'Selmer structures' associated to elliptic curves E/F which we call the (co)-restriction Selmer structures. Each structure imposes conditions at every $v \in \Omega_F$ on cohomology classes in $H^1(F, E[p])$, and possesses an associated 'Selmer group' - the subgroup of cohomology classes obeying these local conditions at every local place. The Selmer groups for our structures are denoted by

$$\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]),\ \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]) \leq H^1(F, E[p]),$$

where the former is called the restriction Selmer group and the latter the corestriction Selmer group.

In Chapter 2 we determine some useful facts about these groups. The most useful properties are the following.

(i) We have relations between these new Selmer groups and the usual p-Selmer group over the base field:

$$\mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]) \subseteq \mathrm{Sel}_p(E/F) \subseteq \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]).$$

(immediate from definitions, see (2.4))

(ii) The restriction Selmer group approximates (in a precise sense) the Galois fixed space in the p-Selmer group over K:

$$\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) \approx \mathrm{Sel}_p(E/K)^G.$$

(Lemma 2.2.7 (2.3))

(iii) The corestriction Selmer group is, in a sense, the everywhere-local norm group, and so bounds the image of the norm map acting on the p-Selmer group over K:

$$\left(\sum_{\sigma \in G} \sigma\right) \cdot \mathrm{Sel}_p(E/K) \subsetneq \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]).$$

(Lemma 2.2.7 (2.2))

(iv) The quantity

$$g_p(K/F; E) = \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) - \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p])$$

is purely local, in that it is determined by the behaviour of E over all of the completions of F. More precisely, it depends on local norm indices (Definition 2.2.8 and Lemma 2.2.11). We call this quantity the genus theory of the p-Selmer group (it will be defined properly later in the thesis).

In Chapter 3 we compute local norm indices in various settings. The aim here is to determine enough of these indices to obtain statistical control of $g_p(K/F;E)$ as E varies in the families to be studied in Parts II and III.

§ 1.5.2 | Part II

In Part II we consider the setting where $p = 2$, $F = \mathbb{Q}$ and $K/\mathbb{Q}$ is a quadratic extension, so that G has order 2, and we allow our elliptic curve to vary in the family $\{E_d \,:\, d \in \mathbb{Z} \text{ squarefree}\}$ of quadratic twists of a fixed elliptic curve E to obtain the results in §1.2.

In order to motivate our approach: as in (1.5), there is a unique pair $(e_1, e_2) = (e_1(d), e_2(d)) \in \mathbb{Z}^2_{\geq 0}$ such that

$$\mathrm{Sel}_2(E_d/K) \cong \mathbb{F}_2^{e_1} \oplus \mathbb{F}_2[G]^{e_2}, \tag{1.6}$$

where $\mathbb{F}_2$ is considered to have trivial action of G and $\mathbb{F}_2[G]$ is a free rank one module over the group algebra [Alp86, page 24]. Moreover, if σ is the nontrivial element of G then note that the image of the norm has dimension

$$\dim_{\mathbb{F}_2}(1+\sigma)\cdot \mathrm{Sel}_2(E_d/K) = e_2. \tag{1.7}$$

We use methods of Heath-Brown [HB93, HB94], as developed by Fouvry–Klüners [FK07], to determine our key result: that if $E[2] \subseteq E(\mathbb{Q})$ then

$$\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) = 0$$

for 100% of squarefree d. Thus, via (iii), and the decomposition of $\mathrm{Sel}_2(E_d/K)$ above we obtain that

$$\mathrm{Sel}_2(E_d/K) = \mathrm{Sel}_2(E_d/K)^G \tag{1.8}$$

for 100% of squarefree d. Moreover, (iv) then allows us to prove the rest of Theorem 1.2.2.

Now, by (iv) and our key result above, we know that $\dim \mathrm{Sel}_{\mathscr{F}(K)}(\mathbb{Q}, E[2])$ is typically just the genus theory $g_2(K/\mathbb{Q};E)$. We prove that, as long as $K \cap \mathbb{Q}(E[2]) = \mathbb{Q}$, the genus theory quantity $g_2(K/\mathbb{Q};E_d)$ is asymptotically normally distributed as d varies in a sense similar to the classical Erdős–Kac theorem. Combining with (ii) we can move this distribution over to the fixed space $\mathrm{Sel}_2(E/K)^G$, which by §1.2 is the whole Selmer group 100% of the time, proving Theorem 1.2.1.

The Mordell–Weil decomposition result in Theorem 1.2.4 then follows from the fact that (1.8) holds for 100% of d, by considering the possible images of the inclusion

$E_d(K)/2E_d(K) \subseteq \mathrm{Sel}_2(E_d/K)$.

§ 1.5.3 | Part III: The Failure of Galois Descent

We begin in Chapter 5 by considering the most general case: K/F is again a finite Galois extension of a number field with Galois group $G = \mathrm{Gal}(K/F)$, p is any prime number, and we examine $\mathrm{Sel}_p(E/K)$ as E varies in the family $\mathcal{E}$ of all elliptic curves defined over $\mathbb{Q}$. The key result here is Theorem 1.3.8, that the failure of Galois descent, i.e. the quantity

$$\left|\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K)^G - \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F)\right|, \tag{1.9}$$

has average value bounded by an explicit constant $C_p(K/F)$.

We prove Theorem 1.3.8 by using the inclusions in (i) and the relation (iv) to bound (1.9) in terms of the genus theory $g_p(K/F; E)$, which is determined by local norm indices. We then use the computations in Chapter 3 (specifically §3.1) to gain sufficient statistical control of the genus theory to show that it has bounded average, giving the result.

Assume from this point on that G is a p-group. One can bound the dimension of an $\mathbb{F}_p[G]$-module M in terms of its fixed space M^G. To give an impression of why this is true: if we decompose M as a sum of indecomposable modules,

$$M \cong M_1 \oplus \cdots \oplus M_k,$$

then the orbit stabiliser theorem shows that each M_i must have a nontrivial element fixed by G, and so is contributing to the fixed space M^G. This argument is precisely how one argues for $G = \mathbb{Z}/p\mathbb{Z}$. For general p-groups there could be infinitely many indecomposable modules, and so we proceed by taking a Jordan–Hölder decomposition of G and using each intermediate factor $\mathbb{Z}/p\mathbb{Z}$ as above. This allows us to use the Galois descent result above, when G is a p-group, to bound the average of $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K)$ as

$$\mathrm{Avg}\, \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/K) \leq [K : F] \left(\mathrm{Avg}\, \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) + C_p(K/F)\right),$$

as stated precisely in Theorem 5.4.1. Of course, this leaves us with the problem of studying the average dimension of the Selmer groups over F.

Remark 1.5.1. This result is specific to p-groups. If G is not a p-group, then it has at least two conjugacy classes of elements with order coprime to p, meaning that there is at least one simple $\mathbb{F}_p[G]$-module which does not carry the trivial action of G [Alp86, I.3, Theorem 2]. This module could appear as a summand in $\mathrm{Sel}_p(E/K)$, and contribute arbitrarily often to the dimension without interacting with the fixed space.

Assume from this point on that F is $\mathbb{Q}$ or a multiquadratic number field. If p is odd

then we can decompose

$$\mathrm{Sel}_p(E/F) = \bigoplus_{i=1}^{[F:\mathbb{Q}]} \mathrm{Sel}_p(E_{D_i}/\mathbb{Q}),$$

where the set of D_i that we are quadratic twisting by depends only on F. We then use the work of Bhargava–Shankar in Theorem 1.1.6, or assume Hypothesis 1 if $p > 5$, to bound the average of $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E_{D_i}/\mathbb{Q})$ for each D_i and so bound the average of $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F)$ (see §5.2.3). Thus we obtain Theorem 1.3.9, and so Theorem 1.3.5.

Remark 1.5.2. One might wonder how much dependence there is on F being multiquadratic here. For a finite Galois extension $F/\mathbb{Q}$ one can (for all $p \nmid [F:\mathbb{Q}]$) similarly decompose the p-Selmer group $\mathrm{Sel}_p(E/F)$ into a sum of Selmer groups of 'twists' (over $\mathbb{Q}$) in the sense of [MRS07]. If F is multiquadratic then these twists are the quadratic twists above, and since they are elliptic curves we are able to use the result of Bhargava–Shankar. For other extensions, these twists are higher dimensional abelian varieties, for which there is no corresponding result to replace the one of Bhargava–Shankar.

Returning to the setting where G is any group and F any number field, we can deduce Theorem 1.3.11 similarly: we use the Galois descent theorem without substituting $\mathrm{Sel}_p(E/K)$ in place of $\mathrm{Sel}_p(E/K)^G$ (so we do not need G to be a p-group) and then use the above argument for multiquadratic fields to control the average dimension of the Selmer group over the base field $\mathrm{Sel}_p(E/F)$ when F is $\mathbb{Q}$ or multiquadratic.

§ 1.5.4 | Part III: 2-Selmer Groups over Multiquadratic Extensions

We continue our excursion with the family $\mathcal{E}$ in Chapters 6 and 7. In these chapters we restrict to the setting $F = \mathbb{Q}$ and $K/\mathbb{Q}$ is a multiquadratic extension, so G is an elementary abelian 2-group. The division of labour between the two chapters is easy to state:

- Chapter 6 is focussed on obtaining the precise average for the genus theory $g_2(K/\mathbb{Q}; E)$;
- Chapter 7 is focussed on determining the average size of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$.

More precisely, in Chapter 6 we provide a general machinery for averaging certain 'orderly' sums of local constants over the family $\mathcal{E}$. We then apply this machinery to the genus theory, which we are able to completely understand for multiquadratic fields by using the local norm index calculations of Chapter 3 (specifically §3.2). In §6.5 we state the main theorem from Chapter 7 on the average size of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$, postponing the proof to Chapter 7. This tells us that $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ tends to have a small positive average size for a general multiquadratic field K (see Theorem 7.7.13). We combine this with the average of the genus theory to obtain strong upper and lower bounds for the average dimension of the fixed space $\mathrm{Sel}_p(E/K)^G$ via (ii) and (iv), which are presented in Theorem 1.4.2.

Remark 1.5.3. The average size of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ here differs from similar results in two ways. Firstly it is *greater than 1*, so $\mathcal{E}$ differs in behaviour from the quadratic twist families in Chapter 4. Secondly, this average size is a product of certain local densities which *change* depending on which 'large family' of elliptic curves we look at – differing from the average of $\#\mathrm{Sel}_2(E/\mathbb{Q})$ which is independent of the choice of large family.

In Chapter 7 we use the 'Bhargavology' machinery found in the work of Bhargava–Shankar [BS15a]. We repurpose their work on 2-Selmer groups to produce a machine which computes the average size of Selmer groups for those Selmer structures which 'behave well'. This notion is made precise in §7.5 by the definition of a 2-Selmer bundle. We prove that the corestriction Selmer groups behave well in this sense, and so the machine tells us the average size of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ as $E/\mathbb{Q}$ varies.

If K is a quadratic field then we can decompose the Selmer group as we did in (1.6), to derive more information. Specifically, (1.7) tells us that the dimension of the image of the norm element on $\mathrm{Sel}_2(E/K)$ measures how nontrivial its $\mathrm{Gal}(K/\mathbb{Q})$-action is, and (iii) tells us that this is bounded by the corestriction Selmer group which we have shown to be typically rather small. This leads to Corollary 1.4.3 which shows that for a general quadratic field K, the proportion of $E/\mathbb{Q}$ for which $\mathrm{Sel}_2(E/K)$ is acted on nontrivially by $\mathrm{Gal}(K/\mathbb{Q})$ is very small.

We finally obtain Theorem 1.4.4 from the fixed space result, since the average size of the corestriction Selmer group (which controls the nontrivial action not accounted for by that result) is small.

§ 1.6 | Notation and Conventions

We begin my fixing certain objects and notations, to allow for ease of exposition.

Galois Modules

For a field F of characteristic 0, we write $\overline{F}$ for a (fixed once and for all) algebraic closure of F, and denote its absolute Galois group by $G_F = \mathrm{Gal}(\overline{F}/F)$. By a G_F-module M we mean a discrete abelian group M on which G_F acts continuously, and for each $i \geq 0$ we write $H^i(F, M)$ as a shorthand for the continuous cohomology groups $H^i(G_F, M)$. If moreover M is p-torsion for some prime number p then we say that M is an $\mathbb{F}_p[G_F]$-module, and for $V \subseteq H^i(F, M)$ we write $\dim V$ for the $\mathbb{F}_p$-dimension of V. For such M, we define the *dual* of M to be

$$M^* := \mathrm{Hom}(M, \boldsymbol{\mu}_p),$$

where $\boldsymbol{\mu}_p$ is the G_F-module of p^{th} roots of unity in $\overline{F}$. This is an $\mathbb{F}_p[G_F]$-module with action given as follows: for $\sigma \in G_F$, $\phi \in M^*$ and $m \in M$,

$$^{\sigma}\phi(m) = \sigma\phi(\sigma^{-1}m).$$

For $i \geq 0$, if L/F is a finite extension we denote the corresponding restriction and corestriction maps by

$$\mathrm{res}_{L/F} : H^i(F, M) \to H^i(L, M)$$

and

$$\mathrm{cor}_{L/F} : H^i(L, M) \to H^i(F, M),$$

respectively.

Moreover, if M is a G_F-module and L/F is a finite Galois extension then there is a natural action of $\mathrm{Gal}(L/F)$ on the cohomology groups (for $i \geq 0$) $H^i(L, M)$. For $i = 0$ this is given by the usual action of G_F on M^{G_L}, which factors through $G_F/G_L \cong \mathrm{Gal}(L/F)$. For $i \geq 1$, for each cocycle class $[f] \in H^i(L, M)$ represented by a continuous cocycle $f : G_L^i \to M$, an element $\sigma \in G_F$ acts via $\sigma \cdot [f] = [\sigma \cdot f]$ where for $(\tau_1, \ldots, \tau_i) \in G_L^i$

$$\sigma \cdot f(\tau_1, \ldots, \tau_i) = \sigma f(\sigma^{-1}\tau_1\sigma, \ldots, \sigma^{-1}\tau_i\sigma).$$

Number Fields

For a number field F, we write Ω_F for the set of places of F and for each $v \in \Omega_F$ we write F_v for the completion of F at v. For each $v \in \Omega_F$ we fix (once and for all) an embedding $\overline{F} \hookrightarrow \overline{F}_v$, and so an inclusion $G_{F_v} \subseteq G_F$. Thus each G_F-module M is naturally a G_{F_v}-module and moreover when v is non-archimedean (finite), we denote by F_v^{nr} the maximal unramified extension of F_v, and write

$$H^1_{\mathrm{nr}}(F_v, M) = \ker\left(H^1(F_v, M) \xrightarrow{\mathrm{res}} H^1(F_v^{\mathrm{nr}}, M)\right)$$

for the subgroup of unramified classes. We write $\mathcal{O}_F$ for the ring of integers of F.

Elliptic Curves

For a number field F, an elliptic curve E/F and a finite place $v \in \Omega_F$, when we describe the reduction type of E at v are implicitly referring to the type of E in the Kodaira–Néron classification (see e.g. [Sil94, IV Theorem 8.2]).

We will often identify E with the set of points $E(\overline{F})$, and when describing Galois module structure this will always be the notation. Moreover, for each positive integer n, we write $E[n]$ for the n–torsion subgroup of E.

If F is a non-archimedean local field, and E/F an elliptic curve, then we write $c(E/F)$ for the associated Tamagawa number.

Quadratic twists

For a field F of characteristic 0, and for an element d of $F^\times/F^{\times 2}$, we write χ_d for the associated quadratic character. Thus χ_d is the function from G_F to $\{\pm 1\}$ defined by, for $\sigma \in G_F$, the formula

$$\chi_d(\sigma) = \sigma(\sqrt{d})/\sqrt{d}.$$

Given an abelian variety A over F we write A_d for the quadratic twist of A by d. That is, A_d is an abelian variety over F, equipped with an $\overline{F}$-isomorphism

$$\psi_d \colon A \xrightarrow{\sim} A_d \tag{1.10}$$

such that for all σ in G_F, $\psi_d^{-1}\psi_d^{\sigma}$ is multiplication by $\chi_d(\sigma)$ on A. In particular, A is isomorphic to A_d over $F(\sqrt{d})$.

Arithmetic Functions

By an arithmetic function, we will mean a function $f : \mathbb{Z}\backslash\{0\} \to \mathbb{C}$ such that for each $n \in \mathbb{Z}$ we have $f(-n) = f(n)$. We denote by μ the Möbius function and by gcd the greatest common divisor function, each extended from $\mathbb{Z}_{>0}$ to $\mathbb{Z}\backslash\{0\}$ by composition with the archimedean absolute value. For arithmetic functions f and g, we denote by $f * g$ the Dirichlet convolution of the two, i.e. for each $n \in \mathbb{Z}\backslash\{0\}$

$$(f * g)(n) := \sum_{d|n} f(d)g(n/d),$$

where the sum is over positive divisors of n. We say that an arithmetic function f is multiplicative if for coprime integers $m, n \in \mathbb{Z}\backslash 0$ we have that $f(mn) = f(m)f(n)$.

For each prime number ℓ we write v_ℓ for the normalised valuation on $\mathbb{Q}_\ell$, i.e. the unique valuation such that $v_\ell(\ell) = 1$.

General Conventions

We write $\emptyset$ for the empty set, and define $\max \emptyset$ to be 0, so that max is now defined on every finite set of real numbers.

Frequently Used Notation

We provide below a table for frequently used notation not mentioned above, indicating where it is first defined for the readers convenience.

Notation	Meaning	Location
$\mathcal{E}$	Family of all elliptic curves over $\mathbb{Q}$	Notation 1.1.5
$E_{A,B}$	Elliptic curve corresponding to $(A,B) \in \mathcal{E}$	Notation 1.1.5
E_d	Quadratic Twist of E by d	Definition 1.1.1
$\mathscr{C}(K)$, $\mathscr{C}(K/F;E)$	Corestriction Selmer structure	Definition 2.2.1
$\mathscr{F}(K)$, $\mathscr{F}(K/F;E)$	Restriction Selmer structure	Definition 2.2.1
$\mathscr{C}(K)_v$, $\mathscr{F}(K)_v$	Local groups at v for $\mathscr{C}(K)$ and $\mathscr{F}(K)$	Definition 2.2.1
$\mathrm{Sel}_{\mathscr{C}(K)}$, $\mathrm{Sel}_{\mathscr{F}(K)}$	Selmer groups for $\mathscr{C}(K)$ and $\mathscr{F}(K)$	Definition 2.1.3
$\omega_F(n)$	Number of distinct primes of F dividing $n\mathcal{O}_F$	Definition 1.3.4
Δ_E	Discriminant of a fixed model of elliptic curve E	§3.1
$g_p(K/F;E)$	Genus theory part of $\mathrm{Sel}_p(E/K)$	Definition 2.2.8
$\mathcal{T}(K/F;E)$	Tamagawa Ratio	Definition 3.2.1
$\iota_v(K/\mathbb{Q};E)$	Norm index modulo 2 for E at v from K	Notation 6.0.1
$\iota_v^{\mathrm{mult}}(K/\mathbb{Q};A,B)$	$\iota_v(K/\mathbb{Q};E_{A,B})$ for twisted multiplicative reduction	Notation 6.3.5
$\iota_v^{\mathrm{add}}(K/\mathbb{Q};A,B)$	$\iota_v(K/\mathbb{Q};E_{A,B})$ for other reduction types	Notation 6.2.6
$\mathcal{G}_K(v)$	Average of $\iota_v(K/\mathbb{Q};E)$ over $\mathcal{E}$	Definition 6.5.1
$\mathcal{G}_K^{\mathrm{mult}}(v)$	Average of $\iota_v^{\mathrm{mult}}(K/\mathbb{Q};A,B)$ over $\mathcal{E}$	Notation 6.3.1
$\mathcal{G}_K^{\mathrm{add}}(v)$	Average of $\iota_v^{\mathrm{add}}(K/\mathbb{Q};A,B)$ over $\mathcal{E}$	Notation 6.2.1
$\mathbb{E}_\ell$	ℓ-adic average	Notation 6.1.7
M_ψ	Level for the function ψ	Notation 6.1.7
$\mathcal{E}_\ell$	minimal models for elliptic curves over $\mathbb{Q}_\ell$	Notation 6.1.7
α	Local constant	Definition 6.1.9
$\mathbf{M}_\alpha, C_\alpha, \Sigma_\alpha$	Level, bound and exceptional primes for α	Definition 6.1.9
$\mathcal{F}$	Large family of elliptic curves	Definition 7.4.7
$\mathrm{Inv}(\mathcal{F})$, $\mathrm{Inv}_v(\mathcal{F})$	Invariants of large family	Notation 7.4.5
V_R	Binary quartic forms with coefficients in R	Notation 7.2.1
$H'(E)$	Naive height of E	Definition 7.4.1
$H(f)$	Height of binary quartic form f	Definition 7.4.9
$L_v(\mathscr{C}(K))$	Factor for average size of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q},E[2])$ over $\mathcal{E}$	Definition 7.7.12

Table 1.1: Frequently used notation

Part I

Algebraic Results

Chapter 2

Selmer Groups

The core algebraic objects of this thesis are Selmer structures. These are natural generalisations of the data used to construct the usual n-Selmer groups of elliptic curves, and come with associated Selmer groups. One way to think of n-Selmer groups is that they consist of cohomology classes which 'arise from points everywhere locally'; in much the same way, Selmer structures prescribe local conditions (such as arising from points on the curve) and their associated Selmer groups are made up of cohomology classes which obey these prescribed conditions. These are introduced in §2.1, which is background for the chapter.

In §2.2 we define the (co-)restriction Selmer structures, some novel Selmer structures which generalise and reformulate an earlier construction of Kramer [Kra81], which we show to capture certain representation-theoretic invariants of p-Selmer groups. These results will then be applied later in the thesis in Parts II and III to reduce studying the statistical behaviour of these representation-theoretic invariants to a study of certain Selmer structures and associated data. We are able to produce our strongest results for 2-Selmer groups over multiquadratic extensions, which we do in §2.3. We provide an alternative description of the corestriction Selmer groups in this setting, in terms of the usual Selmer groups of elliptic curves and of their quadratic twists.

For the duration of this chapter we let F be a number field, K/F be a finite Galois extension and $G := \mathrm{Gal}(K/F)$ be its Galois group. The material in §2.2 and §2.3 is original work of the author or joint work with Adam Morgan (and we note clearly when the latter is the case), unless clearly noted otherwise.

§ 2.1 | Selmer Structures

We will now review the properties of Selmer structures and their associated Selmer groups. More details on Selmer structures can be found in [Was97a, MR04] and the references therein. Throughout this section, let p be any prime number.

For each place $v \in \Omega_F$ and every $\mathbb{F}_p[G_F]$–module M, we have the *local Tate pairing*

$$\langle\ ,\ \rangle_v : H^1(F_v, M) \times H^1(F_v, M^*) \longrightarrow H^2(F_v, \boldsymbol{\mu}_p) = \mathrm{Br}(F_v)[p] \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

given by the composition of cup-product and the local invariant map.

Theorem 2.1.1 (Tate local duality)**.** *For each place v of F and every $\mathbb{F}_p[G_F]$–module M, the pairing $\langle\ ,\ \rangle_v$ is non-degenerate. Moreover, for each non-archimedean place $v \nmid p$ such that the inertia group I_{F_v} acts trivially on M, $H^1_{\mathrm{nr}}(F_v, M)$ and $H^1_{\mathrm{nr}}(F_v, M^*)$ are orthogonal complements under this pairing.*

Proof. See [NSW08, Corollary 7.2.6] for non-archimedean v and op. cit. Theorem 7.2.17 for archimedean v. The claim about the unramified subspaces is op. cit. Theorem 7.2.15. □

Example 2.1.2. *Let $p = 2$, and consider $M = \boldsymbol{\mu}_2$, which is self-dual. For each place v of F, Kummer theory gives a canonical isomorphism $H^1(F_v, \boldsymbol{\mu}_2) \cong F_v^\times / F_v^{\times 2}$ (and we have the corresponding isomorphism globally also). For any non-archimedean place $v \nmid 2$ of F we have*

$$H^1_{\mathrm{nr}}(F_v, \boldsymbol{\mu}_2) = \mathcal{O}_{F_v}^\times / \mathcal{O}_{F_v}^{\times 2} \subseteq F_v^\times / F_v^{\times 2}.$$

The local Tate pairing

$$F_v^\times / F_v^{\times 2} \times F_v^\times / F_v^{\times 2} \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is the Hilbert symbol $(x, y) \mapsto (x, y)_v \in \{\pm 1\} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ (see e.g.[Har20, Example 9.11]*).*

We are now ready to define a central concept to the work in this thesis.

Definition 2.1.3. A *Selmer structure* $\mathscr{L} = \{\mathscr{L}_v\}_v$ for a finite $\mathbb{F}_p[G_F]$-module M is a collection of subgroups

$$\mathscr{L}_v \subseteq H^1(F_v, M),$$

one for each $v \in \Omega_F$, such that $\mathscr{L}_v = H^1_{\mathrm{nr}}(F_v, M)$ for all but finitely many v. The associated *Selmer group* $\mathrm{Sel}_{\mathscr{L}}(F, M)$ is defined by the exactness of the sequence

$$0 \to \mathrm{Sel}_{\mathscr{L}}(F, M) \to H^1(F, M) \to \prod_{v \in \Omega_F} H^1(F_v, M)/\mathscr{L}_v.$$

For each $v \in \Omega_F$ we write $\mathscr{L}_v^*$ for the orthogonal complement of $\mathscr{L}_v$ with respect to the local Tate pairing, so that $\mathscr{L}_v^* \subseteq H^1(F_v, M^*)$. We then define the *dual Selmer structure* $\mathscr{L}^*$ for M^* by taking $\mathscr{L}^* = \{\mathscr{L}_v^*\}$, and refer to $\mathrm{Sel}_{\mathscr{L}^*}(F, M^*)$ as the *dual Selmer group*.

The following theorem describes the difference in dimension between a Selmer group and its dual.

Theorem 2.1.4 (Greenberg–Wiles)**.** *Let $\mathscr{L} = \{\mathscr{L}_v\}_v$ be a Selmer structure for a finite $\mathbb{F}_p[G_F]$-module M. Then we have*

$$\begin{aligned}&\dim \mathrm{Sel}_{\mathscr{L}}(F, M) - \dim \mathrm{Sel}_{\mathscr{L}^*}(F, M^*) \\ &\quad = \dim M^{G_F} - \dim (M^*)^{G_F} + \sum_{v \in \Omega_F} (\dim \mathscr{L}_v - \dim M^{G_{F_v}}).\end{aligned}$$

Proof. This is [Wil95, Prop 5.1(b)]. See also [Was97a, Theorem 2]. □

Remark 2.1.5. Note that if E/F is an elliptic curve, then $E[p]$ is naturally an $\mathbb{F}_p[G_F]$-module and the Weil pairing induces an $\mathbb{F}_p[G_F]$-isomorphism $E[p] \cong E[p]^*$. Making this identification, the local Tate pairing at a place $v \in \Omega_F$ becomes an alternating bilinear pairing on $H^1(F_v, E[p])$, and the two global terms on the right hand side of Theorem 2.1.4 cancel.

As an example, we recall the usual p-Selmer groups of elliptic curves in the language of Selmer structures.

Definition 2.1.6. For each finite extension L/F, every place $v \in \Omega_L$, and each elliptic curve E/L_v, we denote by $\mathscr{S}_v(L;E)$ the image of the coboundary map

$$\delta_v : E(L_v)/pE(L_v) \hookrightarrow H^1(L_v, E[p]),$$

arising from the short exact sequence of G_{L_v}-modules

$$0 \longrightarrow E[p] \longrightarrow E \xrightarrow{p} E \longrightarrow 0. \tag{2.1}$$

Note that if E is in fact defined over L then these local groups form a Selmer structure $\mathscr{S}(L) = \mathscr{S}(L;E) = \{\mathscr{S}_v(L;E)\}_v$. Note that the associated Selmer group is $\mathrm{Sel}_{\mathscr{S}(L)}(L, E[p]) = \mathrm{Sel}_p(E/L)$, the classical p-Selmer group. We will often refer to the local groups $\mathscr{S}_v(L;E)$ as Kummer images.

§ 2.2 | The (Co-)Restriction Selmer Structures

We now introduce the novel Selmer structures with which we will most often be occupied, and explain some elementary properties. As in the previous section, let p be a prime number. In the case that $p = 2$, this can be found in earlier work of Kramer [Kra81], see also the work of the author with Adam Morgan [MP22] where we rephrase this case from Kramer in the language of Selmer groups. The general case is work of the author [Pat21].

§ 2.2.1 | Definitions of the (Co-)Restriction Selmer Structures

Definition 2.2.1. For each elliptic curve E/F, each place $v \in \Omega_F$ and any $w \in \Omega_K$ extending v, let

$$\mathscr{F}_v(K/F;E) := \mathrm{res}^{-1}_{K_w/F_v}(\mathscr{S}_w(K;E)) \leq H^1(F_v, E[p]).$$

Note that the definition does not depend on the choice of w as our extension is Galois. We then have a Selmer structure $\mathscr{F}(K) = \mathscr{F}(K/F;E) = \{\mathscr{F}_v(K/F;E)\}_v$ for $E[p]$ over F, and call this the restriction Selmer structure. We further define the Selmer structure $\mathscr{C}(K) = \mathscr{C}(K/F;E)$ for $E[p]$ to be the dual of $\mathscr{F}(K)$, denote the corresponding local groups by $\mathscr{C}_v(K/F;E)$, and call this (for reasons to be revealed shortly) the corestriction Selmer structure.

Of course, we ought to justify our assertion that these local groups do, in fact, define Selmer structures. Before doing so, we provide a useful alternative description of the corestriction Selmer structure, justifying its name.

Lemma 2.2.2. *For every $v \in \Omega_F$, every elliptic curve E/F_v and every place $w \in \Omega_K$ extending v, the orthogonal complement (with respect to the local Tate pairing) of the subgroup $\mathrm{res}^{-1}_{K_w/F_v}(\mathscr{S}_v(E;K_w)) \leq H^1(F_v, E[p])$ is precisely $\mathrm{cor}_{K_w/F_v}(\mathscr{S}_v(E;K_w))$.*

In particular, when E is defined over F, we have the identity

$$\mathscr{C}_v(K/F;E) = \mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E)) \leq H^1(F_v, E[p]).$$

Proof. For $v \in \Omega_F$ and $w \in \Omega_K$ extending v, it follows from [Neu13, I.5.4] and [Neu13, II Proposition 1.4(c) and Theorem 5.6] that res_{K_w/F_v} and cor_{K_w/F_v} are adjoints with respect to the local Tate pairings. By [PR12, Proposition 4.10], $\mathscr{S}_v(F;E)$ and $\mathscr{S}_w(K;E)$ are maximal isotropic subspaces of the corresponding cohomology groups with respect to the Tate pairings. Thus we have inclusions

$$\mathrm{cor}_{K_w/F_v}(\mathscr{S}_v(K;E)) \subseteq \left(\mathrm{res}^{-1}_{K_w/F_v}(\mathscr{S}_v(K;E))\right)^*$$

and

$$\mathrm{res}_{K_w/F_v}\left(\mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E))^*\right) \subseteq \mathscr{S}_w(K;E)^* = \mathscr{S}_w(K;E).$$

The result then follows. □

Remark 2.2.3. In the case $p = 2$ this is already noted by Kramer in the paragraph following Equation 10 in [Kra81].

Using this description it is easy to see that these define Selmer structures.

Lemma 2.2.4. *Let E/F be an elliptic curve. Then the collections $\mathscr{C}(K) = \mathscr{C}(K/F;E)$ and $\mathscr{F}(K) = \mathscr{F}(K/F;E)$ in Definition 2.2.1 are Selmer structures.*

Proof. Note that for every $v \in \Omega_F$ and every $w \in \Omega_K$ extending it, by Lemma 2.2.2 and the compatibility of corestriction maps with connecting maps we have that

$$\mathscr{C}_v(K/F;E) = \mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E)) = \delta\left(\frac{N_{K_w/F_v}E(K_w) + pE(F_v)}{pE(F_v)}\right),$$

where $\delta : E(F_v)/pE(F_v) \to H^1(F_v, E[p])$ is the induced map arising from the connecting map from the by multiplication by p short exact sequence for E. By [Maz72, Corollary 4.4], if v is a place of good reduction for E which is unramified in K/F then $N_{K_w/F_v} : E(K_w) \to E(F_v)$ is surjective and so $\mathscr{C}_v(K/F;E) = \mathscr{S}_v(F;E)$. It is then well known that $\mathscr{S}_v(F;E) = H^1_{\mathrm{nr}}(F, E[p])$ so long as we additionally require that $v \nmid p$ (see, e.g. [Sil09]). Thus $\mathscr{C}_v(K/F;E) = H^1_{\mathrm{nr}}(F, E[p])$ for all but finitely many places $v \in \Omega_F$. The same statement holds for $\mathscr{F}_v(K/F;E)$ since it is the dual structure to $\mathscr{C}_v(K/F;E)$ and for all but finitely many $v \in \Omega_F$ the unramified classes $H^1_{\mathrm{nr}}(F_v, E[p])$ are self-dual (see [PR12, Proposition 4.12 via Remark 4.11] for a more general statement). □

§ 2.2.2 | Properties of the (Co-)Restriction Selmer Groups

We now relate the Selmer groups $\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])$ and $\mathrm{Sel}_{\mathscr{C}(K)}(F, E[p])$ to specific representation theoretic invariants of the $\mathbb{F}_p[G]$-module $\mathrm{Sel}_p(E/F)$.

Lemma 2.2.5. *Let E/F be an elliptic curve. We have*

$$\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) = \mathrm{res}_{K/F}^{-1}\left(\mathrm{Sel}_p(E/K)\right).$$

Proof. This follows from the compatibility of local and global restriction maps. □

Lemma 2.2.6. *Let E/F be an elliptic curve. We have*

$$\mathrm{cor}_{K/F}\left(\mathrm{Sel}_p(E/K)\right) \subseteq \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]).$$

Proof. This is immediate from Lemma 2.2.2 □

Lemma 2.2.7. *Let E/F be an elliptic curve, and $N_{K/F} := \sum_{g\in G} g \in \mathbb{Z}[G]$ be the norm element. We have that*

$$\dim\left(N_{K/F}\cdot \mathrm{Sel}_p(E/K)\right) \leq \dim \mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]), \tag{2.2}$$

$$\dim\left(\mathrm{Sel}_p(E/K)^G\right) = \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) - \dim H^1(K/F, E(K)[p]) + \dim(\mathrm{im}(\tau)), \tag{2.3}$$

where $\tau : H^1(K, E[p]) \to H^2(K/F, E(K)[p])$ is the transgression map.

Proof. (2.2) is given by naturality of the corestriction map, which is induced by action of $N_{K/F}$. By Lemma 2.2.5, the inflation-restriction sequence yields an exact sequence

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(K/F, E(K)[p]) & \xrightarrow{\inf} & \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]) & \xrightarrow{\mathrm{res}} & \mathrm{Sel}_p(E/K)^G \\ & & & & & & \downarrow \tau \\ & & & & & & H^2(K/F, E(K)[p]). \end{array}$$

Thus (2.3) holds. □

We now introduce the function that will bound the failure Galois descent in our statistical results.

Definition 2.2.8. We define the genus theory of the p-Selmer group of an elliptic curve E/F arising from the extension K/F to be

$$g_p(K/F; E) := \sum_{v\in\Omega_F} \dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right),$$

where, in each summand, $w \in \Omega_K$ is any place of K extending v.

Remark 2.2.9. This sum is well defined because only finitely many terms are ever nonzero: by [Maz72, Corollary 4.4] the norm map surjects at primes which are both unramified in the extension and of good reduction for the curve.

We now have a simple lemma relating the local terms in the genus theory to the objects we are already studying.

Lemma 2.2.10. *Let $v \in \Omega_F$, E/F_v be an elliptic curve, and choose $w \in \Omega_K$ extending v. Then,*

$$\dim\left(E(F_v)/pE(F_v)\right) = \dim \mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E)) + \dim \frac{E(F_v)}{\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right)}$$

Proof. Note that cor_{K_w/F_v} acts as the norm map N_{K_w/F_v} on points in $E(K_w)$, so, via the second isomorphism theorem,

$$\mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E)) = \left(N_{K_w/F_v}E(K_w) + pE(F_v)\right)/pE(F_v).$$

The claimed formula then follows from the natural short exact sequence

$$0 \longrightarrow \frac{N_{K_w/F_v}E(K_w)+pE(F_v)}{pE(F_v)} \longrightarrow \frac{E(F_v)}{pE(F_v)} \longrightarrow \frac{E(F_v)}{\left(N_{K_w/F_v}E(K_w)+pE(F_v)\right)} \longrightarrow 0\ .$$

□

This, along with the Greenberg-Wiles theorem, then tells us the following.

Lemma 2.2.11. *Let E/F be an elliptic curve. Then*

$$\dim \mathrm{Sel}_{\mathscr{F}(K)}(F,E[p]) - \dim \mathrm{Sel}_{\mathscr{C}(K)}(F,E[p]) = g_p(K/F;E),$$

and moreover,

$$0 \leq \dim \mathrm{Sel}_{\mathscr{F}(K)}(F,E[p]) - \dim \mathrm{Sel}_p(E/F) \leq g_p(K/F;E).$$

Proof. For each $v \in \Omega_F$, the groups $\mathscr{C}_v = \mathscr{C}_v(K/F;E)$ and $\mathscr{F}_v = \mathscr{F}_v(K/F;E)$ are orthogonal complements under the local Tate pairing. We therefore have $\dim \mathscr{F}_v = \dim H^1(F_v,E[p]) - \dim \mathscr{C}_v$. Moreover, since $\mathscr{S}_v(F;E)$ is maximal isotropic, we have $\dim H^1(F_v,E[p])$ is equal to $2\dim E(F_v)/pE(F_v)$. Combining this with Lemma 2.2.2 and Lemma 2.2.10, we obtain

$$\begin{aligned}\dim \mathscr{F}_v &= 2\dim E(F_v)/pE(F_v) - \dim \mathscr{C}_v \\ &= \dim E(F_v)/pE(F_v) + \dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right).\end{aligned}$$

It then follows from Theorem 2.1.4 that

$$\begin{aligned}\dim \mathrm{Sel}_{\mathscr{F}(K)}(F,E[p]) - \dim \mathrm{Sel}_{\mathscr{C}(K)}(F,E[p]) =& \sum_{v\in\Omega_F} \dim\left(\frac{E(F_v)}{N_{K_w/F_v}E(K_w)+pE(F_v)}\right) \\ &+ \sum_{v\in\Omega_F}\left(\dim\frac{E(F_v)}{pE(F_v)} - \dim E(F_v)[p]\right) \\ =& g_p(K/F;E),\end{aligned}$$

where the last equality is obtained by applying Theorem 2.1.4 to the self-dual Selmer structure $\mathscr{S}(E/F)$, so the first equation in the lemma statement holds.

The second equation follows from the inclusions

$$\mathrm{Sel}_{\mathscr{C}(K)}(F, E[p]) \subseteq \mathrm{Sel}_p(E/F) \subseteq \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p]), \tag{2.4}$$

and so the result holds. □

§ 2.2.3 | A Useful Lemma for p-Extensions

Here we provide a useful lemma for bounding the behaviour of $\mathrm{Sel}_p(E/K)$ using only $\mathrm{Sel}_p(E/K)^G$ when G is a p-group. Firstly, however, we will require the classification of finite dimensional $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-modules.

Lemma 2.2.12. *Assume that G is a cyclic group of order p. The isomorphism classes of finitely generated indecomposable $\mathbb{F}_p[G]$-modules are represented precisely by $\{M_k\}_{k=1}^p$, where M_1 is the 1-dimensional vector space $\mathbb{F}_p$ with trivial G-action and M_k is a non-split extension of M_{k-1} by M_1. Moreover, every $\mathbb{F}_p[G]$-module is isomorphic to a unique direct sum of these indecomposable modules.*

Proof. By the orbit-stabiliser theorem we have that there is precisely one simple $\mathbb{F}_p[G]$-module, the trivial module M_1. The result then follows from the Krull-Schmidt theorem and the existence of Jordan normal form (see, for example, [Alp86, page 24]). □

We can then use this as a base-case to prove the useful bound.

Lemma 2.2.13. *Assume that G is a p-group, then for every finite dimensional $\mathbb{F}_p[G]$-module M we have an inequality*

$$\dim M \leq (\#G) \cdot \dim M^G.$$

Proof. The case $\#G = 1$ is trivial. Moreover the case $\#G = p$ is immediate from Lemma 2.2.12: decompose M as a sum of indecomposable $\mathbb{F}_p[\mathbb{Z}/p\mathbb{Z}]$-modules and then note that each such module has a 1-dimensional fixed space and dimension at most $p = \#G$.

In general, if $\#G = p^k$ for some $k \geq 1$, then by the Jordan–Hölder theorem we can select a chain of (maximal) normal subgroups

$$0 = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$$

where each successive quotient satisfies $G_{i+1}/G_i \cong \mathbb{Z}/p\mathbb{Z}$. Now for each $0 \leq i \leq k-1$ we note that M^{G_i} is a finite dimensional $\mathbb{F}_p[G_{i+1}/G_i]$-module and so by the case $k = 1$ above satisfies

$$\dim M^{G_i} \leq p \dim (M^{G_i})^{G_{i+1}} = p \dim M^{G_{i+1}}.$$

Then since $M^{G_0} = M$ and $M^{G_k} = M^G$ we have the result. □

§ 2.3 | (Co-)Restriction Selmer Structures for $p = 2$

We now consider a special case for the Selmer structures of §2.2: when $p = 2$. This case is rather special in that the quadratic twists of a fixed elliptic curve E/F all have isomorphic 2-torsion (as G_F–modules). In this section we maintain the notation of the previous section, but restrict to the case $p = 2$. The subsections §2.3.1, §2.3.2, and §2.3.3 consist of original work of the author unless otherwise stated. The subsection §2.3.4 consists of joint work with Adam Morgan.

We firstly explicate the isomorphism between the 2-torsion modules of quadratic twists. Let L be a characteristic 0 field, and E/L be an elliptic curve. Recall that for each $\theta \in L^\times/L^{\times 2}$ there is an $L(\sqrt{\theta})$ isomorphism $E_\theta \cong E$, where the former is the quadratic twist of E by θ. Explicitly, if we are given Weierstrass equations

$$E : y^2 = x^3 + Ax + B$$
$$E_\theta : \theta y^2 = x^3 + Ax + B$$

then the map is

$$E_\theta \to E$$
$$(x, y) \mapsto (x, \sqrt{\theta} y)$$

If θ is not the trivial class, then clearly this isomorphism maps the points of $E_\theta(L)$ exactly to those of $E(L(\sqrt{\theta}))$ which are acted on by -1 by $\mathrm{Gal}(L(\sqrt{\theta})/L)$, and so in particular it restricts to an isomorphism of G_L-modules $\varphi_\theta : E_\theta[2] \cong E[2]$.

§ 2.3.1 | Twisted Kummer Images

The map φ_θ gives rise to various twisted Kummer images locally, which will turn out to define a Selmer structure and will turn out to be related to our (co-)restriction Selmer groups in the previous section.

Definition 2.3.1. For each place v of F, each elliptic curve E/F_v and each $\theta \in F_v^\times/F_v^{\times 2}$, we write $\mathscr{S}_v^{(\theta)}(F; E)$ for the associated twisted Kummer image. That is, the image of

$$E_\theta(F_v)/2E_\theta(F_v) \xrightarrow{\delta_\theta} H^1(F_v, E_\theta[2]) \xrightarrow[\sim]{(\varphi_\theta)^*} H^1(F_v, E[2]),$$

where δ_θ is the usual connecting map from the short exact sequence induced by multiplication by 2 on E_θ. When θ is the trivial class, we will abbreviate $\mathscr{S}_v(F; E) := \mathscr{S}_v^{(1)}(F; E)$, since these groups are precisely those in Definition 2.1.6.

With respect to Tate local duality, these local groups are self-dual.

Lemma 2.3.2. *For every place v of F, each elliptic curve E/F_v and each $\theta \in F_v^\times/F_v^{\times 2}$, the twisted Kummer image $\mathscr{S}_v^{(\theta)}(F; E) \subseteq H^1(F_v, E[2])$ is self-dual with respect to the local Tate pairing.*

Proof. Note that since φ_θ is an $F_v(\sqrt{\theta})$-isomorphism, the Weil pairing on $E_\theta[2]$ is preserved by φ_θ and so this follows from the case when θ is the trivial class which, in turn, follows from Tate Duality [Tat63, Theorem 2.3]. □

We now note that these local groups do, in fact, define Selmer structures.

Proposition 2.3.3. *For every elliptic curve E/F and each element $\theta \in F^\times/F^{\times 2}$, the collection $\mathscr{S}^{(\theta)}(F;E) := \left\{\mathscr{S}_v^{(\theta)}(F;E)\right\}_{v\in\Omega_F}$ defines a Selmer structure for $E[2]$.*

Proof. The only thing which needs to be checked is that for all but finitely many $v \in \Omega_F$, we have an equality $\mathscr{S}_v^{(\theta)}(F;E) = H^1_{\mathrm{nr}}(F_v, E[2])$.

Firstly, (see e.g. [Sil09]) for all but finitely many $v \in \Omega_F$ we have two equalities

$$\mathscr{S}_v(F;E) = H^1_{\mathrm{nr}}(F_v, E[2]), \qquad \mathscr{S}_v^{(\theta)}(F;E) = \varphi_\theta^*\left(H^1_{\mathrm{nr}}(F_v, E_\theta[2])\right).$$

Assume that v is such a place. Compatibility of restriction maps shows that

$$\varphi_\theta^*\left(H^1_{\mathrm{nr}}(F_v, E_\theta[2])\right) \subseteq H^1_{\mathrm{nr}}(F_v, E[2]).$$

Since both $H^1_{\mathrm{nr}}(F_v, E[2])$ and $H^1_{\mathrm{nr}}(F_v, E_\theta[2])$ are self-dual with respect to the (alternating) local Tate pairings in $H^1(F_v, E[2])$ and $H^1(F_v, E_\theta[2])$ respectively, we have that their dimensions are half of those of the total spaces which are in turn isomorphic. Thus, since the two spaces of unramified classes have the same dimension, and φ_θ^* is injective and maps one into the other, we must have that in fact $\mathscr{S}_v(K/F;E) = \mathscr{S}_v(K/F;E) = H^1_{\mathrm{nr}}(F_v, E[2])$ for such v. □

§ 2.3.2 | Multiquadratic Extensions: Local Theory

We now study some useful properties of the (co-)restriction Selmer groups in the situation that $p = 2$ and K/F is a multiquadratic extension. We will relate the local groups to twisted Kummer images, which will later enable us to study the statistics of these via Bhargavology.

Thus **for the duration of this subsection only** we take the following notation

Notation 2.3.4. Let $v \in \Omega_F$, and assume that $w \in \Omega_K$ is a place extending v such that K_w/F_v is multiquadratic. Let E/F_v be an elliptic curve with a fixed Weierstrass equation

$$E : y^2 = f(x),$$

whose discriminant we denote by Δ_E.

We now prove some useful lemmata, before going on to provide the main proposition for this subsection.

Lemma 2.3.5. *Write $G_v := \mathrm{Gal}(K_w/F_v)$. Then exactly one of the following holds.*

1. $E(K_w)[2] = E(F_v)[2]$.

2. $\Delta_E \in K_w^{\times 2} \backslash F_v^{\times 2}$ *and, writing* $H_v = \mathrm{Gal}(K_w/F_v(\sqrt{\Delta_E}))$*, there is an isomorphism of* $\mathbb{F}_2[G_v]$*–modules* $E(K_w)[2] \cong_{\mathbb{F}_2[G_v]} \mathbb{F}_2[G_v/H_v]$.

Proof. The nontrivial 2-torsion points on E over the algebraic closure are precisely the points which have x-coordinates which are roots of the cubic polynomial $f(x)$. In particular, the only situation in which $E(F_v)[2] \neq E(K_w)[2]$ must be when $\dim_{\mathbb{F}_2} E(F_v)[2] = 1$ and $\dim_{\mathbb{F}_2} E(K_w)[2] = 2$. In this latter case, the extra 2-torsion point is obtained over the quadratic extension $F_v(\sqrt{\Delta_E})$. Then G_v acts on $E(K_w)[2]$ via the quotient G_v/H_v, and this module must be 2-dimensional with a 1-dimensional fixed space and so (by e.g. [Alp86, page 24]) there is precisely one isomorphism class of module to which it can belong: that of $\mathbb{F}_2[G_v/H_v]$. □

Lemma 2.3.6. *Let* $r \in \mathbb{Z}_{\geq 1}$ *be such that* K_w/F_v *has degree* 2^r*, and say* $K_w = F_v(\sqrt{\theta_1}, \ldots, \sqrt{\theta_r})$*. If* $F_v(\sqrt{\Delta_E})/F_v$ *is a quadratic extension contained in* K*, then additionally fix* $\theta_1 = \Delta_E$*. Writing* $K_{w,i} := F_v(\sqrt{\theta_i})$*, we have that*

$$H^1(K_w/F_v, E(K)[2]) = \oplus_{i=1}^r \inf_i \left(H^1\left(K_{w,i}/F_v, E(K_i)[2]\right)\right)$$

where the direct sum here is the internal sum of $\mathbb{F}_2$*-vector spaces, and*

$$\inf_i : H^1(K_{w,i}/F_v, E(K_{w,i})[2]) \to H^1(K_w/F_v, E(K_w)[2])$$

denotes the usual inflation map from $K_{w,i}$ *to* K_w.

Proof. If $E(F_v)[2] = E(K_w)[2]$ then the $\mathrm{Gal}(K_w/F_v)$ action is trivial on $E(K_w)[2]$, and so the cohomology groups in the statement are just $\mathrm{Hom}(\mathrm{Gal}(K_w/F_v), E(K_w)[2])$ and similarly for the $K_{w,i}$. Moreover the inflation maps are simply given by extension of homomorphisms, and so the result is clear.

By Lemma 2.3.5, it remains to consider the case that $\Delta_E \in K_w^{\times 2} \backslash F_v^{\times 2}$ and $E(K_w)[2] \cong_{\mathbb{F}_2[G_v]} \mathbb{F}_2[G_v/H_v]$ where

$$G_v := \mathrm{Gal}(K_w/F_v) \geq \mathrm{Gal}(K_w/K_{w,1}) = \mathrm{Gal}\left(K_w/F_v(\sqrt{\Delta_E})\right) =: H_v.$$

In this case we have a commutative diagram for each $2 \leq i \leq r$

$$\begin{array}{ccc} H^1(K_w/F_v,\ E(K_w)[2]) & \xrightarrow{\sim} & H^1(K_w/K_{w,1},\ \mathbb{F}_2) \\ {\scriptstyle \inf_i}\uparrow & & {\scriptstyle \inf_i}\uparrow \\ H^1(K_{w,i}/F_v,\ E(K_{w,i})[2]) & \xrightarrow{\sim} & H^1(K_{w,i} \cdot K_{w,1}/K_{w,1},\ \mathbb{F}_2), \end{array}$$

where the vertical maps are the natural inflation maps, the lower horizontal is induced by the natural isomorphism $\mathrm{Gal}(K_{w,i} \cdot K_{w,1}/K_{w,1}) \cong \mathrm{Gal}(K_{w,i}/F_v)$ and the fact that $E(K_{w,i})[2] = E(F_v)[2] \cong \mathbb{F}_2$, and the top horizontal is the isomorphism of Shapiro's lemma (as in, for example, [Neu13, Theorem 4.19]). That this diagram commutes is

clear from the definitions of the maps. Clearly (as in the previous case), we have

$$H^1(K_w/K_{w,1},\ \mathbb{F}_2) = \oplus_{i=2}^{r} \inf_i \left(H^1(K_{w,i} \cdot K_{w,1}/K_{w,1},\ \mathbb{F}_2) \right),$$

since both are just groups of homomorphisms, and so in particular by the diagram above

$$H^1(K_w/F_v,\ E(K_w)[2]) \cong \oplus_{i=2}^{r} \inf_i \left(H^1(K_{w,i}/F_v,\ E(K_{w,i})[2]) \right).$$

Noting that $E(K_w)[2] \cong_{\mathbb{F}_2[G_v]} \mathbb{F}_2[G_v/H_v]$ we have from Shapiro's Lemma that

$$H^1(K_{w,1}/F_v, E(K_{w,1})[2]) = 0,$$

and so the result follows.

□

Lemma 2.3.7. *Let $\delta : E(K_w) \to H^1(K_w, E[2])$ be the connecting map arising from the multiplication by 2 exact sequence on E, and write $S := \ker(F_v^\times/F_v^{\times 2} \to K_w^\times/K_w^{\times 2})$. For every point $P \in E(K_w)$ such that $\delta(P) \in \mathrm{im}(\mathrm{res}_{K_w/F_v} : H^1(F_v, E[2]) \to H^1(K_w, E[2]))$, there are points $(P_\theta) \in \prod_{\theta \in S} E_\theta(F_v)$ such that*

$$P = \sum_{\theta \in S} \varphi_\theta(P_\theta)$$

Proof. We will prove this by induction on $r = \dim_{\mathbb{F}_2} \mathrm{Gal}(K_w/F_v)$. If $r = 0$ then the claim is trivial. Assuming that $r > 0$, let M be an intermediate field such that $[K_w : M] = 2$ and write $K_w = M(\sqrt{\theta})$ for some $\theta \in S$. Let $x \in H^1(F_v, E[2])$ be such that $\delta(P) = \mathrm{res}_{K_w/F_v}(x)$. Observe that the commutative diagram

$$\begin{array}{ccc} E(K_w) & \xrightarrow{\delta} & H^1(K_w, E[2]) \\ \downarrow{\scriptstyle N_{K_w/M}} & & \downarrow{\scriptstyle \mathrm{cor}_{K_w/M}} \\ E(M) & \xrightarrow{\delta} & H^1(M, E[2]), \end{array}$$

shows that

$$\delta(N_{K_w/M}(P)) = \mathrm{cor}_{K_w/M} \circ \mathrm{res}_{K_w/M} \circ \mathrm{res}_{M/F_v}(x) = 2\mathrm{res}_{M/F_v}(x).$$

Since $H^1(M, E[2])$ is a 2-torsion group we have that $N_{K_w/M}(P) \in \ker(\delta) = 2E(M)$, so let $Q \in E(M)$ be a point such that $2Q = N_{K_w/M}(P)$. Let $R := P - Q$, and let $\sigma \in \mathrm{Gal}(K_w/M)$ be the nontrivial element, and observe that

$$\sigma(R) = \sigma(P) - Q = N_{K_w/M}(P) - P - Q = Q - P = -R.$$

In particular $R = \varphi_\theta(P_\theta)$ for some point $P_\theta \in E_\theta(M)$. Now since P_θ and Q are both points on elliptic curves satisfying the constraints above (and since $\varphi_\theta \circ \varphi_{\theta'} = \varphi_{\theta\theta'}$) but with K_w/F_v replaced by the degree 2^{r-1} extension M/F_v, we conclude the result. □

These lemmata then allow us to prove the following very useful result on the core-

striction and the preimage under restriction of the Kummer image.

Proposition 2.3.8. *Write* $S := \ker(F_v^\times/F_v^{\times 2} \to K_w^\times/K_w^{\times 2})$. *Then we have identities:*

$$\begin{aligned}\mathrm{res}^{-1}_{K_w/F_v}(\mathscr{S}_w(K;E)) &= \sum_{\theta\in S} \mathscr{S}_v^{(\theta)}(F;E),\\ \mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E)) &= \bigcap_{\theta\in S} \mathscr{S}_v^{(\theta)}(F;E).\end{aligned}$$

Proof. To ease notation, we write $\mathscr{F}_v := \mathrm{res}^{-1}_{K_w/F_v}(\mathscr{S}_w(K;E))$ and $\mathscr{C}_v := \mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E))$. Firstly we note that the property for $\mathscr{C}_v$ follows from that of $\mathscr{F}_v$, the fact that these two are dual with respect to the local Tate pairing and that $\mathscr{S}_v^{(\theta)}(F;E)$ is its own orthogonal complement (Lemma 2.3.2). The equality for the Selmer group then follows from the equality for $\mathscr{C}_v$.

It remains to prove the identity for $\mathscr{F}_v$, which we now do. If $\theta \in S$ then it is easy to see that the following diagram commutes:

$$\begin{array}{ccccc} E_\theta(F_v) & \xrightarrow{\delta} & H^1(F_v, E_\theta[2]) & \xrightarrow{\varphi_\theta^*} & H^1(F_v, E[2]) \\ \downarrow{\scriptstyle \varphi_\theta} & & & & \downarrow{\scriptstyle \mathrm{res}_{K_w/F_v}} \\ E(F_v(\sqrt{\theta})) & \longrightarrow & E(K_w) & \xrightarrow{\delta} & H^1(K_w, E[2]), \end{array} \tag{2.5}$$

and so $\mathscr{S}_v^{(\theta)}(F;E) \subseteq \mathscr{F}_v$.

It remains to prove the converse. Let $x \in \mathscr{F}_v$, and choose $P \in E(K_w)$ such that $\delta(P) = \mathrm{res}_{K_w/F_v}(x)$. Note that by Lemma 2.3.7 we can write

$$P = \sum_{\theta\in S} \varphi_\theta(P_\theta)$$

for some points $P_\theta \in E_\theta(F_v)$. Then by commutativity of (2.5) we have

$$\begin{aligned}\mathrm{res}_{K_w/F_v}(x) = \delta(P) &= \sum_{\theta\in S} \delta\circ\varphi_\theta(P_\theta)\\ &= \mathrm{res}_{K_w/F_v}\left(\sum_{\theta\in S} \varphi_\theta^*\circ\delta(P_\theta)\right) \in \mathrm{res}_{K_w/F_v}\left(\sum_{\theta\in S}\mathscr{S}_v^{(\theta)}(F;E)\right).\end{aligned}$$

It is then sufficient to prove that $\ker(\mathrm{res}_{K_w/F_v}) \subseteq \sum_{\theta\in S}\mathscr{S}_v^{\theta}(F;E)$ when K_w/F_v is a multiquadratic local extension, which we now do. Using the inflation-restriction exact sequence, Lemma 2.3.6 and compatibility of inflation maps, there is an equality

$$\begin{aligned}\ker(\mathrm{res}_{K_w/F_v}) &= \mathrm{im}\left(\inf : H^1(K_w/F_v, E(K_w)[2]) \to H^1(F_v, E[2])\right)\\ &= \sum_{\theta\in S} \mathrm{im}\left(\inf : H^1\left(F_v(\sqrt{\theta})/F_v, E(F_v(\sqrt{\theta}))[2]\right) \to H^1\left(F_v, E[2]\right)\right)\\ &= \sum_{\theta\in S} \ker\left(\mathrm{res}_{F_v(\sqrt{\theta})/F_v}\right).\end{aligned}$$

By [Kra81, Lemma 3], for each $\theta \in S$

$$\ker\left(\mathrm{res}_{F_v(\sqrt{\theta}/F_v)}\right) \subseteq \mathscr{S}_v(E) + \mathscr{S}_v^{(\theta)}(E),$$

and so the required result holds. □

§ 2.3.3 | Multiquadratic Extensions: Global Theory

We now aim to use the local results of the previous subsection to describe the corestriction Selmer groups in terms of twisted Kummer images. This will be especially useful when we come to study the statistical behaviour of the corestriction Selmer group for multiquadratic extensions – these twisted Kummer images will turn out to be accessible for statistics.

Proposition 2.3.9. *Assume that K/F is a multiquadratic extension and let E/F be an elliptic curve. Let $v \in \Omega_F$ and $w \in \Omega_K$ be a place extending v, and $S := \ker(F_v^\times/F_v^{\times 2} \to K_w^\times/K_w^{\times 2})$. Then*

$$\mathscr{F}_v(K/F;E) = \sum_{\theta\in S} \mathscr{S}_v^{(\theta)}(F;E),$$
$$\mathscr{C}_v(K/F;E) = \bigcap_{\theta\in S} \mathscr{S}_v^{(\theta)}(F;E).$$

Moreover,

$$\mathrm{Sel}_{\mathscr{C}(K)}(F,E[2]) = \bigcap_{\substack{\theta\in F^\times/F^{\times 2}\\ F(\sqrt{\theta})\subseteq K}} (\varphi_\theta)^*\left(\mathrm{Sel}_2(E_\theta/F)\right)$$

Proof. The first two identities follows from Proposition 2.3.8. The equality for the Selmer group then follows from the equalities for the local groups $\{\mathscr{C}_v(K/F:E)\}_{v\in\Omega_F}$. □

Remark 2.3.10. In the case that K/F is a quadratic extension, Proposition 2.3.9 was shown by Kramer [Kra81, Proposition 7], the novelty here is in proving the local results in the case of multiquadratic extensions.

§ 2.3.4 | Quadratic Extensions

We now restrict further to the case that $p = 2$ and K/F is a quadratic extension. We will describe a strong relationship between the 2-Selmer group of E/K and the (co-)restriction Selmer groups. This section consists of joint work with Adam Morgan (see [MP22])

Lemma 2.3.11. (*cf.* [Kra81, Lemma 3]). *Assume that K/F is a quadratic extension, let $v \in \Omega_F$ and let $w \in \Omega_K$ be a place extending v. We have an exact sequence*

$$0 \to H^1\left(K/F, E(K)[2]\right) \overset{\mathrm{inf}}{\to} \mathrm{Sel}_{\mathscr{F}(K)}(F,E[2]) \overset{\mathrm{res}_{K/F}}{\to} \mathrm{Sel}_2(E/K) \overset{\mathrm{cor}_{K/F}}{\to} \mathrm{Sel}_{\mathscr{C}(K)}(F,E[2]). \tag{2.6}$$

Proof. We first claim that the sequence

$$H^1(F, E[2]) \overset{\mathrm{res}_{K/F}}{\longrightarrow} H^1(K, E[2]) \overset{\mathrm{cor}_{K/F}}{\longrightarrow} H^1(F, E[2])$$

is exact. To see this, consider the exact sequence of G_F–modules

$$0 \longrightarrow \mathbb{F}_2 \longrightarrow \mathbb{F}_2[G] \xrightarrow{\varepsilon} \mathbb{F}_2 \longrightarrow 0,$$

where ε is the augmentation map (sending $\sum_{g\in G} \lambda_g g$ to $\sum_{g\in G} \lambda$) and G_F acts on G via the quotient map $G_F \twoheadrightarrow G$. Taking the tensor product over $\mathbb{F}_2$ with $E[2]$, and then taking Galois cohomology over F, gives an exact sequence of G_F-modules

$$H^1(F, E[2]) \longrightarrow H^1(F, E[2] \otimes_{\mathbb{F}_2} \mathbb{F}_2[G]) \longrightarrow H^1(F, E[2]).$$

Using Shapiro's Lemma to identify $H^1(F, E[2] \otimes_{\mathbb{F}_2} \mathbb{F}_2[G])$ with $H^1(K, E[2])$ yields the sought exact sequence.

Having shown the claim, the result follows by combining the inflation-restriction exact sequence with Lemma 2.2.5 and Lemma 2.2.6. □

Corollary 2.3.12. *Assume that K/F is a quadratic extension. If $\mathrm{Sel}_{\mathscr{C}(K)}(F, E[2]) = 0$, then all of the following hold.*

(i) There is a short exact sequence

$$0 \longrightarrow H^1(K/F, E(K)[2]) \xrightarrow{\mathrm{inf}} \mathrm{Sel}_{\mathscr{F}(K)}(F, E[2]) \overset{\mathrm{res}_{K/F}}{\longrightarrow} \mathrm{Sel}_2(E/K) \longrightarrow 0,$$

where the first map is inflation.

(ii) We have

$$\dim \mathrm{Sel}_2(E/K) = g_2(K/F; E) - \dim\left(\frac{E(F)[2]}{N_{K/F}E(K)[2]}\right).$$

(iii) The G-action on $\mathrm{Sel}_2(E/K)$ is trivial.

Proof. (i): follows immediately from Lemma 2.3.11.

(ii): follows from (i) and Lemma 2.2.11 upon noting that, since $\mathrm{Gal}(K/F)$ is cyclic, we have

$$H^1(K/F, E(K)[2]) \cong \frac{E(F)[2]}{N_{K/F}(E(K))[2]}.$$

(See e.g. [AW67, Section 8] for the description of the cohomology of cyclic groups we are using in the above.)

(iii): follows from (i) and the fact that the image of the restriction map from $H^1(F, E[2])$ to $H^1(K, E[2])$ is contained in the invariant subspace $H^1(K, E[2])^G$. □

For a similar result to Corollary 2.3.12 (ii) which holds when K/F is replaced by a cyclic degree p extension for an odd prime p, see [Bra14, Theorem 1.2].

Remark 2.3.13. Combining Lemma 2.2.11 with Lemma 2.3.11 allows one to recover the formula for the rank of E/K given in [Kra81, Theorem 1]. In the second part of that theorem, Kramer studies the group $\mathrm{Sel}_{\mathscr{C}(K)}(F, E[2])/\mathrm{cor}_{K/F}(\mathrm{Sel}_2(E/K))$, which he refers to as the everywhere local/global norms group, and shows that it carries a non-degenerate alternating pairing given by the sum of the Cassels–Tate pairing on $\mathrm{Sel}_2(E/F)$ and the pushforward (under φ_θ^*) of the Cassels–Tate pairing on $\mathrm{Sel}_2(E_\theta/F)$ (recall from Proposition 2.3.9 that $\mathrm{Sel}_{\mathscr{C}(K)}(F, E[2]) = \mathrm{Sel}_2(E/F) \cap \varphi_\theta^*(\mathrm{Sel}_2(E_\theta/F))$). In particular, this quotient group has even dimension.

When $\mathrm{Sel}_{\mathscr{C}(K)}(F, E[2])$ is not necessarily trivial we still get a lower bound for the dimension of the 2-Selmer group of E over K.

Lemma 2.3.14. *Assume that K/F is a quadratic extension. Then we have*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) \;\geq\; -2 + \sum_{v \in \Omega_F} \dim_{\mathbb{F}_2} E(F_v)/N_{K_w/F_v} E(K_w).$$

Proof. From Lemma 2.3.11 and Lemma 2.2.11 we find

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) \geq g_2(K/F; E) - \dim_{\mathbb{F}_2} H^1(K/F, E(K)[2]).$$

Note the inequality

$$\dim_{\mathbb{F}_2} H^1(K/F, E(K)[2]) \leq 2,$$

which is a consequence of the explicit description of cohomology of cyclic groups. The result then follows. □

Chapter 3

Local Norm Indices

Our approach to studying the statistical behaviour of p-Selmer groups over Galois extensions is to study the (co)-restriction Selmer groups and glimpse information about the p-Selmer group from those via the results in §2.2.2. This will, via Lemma 2.2.11, involve studying the genus theory of the p-Selmer group. The genus theory of the p-Selmer group of an elliptic curve E defined over a number field F arising from a finite Galois extension K/F is

$$g_p(K/F;E) := \sum_{v\in\Omega_F} \dim_{\mathbb{F}_p} E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right),$$

where in each summand, $w \in \Omega_K$ is a choice of place extending v and N_{K_w/F_v} is the norm map. In this chapter we study the summands in the genus theory: we compute local norm indices of elliptic curves in various settings.

The main applications of these results will be in Parts II and III. In §3.1 we describe the local norm index when $v \in \Omega_F$ is unramified in K/F, showing, in particular, that if E/F_v has Kodaira type I_0 or I_1 then the local norm index at v is trivial. This will be vital in Chapter 5 as the places with these reduction type are very common, and if the local norm index were nonzero then the average of the genus theory would grow very quickly. In §3.2 we consider the local norm index at places $v \in \Omega_F$ of residue characteristic at least 5. We list a complete set of conditions on the coefficients of E which determine the local norm index when K/F is a multiquadratic field and $p = 2$. This will will ultimately allow us to compute the average of $g_2(K/F;E)$ in Chapter 6 as E varies in the family of all elliptic curves.

The material in this chapter, unless clearly stated otherwise, is original work of the author. We let $F, \mathcal{O}_F, v$ be a finite extension of $\mathbb{Q}_\ell$ for some prime number ℓ, its ring of integers and normalised valuation, respectively.

§ 3.1 | Multiplicative Reduction and Unramified Extensions

In this section we consider local norm indices over unramified extensions when the elliptic curve in question has multiplicative reduction. Such places will turn out to be

the 'statistically significant' places in families such as that of 'all elliptic curves' – see Chapter 5 for more details, and for the main applications of the results here.

In this section, let E/F be an elliptic curve with multiplicative reduction. Moreover, let K/F be an unramified extension, let n be its degree and write $N_{K/F} = \sum_{g\in \mathrm{Gal}(K/F)} g \in \mathbb{Z}[\mathrm{Gal}(K/F)]$ for the usual norm element. We perform some local computations, extending results of Kramer [Kra81] in the case $n = 2$. Specifically, we determine the norm index for such E using the Tate parametrisation (see e.g. [Sil94, V§3-5]), the properties of which we recall below.

Recall from [Sil94, V Thms 3.1 and 5.3] that there is a unique element $q \in \mathcal{O}_F$ with $v(q) > 0$ such that $E(\overline{F})$ is isomorphic to $\overline{F}/q^{\mathbb{Z}}$. We call q the Tate parameter associated to E, and fix such an isomorphism and call it the Tate parametrisation. Moreover, if E has split multiplicative reduction, then we may assume that the Tate parametrisation is an isomorphism of G_F-modules.

Let L/F be the unramified quadratic extension, for each extension M/F define

$$I(M) := \left\{x \in (M\cdot L)^\times \ : \ N_{(M\cdot L)/M}(x) \in q^{\mathbb{Z}}\right\},$$
$$I_0(M) := \left\{x \in (M\cdot L)^\times \ : \ N_{(M\cdot L)/M}(x) = 1\right\}.$$

If E has non-split multiplicative reduction, then the quadratic twist of E by L has split multiplicative reduction, so we may assume that the Tate parametrisation is at least an isomorphism of G_L-modules. However, for a finite extension M/F which does not contain L, by [Sil94, V Cor. 5.4] the Tate parametrisation over the compositum $M\cdot L$ yields an isomorphism between $E(M)$ and $I(M)/q^{\mathbb{Z}}$. This isomorphism identifies $E_0(M)$, the points of the connected component of the identity in the Néron model of E, with $I_0(M)/q^{\mathbb{Z}}$.

Lemma 3.1.1. *If E/F has split multiplicative reduction, then the corresponding Tate parameter q satisfies*

$$v(q) = v(\Delta_E),$$

where Δ_E is a minimal discriminant for E/F.

Proof. By [Sil94, V Thm 3.1(b)] we have $\Delta_E = q\prod_{n\geq 1}(1-q^n)^{24}$, so the result is immediate. □

Proposition 3.1.2. *If E/F has split multiplicative reduction, then*

$$E(F)/N_{K/F}E(K) \cong \mathbb{Z}/\gcd(v(\Delta_E), n)\mathbb{Z},$$

where Δ_E is a minimal discriminant for E/F.

Proof. If E has Tate parameter $q \in \mathcal{O}_F$ then, since the Tate parametrisation is defined

over F, we have a commutative square

$$\begin{array}{ccc} E(K) & \xrightarrow{\sim} & K^\times/q^{\mathbb{Z}} \\ \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} \\ E(F) & \xrightarrow{\sim} & F^\times/q^{\mathbb{Z}}, \end{array}$$

and so

$$E(F)/N_{K/F}(E(K)) \cong F^\times/\left(N_{K/F}(K^\times)\cdot q^{\mathbb{Z}}\right).$$

Since the extension K/F is unramified, local class field theory identifies the exact sequence

$$0 \longrightarrow \tfrac{q^{\mathbb{Z}}}{q^{\mathbb{Z}}\cap N(K^\times)} \longrightarrow \tfrac{F^\times}{N_{K/F}(K^\times)} \longrightarrow \tfrac{F^\times}{\left(N_{K/F}(K^\times)\cdot q^{\mathbb{Z}}\right)} \longrightarrow 0,$$

with

$$0 \longrightarrow \langle v(q)\rangle \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\gcd(v(q),n)\mathbb{Z} \longrightarrow 0\ .$$

The result now follows from Lemma 3.1.1. □

Proposition 3.1.3. *If E/F has non-split multiplicative reduction and $n \in 2\mathbb{Z}$, then*

$$\#\left(E(F)/N_{K/F}E(K)\right) = \begin{cases} 2 & \text{if } v(\Delta_E) \in 2\mathbb{Z}, \\ 1 & \text{else.} \end{cases}$$

Proof. E has split multiplicative reduction over the unramified quadratic extension L/F, which is contained in K. Write $\tau \in \mathrm{Gal}(K/F)$ for the Frobenius element, so that $N_{K/F} = \sum_{k=0}^{n-1}\tau^k$, and L/F is the fixed field of the group generated by τ^2. The Tate parametrisation of E/K gives a commutative diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\sim} & K^\times/q^{\mathbb{Z}} \\ \downarrow{\scriptstyle N_{K/F}} & & \vdots{\scriptstyle \alpha} \\ E(F) & \xrightarrow{\sim} & I(F)/q^{\mathbb{Z}}, \end{array}$$

where since the norm map $N_{K/F}$ factors through the field L over which the Tate parametrisation is defined, the rightmost vertical map α is induced by the action of the element $\sum_{k=0}^{n-1}\chi_L(\tau^k)\tau^k$, where χ_L is the quadratic character cutting out the extension L/F. Note that for $x \in K^\times/q^{\mathbb{Z}}$

$$\alpha(x) = \prod_{k=1}^{n/2}\frac{\tau^{2k}(x)}{\tau^{2k+1}(x)} = \prod_{k=1}^{n/2}\tau^{2k}\left(\frac{x}{\tau(x)}\right) = N_{K/L}\left(\frac{x}{\tau(x)}\right).$$

Thus, since by Hilbert's theorem 90 we have

$$\left\{\frac{x}{\tau(x)}\ :\ x\in K^\times\right\} = \ker(N_{K/F}: K^\times \to F^\times),$$

we obtain that

$$\begin{aligned} E(F)/N_{K/F}(E(K)) &\cong \frac{I(F)}{N_{K/L}(\ker(N_{K/F}))\cdot q^{\mathbb{Z}}} \\ &\cong \frac{N_{L/F}(L^{\times})\cap q^{\mathbb{Z}}}{q^{2\mathbb{Z}}}, \end{aligned}$$

where since the norm map is surjective on units in unramified extensions, in particular $\ker(N_{L/F})\cap I(F) \subseteq N_{K/L}(\ker(N_{K/F}))$, the final isomorphism is just obtained by pushing through the map $N_{L/F}$. It is then clear that the size of this norm index is at most 2, and is 2 precisely when q is a norm from L, which by local class field theory occurs precisely when $v(q)$ is even. The result then follows from Lemma 3.1.1. □

Proposition 3.1.4. *If E/F has non-split multiplicative reduction, and n is odd then*

$$\#\left(E(F)/N_{K/F}E(K)\right) = 1.$$

Proof. Let χ_L be the character associated to the unramified quadratic extension L/F and write $\mathrm{Gal}(K\cdot L/F) = \langle \tau \ : \ \tau^{2n} = 1\rangle$. Letting U denote units, we consider the map f given by the composition

$$U_{K\cdot L} \xrightarrow{\tilde{f}} I_0(K) \xrightarrow{Q} E_0(K),$$

where for $u \in U_{K\cdot L}$ we set $\tilde{f}(u) := \frac{u}{\tau^n(u)}$ and Q is the Tate parametrisation map. By Hilbert's theorem 90 and the fact that the extension $K\cdot L/K$ is unramified, the map $\tilde{f}$ is surjective and so since Q is also surjective we must have that f is a surjection. Moreover for each $u \in U_{K\cdot L}$,

$$\begin{aligned} f(u) &= Q\left(\frac{u}{\tau^n(u)}\right) \\ &= Q(u) - Q\left(\tau^n(u)\right) \\ &= Q(u) - \chi_L(\tau^n)\tau^n\left(Q(u)\right) \\ &= Q(u) + \tau^n\left(Q(u)\right) \\ &= N_{K\cdot L/K}(Q(u)). \end{aligned}$$

Identifying $N_{K/F} = \sum_{k=0}^{n}\tau^{2k}$, we obtain a commutative square

$$\begin{array}{ccc} U_{K\cdot L} & \xrightarrow{f} & E_0(K) \\ \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} \\ U_L & \xrightarrow{f} & E_0(F). \end{array}$$

In particular, the right hand vertical map is now a surjection since the left is by local class field theory. This then means that $E_0(F) = N_{K/F}E_0(K) \subseteq N_{K/F}E(F)$, so in

particular we have a natural surjection

$$E(F)/E_0(F) \twoheadrightarrow E(F)/N_{K/F}E(K).$$

Since E has non-split multiplicative reduction, so has Tamagawa number 1 or 2, we must have that $E(F)/N_{K/F}E(K)$, which has odd order as it is a quotient of $E(F)/nE(F)$, is trivial. □

§ 3.2 | Multiquadratic Extensions

We will now compute local norm indices associated to elliptic curves over multiquadratic extensions. For the duration of this section we make the additional assumption that the residue characteristic of F satisfies $\ell \geq 5$. In order to ensure clarity, we will use v_F, π_F, k_F for the normalised valuation on F, a choice of uniformiser (fixed now and for the rest of the chapter) for F, and the residue field of F. Similarly, for any finite extension K/F we will write v_K, π_K, k_K for the same data associated to K.

§ 3.2.1 | The Tamagawa Ratio

We firstly define a Tamagawa ratio and describe its behaviour, which will have relevance to the local norm index later on.

Definition 3.2.1. For every elliptic curve E/F, and every multiquadratic extension K/F, we define the Tamagawa ratio

$$\mathcal{T}(K/F;E) := \frac{\prod_{d\in S} c(E_d/F)}{c(E/K)}$$

where $S = \ker(F^\times/F^{\times 2} \to K^\times/K^{\times 2})$.

We will now compute these ratios in all cases, postponing the explanation of their utility to later.

Definition 3.2.2. For an elliptic curve E/F, a minimal integral model is a small Weierstrass model

$$E : y^2 = x^3 + Ax + B$$

such that $A, B \in \mathcal{O}_F$ and that either $v_F(A) < 4$ or $v_F(B) < 6$.

Proposition 3.2.3. *Let K/F be the unramified quadratic extension. Let E/F be an elliptic curve, and*

$$E : y^2 = x^3 + Ax + B$$

be a minimal integral model. Then the Tamagawa ratio $\mathcal{T}(K/F;E)$ is given by Table 3.1.

Proof. For ease of notation, let $K = F(\sqrt{u})$. Note that minimal integral models for

K/F an unramified quadratic extension, E/F an elliptic curve, $E : y^2 = x^3 + Ax + B$ a minimal integral model.		
Kodaira Type of E/F	Extra Condition	$\mathcal{T}(K/F;E)$
I_0	-	1
$I_{n>0}$	n even	2
	n odd	1
II	-	1
III	-	2
IV	-	1
I_0^*	$T^3 + A\pi_F^{-2}T + B\pi_F^{-3}$ has 3 roots in $k_F^{\times 2}$	4
	otherwise	1
$I_{n>0}^*$	n even and $-(27B^2+4A^3)\pi_F^{-(6+n)} \in k_F^{\times 2}$	4
	n even and $-(27B^2+4A^3)\pi_F^{-(6+n)} \notin k_F^{\times 2}$	1
	n odd	2
IV^*	-	1
III^*	-	2
II^*	-	1

Table 3.1: Tamagawa ratio for unramified quadratic extensions.

the other curves in the definition of $\mathcal{T}(K/F;E)$ are given by

$$E_u/F : y^2 = x^3 + Au^2x + Bu^3,$$
$$E/K : y^2 = x^3 + Ax + B.$$

This then follows by a case analysis in Tate's algorithm (see Appendix A). In particular, note that the Kodaira types of E/F, E/K and E_u/F are all the same, and the only change can be in the splitness conditions. We list the cases below.

- If E/F has type I_0, II, or II^*, then the Tamagawa numbers in the ratio are all 1 and so $\mathcal{T}(K/F;E) = 1$.
- If E/F has type IV or IV^*, then since u is nonsquare in k_F, precisely one of E or E_u has split subtype (see Appendix A) over F and the other is nonsplit, whilst the type of E/K is automatically split. Thus $\mathcal{T}(K/F;E) = 1$.
- If E/F has type III or III^* then $\mathcal{T}(K/F;E) = 2$.
- If E/F has type I_0^* then write $P_E(T) := T^3 + A\pi_F^{-2}T + B\pi_F^{-3} \in k_F[T]$ and $P_{E_u}(T) := T^3 + Au^2\pi_F^{-2}T + Bu^3\pi_F^{-3} \in k_F[T]$. Note that there is a bijection between the roots of P_E and P_{E_u} given by $\alpha \mapsto u\alpha$, and so

$$\mathcal{T}(K/F;E) = \frac{(1 + \#\{\alpha \in k_F \ : \ P_E(\alpha) = 0\})^2}{(1 + \#\{\alpha \in k_K \ : \ P_E(\alpha) = 0\})}.$$

  If P is a product of linear factors over k_F then immediately $\mathcal{T}(K/F;E) = 4$. If $P(T)$ is irreducible over k_F then it is also over k_K (which is a quadratic extension

of k_F), so $\mathcal{T}(K/F;E) = 1$. Finally if $P(T)$ is a product of a linear and quadratic irreducible factor, then the quadratic factor splits over k_K and so $\mathcal{T}(K/F;E) = 1$.

- If E/F has multiplicative reduction of type I_n, then precisely one of E/F or E_u/F has split multiplicative reduction, with the other being nonsplit. Moreover, E/K must have split reduction of type I_n. Thus $\mathcal{T}(K/F;E) = 2$ if n is even, and $\mathcal{T}(K/F;E) = 1$ otherwise.
- If E/F has potentially multiplicative reduction of type I_n^*, we break into cases depending on the parity of n. If n is even, then either both E/F and E_u/F have split I_n^* reduction or both have nonsplit I_n^* reduction. Moreover, E/K necessarily has split I_n^* reduction. Thus $\mathcal{T}(K/F;E) = 4$ if E/F is split (i.e. $-(27B^2 + 4A^3)/\pi_F^{n+6} \in k_F^{\times 2}$) and $\mathcal{T}(K/F;E) = 1$ otherwise. If, on the other hand, n is odd, then it is clear that precisely one of E/F or E_u/F has split I_n^* reduction and the other must have nonsplit I_n^* reduction. As in the even case, the reduction type is necessarily split over K. Thus we have that $\mathcal{T}(K/F;E) = 2$.

□

Lemma 3.2.4. *Let $K = F(\sqrt{\theta})$ be a ramified quadratic extension. Let E/F be an elliptic curve. The Kodaira types of E_θ/F and E/K are determined by that of E/F and θ, and are listed in Table 3.2.*

Kodaira Types		
E/F	E_θ/F	E/K
$I_{n\geq 0}$	I_n^*	I_{2n}
II	IV^*	IV
III	III^*	I_0^*
IV	II^*	IV^*

Table 3.2: Kodaira types of ramified twists of elliptic curves

Proof. Note that, since this is a ramified quadratic extension where the residue characteristic is odd, $v_F(\theta)$ is odd. This is then a simple check using Tate's algorithm (see, e.g., Appendix A). □

Remark 3.2.5. Since the Kodaira types of E/K and E_θ/K are the same, and quadratic twisting is an involution (on the level of isomorphism classes of curves), we need only list each Kodaira type as either that of E/F or E_θ/F.

Proposition 3.2.6. *Let K/F be a ramified quadratic extension. Let $\theta \in F$ be such that $K = F(\sqrt{\theta})$ and $v_F(\theta) = 1$. Let E/F be an elliptic curve, and*

$$E : y^2 = x^3 + Ax + B$$

be a minimal integral model. Then the Tamagawa ratio $\mathcal{T}(K/F;E)$ is given by Table 3.3.

$K = F(\sqrt{\theta})$ a ramified quadratic extension, E/F an elliptic curve, $E : y^2 = x^3 + Ax + B$ a minimal integral model.			
Kodaira Type of E/F	Extra Condition(s)		$\mathcal{T}(K/F;E)$
I_0	$T^3 + AT + B$ has no roots in k_F		1
	$T^3 + AT + B$ has 1 root in k_F		2
	$T^3 + AT + B$ has 3 roots in k_F		4
I_0^*	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has no roots in k_F		1
	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has 1 root in k_F		2
	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has 3 roots in k_F		4
$I_{2n>0}$	$6B \in k_F^{\times 2}$	$-(27B^2 + 4A^3)\theta^{-2n} \in k_F^{\times 2}$	2
		$-(27B^2 + 4A^3)\theta^{-2n} \notin k_F^{\times 2}$	1
	$6B \notin k_F^{\times 2}$	$-(27B^2 + 4A^3)\theta^{-2n} \in k_F^{\times 2}$	4
		$-(27B^2 + 4A^3)\theta^{-2n} \notin k_F^{\times 2}$	2
$I_{2n>0}^*$	$6B\theta^{-3} \in k_F^{\times 2}$	$-(27B^2 + 4A^3)\theta^{-2n-6} \in k_F^{\times 2}$	2
		$-(27B^2 + 4A^3)\theta^{-2n-6} \notin k_F^{\times 2}$	1
	$6B\theta^{-3} \notin k_F^{\times 2}$	$-(27B^2 + 4A^3)\theta^{-2n-6} \in k_F^{\times 2}$	4
		$-(27B^2 + 4A^3)\theta^{-2n-6} \notin k_F^{\times 2}$	2
I_{2n+1}	$6B(27B^2 + 4A^3)\theta^{-2n-1} \in k_F^{\times 2}$		2
	$6B(27B^2 + 4A^3)\theta^{-2n-1} \notin k_F^{\times 2}$		1
I_{2n+1}^*	$6B(27B^2 + 4A^3)\theta^{-2n-10} \in k_F^{\times 2}$		2
	$6B(27B^2 + 4A^3)\theta^{-2n-10} \notin k_F^{\times 2}$		1
II, II^*, IV, IV^*	-		1
III	$-A\theta^{-1} \notin k_F^{\times 2}$		2
	$-A\theta^{-1} \in k_F^{\times 2}$		1
III^*	$-A\theta^{-3} \notin k_F^{\times 2}$		2
	$-A\theta^{-3} \in k_F^{\times 2}$		1

Table 3.3: Tamagawa ratio for ramified quadratic extensions.

Proof. This will follow from a case analysis and Tate's algorithm, using Lemma 3.2.4. If E/F has Kodaira type $I_{n\geq 0}$, II, III or IV then minimal integral models for the other curves in the definition of $\mathcal{T}(K/F;E)$ are given by

$$E_\theta/F : y^2 = x^3 + A\theta^2 x + B\theta^3,$$
$$E/K : y^2 = x^3 + Ax + B.$$

Otherwise E/F has Kodaira type $I_{n\geq 0}^*$, II^*, III^* or IV^*, and so minimal integral models for the other curves in the definition of $\mathcal{T}(K/F;E)$ are given by

$$E_\theta/F : y^2 = x^3 + A\theta^{-2} x + B\theta^{-3},$$
$$E/K : y^2 = x^3 + A\theta^{-2} x + B\theta^{-3}.$$

With these models in mind, we now perform the case analysis. The uniformisers that we use for Tate's algorithm over F and K will be $\pi_F = \theta$ and $\pi_K = \sqrt{\theta}$ respectively.

- If E/F has type I_0 reduction, then E_θ/F has type I_0^* and E/K has type I_0.

Thus, by Appendix A we have

$$\mathcal{T}(K/F;E) = 1 + \#\left\{\alpha \in k_F \ : \ \alpha^3 + A\alpha + B = 0\right\}.$$

The case that E/F has reduction type I_0^* is similar.

- If E/F has reduction type I_n for some $n > 0$ then by Lemma 3.2.4 E_θ/F has type I_n^* and E/K has type I_{2n}. Moreover, the reduction type of E/F is split if and only if that of E/K is split (the residue fields satisfy $k_F = k_K$). Thus by Appendix A we have

$$\frac{c(E/F)}{c(E/K)} = \begin{cases} 1/2 & \text{if } E/F \text{ has split reduction,} \\ 1/2 & \text{if } n \text{ is odd and } E/F \text{ has nonsplit reduction,} \\ 1 & \text{else.} \end{cases}$$

The result in this case then follows by computing the Tamagawa number $c(E_\theta/F)$, as is shown in Appendix A.

The argument when E/F has type I_n^* reduction is similar, swapping the roles of E and E_θ.

- If E/F has reduction type II, then E_θ/F has reduction type IV^* and E/K has type IV. The splitting conditions for E/K and E_θ/F are equivalent (each is split if and only if $B\theta^{-1} \in k_F^{\times 2}$), and so in particular one notes that $\mathcal{T}(K/F;E) = 1$. Similarly, the cases where E/F has reduction type IV^*, IV or II^* give $\mathcal{T}(K/F;E) = 1$.

- If E/F has reduction type III then E_θ/F has reduction type III^* and E/K has type I_0^*. Moreover $v_K(A) = 2$, $v_K(B) \geq 4$, so via Tate's algorithm Appendix A we have

$$\mathcal{T}(K/F;E) = \frac{4}{1 + \#\left\{\alpha \in k_K \ : \ \alpha^3 + (A/\theta)\alpha = 0\right\}}.$$

so the result is as required. Again, the proof for E/F of type III^* is similar by interchanging the roles of E and E_θ above.

Having treated the case of each possible reduction type of E/F, the proof is complete. □

Since F has odd residue characteristic, there is precisely one multiquadratic extension which is not accounted for by Tables 3.1 and 3.3: the unique biquadratic extension. We now provide the result there.

Proposition 3.2.7. *Let K/F be the biquadratic extension. Write $K = F(\sqrt{u}, \sqrt{\theta})$, where u is a nonsquare unit in the integers of F and $v_F(\theta)$ is odd. Let E/F be an elliptic curve, and*

$$E : y^2 = x^3 + Ax + B$$

be a minimal integral model. Then the Tamagawa ratio $\mathcal{T}(K/F;E)$ is given by Table 3.4.

Proof. It is easy to see from the definition of the Tamagawa ratio that there is an equality

$$\mathcal{T}(K/F;E) = \mathcal{T}(F(\sqrt{u})/F;E)\cdot\mathcal{T}(F(\sqrt{u})/F;E_\theta)\cdot\mathcal{T}(K/F(\sqrt{u});E).$$

Note that the reduction type of E_θ/F can be obtained from that of E/F by applying Lemma 3.2.4, and that the Kodaira type of $E/F(\sqrt{u})$ is the same as that of E/F (with potential changes to splitting conditions). Thus we can compute all of the terms on the right hand side of this equality by Propositions 3.2.3 and 3.2.6, which provides the entries seen in Table 3.4. □

K/F the biquadratic extension, E/F an elliptic curve, $E: y^2 = x^3 + Ax + B$ a minimal integral model.		
Kodaira Type of E/F	Extra Condition(s)	$\mathcal{T}(K/F;E)$
I_0	$T^3 + AT + B$ has no roots in k_F	1
	$T^3 + AT + B$ has 1 root in k_F	4
	$T^3 + AT + B$ has 3 roots in k_F	16
I_0^*	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has no roots in k_F	1
	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has 1 root in k_F	4
	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has 3 roots in k_F	16
I_n	n even and $-(27B^2 + 4A^3)\theta^{-n} \in k_F^{\times 2}$	16
	otherwise	4
I_n^*	n even and $-(27B^2 + 4A^3)\theta^{-n-6} \in k_F^{\times 2}$	16
	otherwise	4
II, II^*, IV, IV^*		1
III, III^*		8

Table 3.4: Tamagawa ratio for the biquadratic extension of F.

§ 3.2.2 | Local Norm Index

We now justify our interest in the Tamagawa ratio above. It turns out to in fact be the local norm index.

Proposition 3.2.8. *Let K/F be a multiquadratic extension. For every elliptic curve E/F we have*

$$\#E(F)/N_{K/F}E(K) = \mathcal{T}(K/F;E).$$

Proof. To ease notation we write $G := \mathrm{Gal}(K/F)$, and $X := \mathrm{Hom}(G, \mathbb{F}_2)$. We write $\chi_0 \in X$ for the trivial homomorphism, and for each $\chi \in X$ we write $\mathbb{Z}^{(\chi)}$ for the $\mathbb{Z}[G]$-module which is isomorphic to $\mathbb{Z}$ as an abelian group and on which $\sigma \in G$ acts by multiplication by $\chi(\sigma)$. We will simply write $\mathbb{Z}$ for $\mathbb{Z}^{\chi_0}$.

Consider the maps of $\mathbb{Z}[G]$-modules given by

$$\begin{aligned}\phi : \mathbb{Z}[G] &\to \bigoplus_{\chi\in X} \mathbb{Z}^{(\chi)} \\ \sum_\sigma a_\sigma \sigma &\mapsto \left(\sum_{\sigma\in G} a_\sigma \chi(\sigma)\right)_{\chi\in X},\end{aligned}$$

and

$$\begin{aligned}\widehat{\phi} : \bigoplus_{\chi\in X} \mathbb{Z}^{(\chi)} &\to \mathbb{Z}[G] \\ (b_\chi)_{\chi\in X} &\mapsto \sum_{\chi\in X} b_\chi \sum_{\sigma\in G} \chi(\sigma)\sigma.\end{aligned}$$

Both $\phi\circ\widehat{\phi}$ and $\widehat{\phi}\circ\phi$ are multiplication by $\#G$ on the respective modules. Thus we have a commutative diagram of $\mathbb{Z}[G]$-modules with exact rows given by:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigoplus_{\chi\in X\setminus\{\chi_0\}} \mathbb{Z}^{(\chi)} & \xrightarrow{\widehat{\phi}} & \mathbb{Z}[G] & \xrightarrow{N} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [\#G]} & & \downarrow{\scriptstyle \phi} & & \| & & \\ 0 & \longrightarrow & \bigoplus_{\chi\in X\setminus\{\chi_0\}} \mathbb{Z}^{(\chi)} & \longrightarrow & \bigoplus_{\chi\in X} \mathbb{Z}^{(\chi)} & \longrightarrow & \mathbb{Z} & \longrightarrow & 0, \end{array}$$

where the map $N : \sum a_\sigma\sigma \mapsto \sum a_\sigma$ is given by action of the norm element of $\mathbb{Z}[G]$, and the maps on the bottom row are the natural inclusion and projection. Via the twisting formalism of [MRS07, Lemma 1.3, Lemma 2.3, Prop 4.1, Example 1.5(ii)], this gives rise to a commutative diagram of abelian varieties with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \bigoplus_{d\in S\setminus\{1\}} E_d & \xrightarrow{\widehat{\phi}} & \mathrm{Res}_{K/F}E & \xrightarrow{N} & E & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [\#G]} & & \downarrow{\scriptstyle \phi} & & \| & & \\ 0 & \longrightarrow & \bigoplus_{d\in S\setminus\{1\}} E_d & \longrightarrow & \bigoplus_{d\in S} E_d & \longrightarrow & E & \longrightarrow & 0, \end{array} \tag{3.1}$$

where $\mathrm{Res}_{K/F}E$ is the Weil restriction, and we abuse notation by reusing $\phi, \widehat{\phi}$ for now the corresponding isogenies of abelian varieties induced by the module maps above. Explicitly, on F-points the the map N acts on $\mathrm{Res}_{K/F}E(F) = E(K)$ as the norm map $N_{K/F}$. Taking F-points above, noting that since the bottom right map is projection it remains surjective on F-points, we obtain a short exact sequence

$$0 \longrightarrow \bigoplus_{d\in S\setminus\{1\}} \frac{E_d(F)}{(\#G)E_d(F)} \longrightarrow \frac{\bigoplus_{d\in S} E_d(F)}{\phi(\mathrm{Res}_{K/F}E(F))} \longrightarrow \frac{E(F)}{N_{K/F}E(K)} \longrightarrow 0. \tag{3.2}$$

Using a result of Schaefer [Sch96, Lemma 3.8], we can describe the order of the central

term:

$$\#\frac{\bigoplus_{d\in S} E_d(F)}{\phi(\mathrm{Res}_{K/F}E(F))} = \frac{|\phi'(0)|_F \prod_{d\in S} c(E_d/F)}{\#\mathrm{Res}_{K/F}E(F)[\phi]\cdot c(\mathrm{Res}_{K/F}E/F)}, \tag{3.3}$$

where $|\phi'(0)|_F$ is the normalised absolute value of the determinant of the Jacobian matrix of partials of ϕ evaluated near 0. An elementary diagram chase in (3.1), using that the rightmost vertical map is equality, we obtain that $\mathrm{Res}_{K/F}E[\phi] \cong \oplus_{d\in S\setminus\{1\}} E_d[\#G]$. Moreover, by [Lor11, 3.19] we have that $c(\mathrm{Res}_{K/F}E/F) = c(E/K)$, and so from (3.3) and (3.2) we obtain

$$\begin{aligned}\#\frac{E(F)}{N_{K/F}E(K)} &= \left(\prod_{d\in S\setminus\{1\}} \frac{\#\frac{E_d(F)}{(\#G)E_d(F)}}{\#E_d(F)[\#G]}\right)\frac{|\phi'(0)|_F \prod_{d\in S} c(E_d/F)}{c(E/K)}\\ &= |\phi'(0)|_F\, \mathcal{T}(K/F;E),\end{aligned}$$

where the second equality uses that the residue characteristic is odd and each $E_d(F)$ contains a finite index subgroup isomorphic to the integers of F (see, e.g., [Sil09, VII Proposition 6.3]).

It remains to show that $|\phi'(0)|_F = 1$, which we now do. Note that $N_{K/F}E(K) \supseteq (\#G)E(F)$, and so the order of the norm index is a power of two, and the computations of Propositions 3.2.3, 3.2.6 and 3.2.7 show that $\mathcal{T}(K/F;E)$ is also a power of 2. On the other hand, $|\phi'(0)|_F$ is an integer power of the residue characteristic, which is odd, and so must be 1 in order for the displayed equation above to hold, concluding the proof. □

Note that we are not actually making use of the norm index all of the time, but in fact the norm index modulo 2 which is the object appearing in the genus theory formula (see Definition 2.2.8) $g_2(K/F;E)$. For quadratic extensions there is nothing to distinguish, but for biquadratic we have to be more careful.

Proposition 3.2.9. *Let K/F be a quadratic extension. Let E/F be an elliptic curve, and*

$$E : y^2 = x^3 + Ax + B$$

be a minimal integral model. Then we have an equality

$$\#E(F)/\left(N_{K/F}E(K) + 2E(F)\right) = \mathcal{T}(K/F;E)$$

and so the norm index modulo 2 is given by: Table 3.1 if K/F is unramified; or Table 3.3 if K/F is ramified.

Proof. Clearly $E(F)/N_{K/F}E(K)$ is $[K:F]$-torsion and so this follows from Proposition 3.2.8 and: if K/F is unramified Proposition 3.2.3 or if K/F is ramified then Proposition 3.2.6. □

For the biquadratic case we must be more careful. First we will need a helpful

lemma which is true in far more generality than it is presented but we will only require it in our present setting.

Lemma 3.2.10. *Let E/F be an elliptic curve. Then there is an isomorphism of groups*

$$E(F)[4] \cong E(F)/4E(F).$$

Proof. There is a finite index subgroup, arising from the filtration by formal groups, of $E(F)$ which is isomorphic to the additive group of integers $\mathcal{O}_F$ of F (see e.g. [Sil09, VII Prop. 6.3]). We will name this subgroup $E_1(F)$, and note that (since the residue characteristic of F is coprime to 4) we have $E_1(F) = 4E_1(F) \subseteq 4E(F)$. Since $E_1(F)$ has finite index in $E(F)$, we certainly have an isomorphism

$$\frac{E(F)}{E_1(F)}[4] \cong \frac{\frac{E(F)}{E_1(F)}}{4\frac{E(F)}{E_1(F)}}. \tag{3.4}$$

Now consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(F) & \longrightarrow & E(F) & \longrightarrow & E(F)/E_1(F) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \times 4} & & \downarrow{\scriptstyle \times 4} & & \downarrow{\scriptstyle \times 4} & & \\ 0 & \longrightarrow & E_1(F) & \longrightarrow & E(F) & \longrightarrow & E(F)/E_1(F) & \longrightarrow & 0. \end{array}$$

An application of the snake lemma, using the fact that multiplication by 4 is bijective on $E_1(F) \cong \mathcal{O}_F$, provides isomorphisms

$$E(F)[4] \cong \frac{E(F)}{E_1(F)}[4] \qquad\qquad E(F)/4E(F) \cong \frac{\frac{E(F)}{E_1(F)}}{4\frac{E(F)}{E_1(F)}}.$$

Combining these with (3.4) we obtain the result. □

We can now deduce the required norm index modulo 2 from the Tamagawa ratio.

Proposition 3.2.11. *Let K/F be the biquadratic extension. Write $K = F(\sqrt{u}, \sqrt{\theta})$, where u is a nonsquare unit in the integers of F and $v_F(\theta)$ is odd. Let E/F be an elliptic curve, and*

$$E : y^2 = x^3 + Ax + B$$

be a minimal integral model. Then the norm index modulo 2, $\#\frac{E(F)}{\left(N_{K/F}E(K)+2E(F)\right)}$, is given by Table 3.5.

Proof. Note firstly that, by Lemma 3.2.10 and the fact that $4E(F) \subseteq N_{K/F}E(K)$, we can identify $E(F)/N_{K/F}E(K)$ as a quotient of a subgroup of the abelian group $(\mathbb{Z}/4\mathbb{Z})^2$. Considering Proposition 3.2.8 it is then clear that whenever $\mathcal{T}(K/F; E) = 1, 2, 8, 16$ then $\#\left(E(F)/N_{K/F}E(K) + 2E(F)\right) = 1, 2, 4, 4$ respectively. Using Proposition 3.2.7 we can then fill in all of the cases aside from those for which $\mathcal{T}(K/F; E) = 4$, in which

K/F the biquadratic extension, E/F an elliptic curve, $E : y^2 = x^3 + Ax + B$ a minimal integral model.		
Kodaira Type of E/F	Extra Condition(s)	$\#\frac{E(F)}{N_{K/F}E(K)+2E(F)}$
I_0	$T^3 + AT + B$ has no roots in k_F	1
	$T^3 + AT + B$ has 1 root in k_F	2
	$T^3 + AT + B$ has 3 roots in k_F	4
I_0^*	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has no roots in k_F	1
	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has 1 root in k_F	2
	$T^3 + A\theta^{-2}T + B\theta^{-3}$ has 3 roots in k_F	4
I_n	n even and $-(27B^2 + 4A^3)\theta^{-n} \in k_F^{\times 2}$	4
	otherwise	2
I_n^*	n even and $-(27B^2 + 4A^3)\theta^{-n-6} \in k_F^{\times 2}$	4
	otherwise	2
II, II^*, IV, IV^*		1
III, III^*		4

Table 3.5: Norm index modulo 2 from the biquadratic extension of F.

case we have two possibilities:

$$E(F)/N_{K/F}E(K) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{or} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \end{cases}$$

and these have different sizes modulo 2. The cases when $\mathcal{T}(K/F; E) = 4$ are when

1. E has Kodaira type $I_{n>0}$ or $I^*_{n>0}$, and the discriminant of the minimal integral model ($\Delta_E = -(27B^2 + 4A^3)$) satisfies $\Delta_E \notin F^{\times 2}$; or

2. E has Kodaira type I_0 and $T^3 + AT + B$ has 1 root in k_F; or

3. E has Kodaira type I_0^* and $T^3 + A\theta^{-2}T + B\theta^{-3}$ has 1 root in k_F.

Before we deal with each of these cases, note that it is enough to show that $E(F)$ does not have full 2-torsion (i.e. $E(F)[2] \ncong (\mathbb{Z}/2\mathbb{Z})^2$) Indeed by Lemma 3.2.10 we would have $E(F)/4E(F) \cong E(F)[4] \subseteq \mathbb{Z}/4\mathbb{Z}$ and since $E(F)/N_{K/F}E(K)$ is a quotient of this group we obtain

$$E(F)/N_{K/F}E(K) \cong \mathbb{Z}/4\mathbb{Z},$$

which would imply the remaining results in the table.

For case 1: the discriminant is nonsquare and as this is also the discriminant of the cubic polynomial $f(T) = T^3 + AT + B$ (whose roots give the 2-torsion points on E), we must have that the Galois group of f is not a subgroup of A_3 so in particular contains an order 2 element. Thus $E(F)[2]$ cannot be full.

For case 2 note that if $E(F)$ has full 2-torsion then since we have good reduction so would the reduced curve (and so we would have 3 roots, not 1 over k_F). Similarly, for case 3, note that there is a bijection between the roots of $T^3 + AT + B$ over F and

those of $T^3 + A\theta^{-2}T + B\theta^{-3}$ (namely send $\alpha \mapsto \theta^{-1}\alpha$) and so again we cannot have full 2-torsion as then we'd have 4 roots in k_F and not 1. $\square$

Part II

Quadratic Twist Families

Chapter 4

Quadratic Twists of Elliptic Curves

This chapter is concerned with joint work with Adam Morgan [MP22]. For the rest of the chapter we fix a quadratic extension $K/\mathbb{Q}$. Write $K = \mathbb{Q}(\sqrt{\theta})$ for a squarefree integer θ, and write $G = \mathrm{Gal}(K/\mathbb{Q})$. Moreover we fix an elliptic curve $E/\mathbb{Q}$. At this point we make no assumption on the 2-torsion of E, in later sections we will reduce to the case of full 2-torsion but we shall be clear when this occurs.

We study the statistical behaviour of the 2-Selmer groups of quadratic twists of E, i.e. $\mathrm{Sel}_2(E_d/K)$ as d varies in the set of squarefree integers. We begin, in §4.1, by recalling the necessary results from Chapter 2 for this chapter. Then in §4.2 we describe the average of $g_2(K/\mathbb{Q}; E_d)$ as d varies, and show that this function usually has a normal distribution in a similar sense to the classical Erdős–Kac theorem. In §4.3, assuming a claim that if E has full 2-torsion then $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) = 0$ for 100% of d, we go on to prove the main results of this section, as stated in §1.4,

§4.4 and §4.5 are then dedicated to the proof of the claim that if E has full 2-torsion then the Selmer groups $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ vanish for 100% of d. To do this we draw on analytic techniques developed by Heath-Brown [HB93, HB94]. That work takes as a point of departure the explicit description of 2-Selmer groups of elliptic curves with full 2-torsion provided by 2-descent. In §4.4 we similarly give an explicit description of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ as a subgroup of $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$.

In §4.5 we opt to replace $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ with a certain subgroup S_d of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ (see Definition 4.5.4) whose vanishing implies the vanishing of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$, but which admits a simpler explicit description. In §4.5.5 we give a formula for the order of S_d as a sum of Jacobi symbols in a form which can be treated by the analytic tools of Heath-Brown mentioned above. The passage from $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ to S_d causes the resulting analysis to be much closer to that carried out by Fouvry–Klüners in [FK07] to determine the distribution of 4-ranks of class groups of quadratic fields. In §4.6 we provide an example of a thin family of quadratic twists for which the Galois action on $\mathrm{Sel}_2(E_d/K)$ is nontrivial, as claimed in §1.2.3.

§ 4.1 | 2-Selmer Groups over Quadratic Extensions

Denote by $\mathrm{Sel}_2(E/K)$ the 2-Selmer group of E/K. The conjugation action of G on $H^1(K, E[2])$ makes $\mathrm{Sel}_2(E/K)$ into an $\mathbb{F}_2[G]$-module.

The structure of $\mathrm{Sel}_2(E/K)$ has been studied by Kramer in [Kra81]. In this section, since it will be useful for what follows, we give a reinterpretation of part of this work in the language of Selmer structures (see also work of Mazur–Rubin [MR07, MR10] for a similar perspective). The results in this section can be adapted in a straightforward way to general quadratic extensions of number fields (and this is the setting in which Kramer proves his results). However, we stick to quadratic extensions of $\mathbb{Q}$ since this is the setting in which all of our counting is to be carried out.

We begin by gathering what we will use about $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ from Chapter 2.

Proposition 4.1.1. *The following properties hold for the Selmer structure $\mathscr{C}(K)$.*

(i) For each place v of $\mathbb{Q}$ we have

$$\mathscr{C}_v(K/\mathbb{Q}; E) = \mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathscr{S}(E/K_w)) \leq H^1(\mathbb{Q}_v, E[2]),$$

where w is any choice of place of K extending v.

(ii) For each place v of $\mathbb{Q}$ we moreover have

$$\mathscr{C}_v(K/\mathbb{Q}; E) = \delta_v(N_{K_w/\mathbb{Q}_v}E(K_w)) = \mathscr{S}_v(\mathbb{Q}; E) \cap \mathscr{S}_v^{(\theta)}(\mathbb{Q}; E),$$

where $\delta_v : E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \hookrightarrow H^1(\mathbb{Q}_v, E[2])$ is the coboundary map arising from the Kummer sequence (2.1).

(iii) Globally we have $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) = \mathrm{Sel}_2(E/\mathbb{Q}) \cap \varphi_\theta^*\left(\mathrm{Sel}_2(E_\theta/\mathbb{Q})\right)$. Moreover, we have

$$\mathrm{cor}_{K/\mathbb{Q}}\left(\mathrm{Sel}_2(E/K)\right) \subseteq \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]).$$

Proof. (i): This is Lemma 2.2.2.

(ii): The first equality follows from the fact that the coboundary maps arising from the respective Kummer sequences (2.1) over K_w and $\mathbb{Q}_v$ commute with corestriction. The second equality follows from Proposition 2.3.9.

(iii): The claim that $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) = \mathrm{Sel}_2(E/\mathbb{Q}) \cap \mathrm{Sel}_2(E_\theta/\mathbb{Q})$ follows from Proposition 2.3.9. The inclusion follows from Lemma 2.2.6 and compatibility of the local and global corestriction maps. □

We may use the Greenberg–Wiles formula (Theorem 2.1.4) to determine the difference between the dimensions of $\mathrm{Sel}_{\mathscr{F}(K)}(\mathbb{Q}, E[2])$ and $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$.

Lemma 4.1.2. *We have*

$$\dim \mathrm{Sel}_{\mathscr{F}(K)}(\mathbb{Q}, E[2]) - \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) = g_2(K/\mathbb{Q}; E),$$

where the right hand side is defined in Definition 2.2.8.

Proof. This is Lemma 2.2.11 in the case $p = 2$, $F = \mathbb{Q}$ and $K/\mathbb{Q}$ quadratic. □

We also have the following results, relating the (co)restriction Selmer groups to the 2-Selmer group over K.

Lemma 4.1.3. *Assume that K/F is a quadratic extension. Then we have*

$$\dim_{\mathbb{F}_2} \mathrm{Sel}_2(E/K) \;\geq\; -2 + \sum_{v \in \Omega_F} \dim_{\mathbb{F}_2} E(F_v)/N_{K_w/F_v} E(K_w).$$

Proof. This is Lemma 2.3.14 when $F = \mathbb{Q}$. □

Corollary 4.1.4. *If $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) = 0$, then all of the following hold.*

(i) There is a short exact sequence

$$0 \longrightarrow H^1(K/\mathbb{Q}, E(K)[2]) \xrightarrow{\inf} \mathrm{Sel}_{\mathscr{F}(K)}(\mathbb{Q}, E[2]) \xrightarrow{\mathrm{res}_{K/\mathbb{Q}}} \mathrm{Sel}_2(E/K) \longrightarrow 0,$$

where the first map is inflation.

(ii) We have

$$\dim \mathrm{Sel}_2(E/K) = g_2(K/\mathbb{Q}; E) - \dim\left(\frac{E(\mathbb{Q})[2]}{N_{K/\mathbb{Q}} E(K)[2]}\right).$$

(iii) The G-action on $\mathrm{Sel}_2(E/K)$ is trivial.

Proof. This is Corollary 2.3.12 when $F = \mathbb{Q}$. □

§ 4.2 | Quadratic Twists and a Distribution Result

Recall that $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ is a quadratic extension, $G = \mathrm{Gal}(K/\mathbb{Q})$ and $E/\mathbb{Q}$ is an elliptic curve. We now consider the effect of replacing $E/\mathbb{Q}$ by its quadratic twist $E_d/\mathbb{Q}$, for a squarefree integer d. We denote by $\mathscr{F}_d$ and $\mathscr{C}_d$ the Selmer structures of Definition 2.2.1 with local conditions $\mathscr{F}_v(K/\mathbb{Q}; E_d)$ and $\mathscr{C}_v(K/\mathbb{Q}; E_d)$ respectively. We have associated Selmer groups $\mathrm{Sel}_{\mathscr{F}_d}(\mathbb{Q}, E_d[2])$ and $\mathrm{Sel}_{\mathscr{C}_d}(\mathbb{Q}, E_d[2])$. For a squarefree integer d we write $\chi_d : G_{\mathbb{Q}} \to \{\pm 1\}$ for the associated quadratic character defined by

$$\chi_d(\sigma) = \sigma(\sqrt{d})/\sqrt{d}.$$

§ 4.2.1 | The Cokernel of the Local Norm Map

It turns out that the cokernel of the local norm map varies in a predictable way as we vary d. First, we fix some notation.

Notation 4.2.1. Fix a choice Σ of a finite set of places of $\mathbb{Q}$ containing the real place, 2, all primes which ramify in $K/\mathbb{Q}$, and all primes at which E has bad reduction.

We begin with the following observation.

Lemma 4.2.2. *Let $p \notin \Sigma$ be a prime divisor of d. Then $E_d(\mathbb{Q}_p^{\mathrm{nr}})$ has no points of exact order 4. In particular, the same is true of $E_d(\mathbb{Q}_p)$.*

Proof. By assumption, E has good reduction at p so that $E[4]$ is unramified at p. Thus any element σ in the inertia group I_p acts on $E_d[4]$ by multiplication by $\chi_d(\sigma)$. Since χ_d is ramified at p by assumption, the restriction of χ_d to I_p is non-trivial and one has

$$E_d[4]^{I_p} = \{P \in E_d[4] \quad | \quad P = -P\} = E_d[2],$$

giving the result. □

Lemma 4.2.3. *Let d be a squarefree integer, let $p \notin \Sigma$ be a prime, and let $\mathfrak{p}$ be a prime of K lying over p. Then*

$$\dim E_d(\mathbb{Q}_p)/N_{K_\mathfrak{p}/\mathbb{Q}_p} E_d(K_\mathfrak{p}) = \begin{cases} 2 & p \mid d,\ p \text{ inert in } K/\mathbb{Q},\ \dim E(\mathbb{Q}_p)[2] = 2, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If p splits in K, then the local extension $K_\mathfrak{p}/\mathbb{Q}_p$ is trivial, so that $N_{K_\mathfrak{p}/\mathbb{Q}_p}$ is the identity map on $E_d(\mathbb{Q}_p)$.

Next, suppose that $p \nmid d$. Since also $p \notin \Sigma$, E_d has good reduction at p, and $K_\mathfrak{p}/\mathbb{Q}_p$ is unramified. It follows from [Maz72, Corollary 4.4] that $N_{K_w/\mathbb{Q}_p}$ is surjective, giving the result.

Now suppose that $p \mid d$ and p is inert in $K/\mathbb{Q}$. In particular, the local extension $K_\mathfrak{p}/\mathbb{Q}_p$ is unramified of degree 2. Lemma 4.2.2 and a dimension count then show that the horizontal maps (induced by the inclusion of $E_d(K_\mathfrak{p})[2]$ into $E_d(K_\mathfrak{p})$) in the commutative square

$$\begin{array}{ccc} E_d(K_\mathfrak{p})[2] & \xrightarrow{\sim} & E_d(K_\mathfrak{p})/2E_d(K_\mathfrak{p}) \\ \downarrow{\scriptstyle N_{K_\mathfrak{p}/\mathbb{Q}_p}} & & \downarrow{\scriptstyle N_{K_\mathfrak{p}/\mathbb{Q}_p}} \\ E_d(\mathbb{Q}_p)[2] & \xrightarrow{\sim} & E_d(\mathbb{Q}_p)/2E_d(\mathbb{Q}_p), \end{array}$$

are isomorphisms. Let σ denote the non-trivial element of $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$. Since -1 acts trivially on $E_d(K_\mathfrak{p})[2]$, we have a short exact sequence

$$0 \to E_d(\mathbb{Q}_p)[2] \longrightarrow E_d(K_\mathfrak{p})[2] \xrightarrow{1+\sigma} N_{K_\mathfrak{p}/\mathbb{Q}_p}\left(E_d(K_\mathfrak{p})[2]\right) \to 0.$$

We thus have

$$\begin{aligned} \dim E_d(\mathbb{Q}_p)/N_{K_\mathfrak{p}/\mathbb{Q}_p} E_d(K_\mathfrak{p}) &= \dim E_d(\mathbb{Q}_p)[2]/N_{K_\mathfrak{p}/\mathbb{Q}_p}\left(E_d(K_\mathfrak{p})[2]\right) \\ &= 2\dim E_d(\mathbb{Q}_p)[2] - \dim E_d(K_\mathfrak{p})[2] \\ &= 2\dim E(\mathbb{Q}_p)[2] - \dim E(K_\mathfrak{p})[2]. \end{aligned}$$

It remains to break into cases according to $\dim E(\mathbb{Q}_p)[2] = 0, 1, 2$. If $\dim E(\mathbb{Q}_p)[2] \neq 1$ then $\dim E(\mathbb{Q}_p)[2] = \dim E(K_\mathfrak{p})[2]$ since the 2-torsion is either already full over $\mathbb{Q}_p$

or given by the splitting of an irreducible cubic. In the case that $\dim E(\mathbb{Q}_p)[2] = 1$, noting that since E has good reduction at p, $\mathbb{Q}_p(E[2])/\mathbb{Q}_p$ is unramified, we have $\dim E(K_{\mathfrak{p}})[2] = 2$, completing the proof. □

Remark 4.2.4. If $p \neq 3$ then this could also be deduced from the tables in §3.2, however since we have not treated 3 there and it can be done here with no extra effort then we leave in the proof above.

Remark 4.2.5. At primes $p \in \Sigma$ the cokernel of the local norm map is more complicated and depends on the reduction type of $E_d/\mathbb{Q}_p$. See [Kra81] or [KT82] for more details. However, since the isomorphism class of E_d over $\mathbb{Q}_p$ depends only on the class of d in $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, the same is true of the cokernel of the local norm map.

To ease notation in what follows, we make the following definition.

Notation 4.2.6. For a squarefree integer d, write

$$g(d) := g_2(K/\mathbb{Q}; E_d)$$

where for a place v of $\mathbb{Q}$, we denote by w a choice of extension of v to K. Further, write

$$\omega_{E,K}(d) := \#\left\{p \mid d \ : \ \begin{smallmatrix} p\not\in\Sigma \\ p \text{ inert in } K/\mathbb{Q} \\ \dim E(\mathbb{Q}_p)[2]=2 \end{smallmatrix}\right\}.$$

Note that by Lemma 4.1.3, the function $g(d)-2$ gives a lower bound for $\dim \mathrm{Sel}_2(E_d/K)$.

Proposition 4.2.7. *As d varies in squarefree integers, we have*

$$g(d) = 2\omega_{E,K}(d) + O(1)$$

where the implied constant depends only on the initial curve E and the quadratic field K.

Proof. Since the places in Σ contribute $O(1)$ to $g(d)$, we may ignore them. The result now follows from Lemma 4.2.3. □

§ 4.2.2 | The Distribution of $g(d)$

Notation 4.2.8. Let $\delta_{E,K}$ be the natural density of primes p such that $\omega_{E,K}(p) = 1$.

The possible values of $\delta_{E,K}$ may be computed by applying the Chebotarev density theorem to the extension $K(E[2])/\mathbb{Q}$ and are given by the following table:

$\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$	$\{1\}$	$\mathbb{Z}/2\mathbb{Z}$ $K\neq\mathbb{Q}(E[2])$	$\mathbb{Z}/2\mathbb{Z}$ $K=\mathbb{Q}(E[2])$	$\mathbb{Z}/3\mathbb{Z}$	S_3 $K\not\subseteq\mathbb{Q}(E[2])$	S_3 $K\subseteq\mathbb{Q}(E[2])$
$\delta_{E,K}$	1/2	1/4	0	1/6	1/12	0

In the following result of Erdős–Kac type, we determine the asymptotic distribution of the function $g(d)$ when the 2-torsion field of E does not interact with K. Since $\dim \mathrm{Sel}_2(E_d/K) \geq g(d) - 2$ by Lemma 4.1.3, this shows that $\dim \mathrm{Sel}_2(E_d/K)$ is (in a precise sense) typically at least as large as a constant times $\log\log(d)$.

Proposition 4.2.9. *Suppose that $\mathbb{Q}(E[2]) \cap K = \mathbb{Q}$. Further, for a squarefree integer d write*

$$\mu(d) := 2\delta_{E,K} \log\log|d| \quad \text{and} \quad \sigma(d) := \sqrt{4\delta_{E,K} \log\log|d|}.$$

Then the quantity

$$\frac{g(d) - \mu(d)}{\sigma(d)}$$

follows a standard normal distribution. That is, for all $z \in \mathbb{R}$ we have

$$\lim_{X\to\infty} \frac{\#\left\{|d| \le X \text{ squarefree } : \frac{g(d)-\mu(d)}{\sigma(d)} \le z\right\}}{\#\left\{|d| \le X \text{ squarefree}\right\}} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-t^2/2} dt.$$

Proof. Let $\gamma(d) := 2\omega_{E,K}(d)$. Since by Proposition 4.2.7 this differs from $g(d)$ by a bounded amount, it is enough to prove the same assertion with g replaced by γ. Moreover, since this function satisfies $\gamma(d) = \gamma(-d)$, it is enough to prove that γ has this distribution on the positive squarefree integers. We will do this by combining the method of moments with [GS07, Prop. 4]. Specifically, in the notation of that proposition, take

$$\mathcal{A} := \{d \text{ squarefree } : \ 1 \le d \le X\}$$

and

$$\mathcal{P} := \left\{p \text{ prime} : p \le X^{\varepsilon(X)}\right\}$$

for a function $\varepsilon(X) = o(1)$ to be chosen later. Further, let $\gamma_{\mathcal{P}}$ be the strongly additive function which agrees with γ for $p \in \mathcal{P}$, and takes the value 0 on primes $p \notin \mathcal{P}$. Note that, still using the notation of [GS07, Prop. 4] we can take

$$h(d) = \prod_{p|d} \frac{p}{p+1}, \qquad r_d \ll d\sqrt{X}, \qquad x = \frac{6X}{\pi^2} + O(\sqrt{X}), \quad \text{and} \quad M = 2,$$

along with

$$\mu_{\mathcal{P}}(\gamma) = \sum_{p\in\mathcal{P}} 2\omega_{E,K}(p) \frac{1}{p+1}$$

and

$$\sigma_{\mathcal{P}}(\gamma)^2 = \sum_{p\in\mathcal{P}} 4\omega_{E,K}(p) \frac{p}{(p+1)^2}.$$

Using the explicit form of the Chebotarev density theorem given in [LO77], standard arguments give

$$\mu_{\mathcal{P}}(\gamma) = 2\delta_{E,K} \log\log(X) + O(\log\varepsilon(X)) \ \text{ and } \ \sigma_{\mathcal{P}}(\gamma)^2 = 4\delta_{E,K} \log\log(X) + O(\log\varepsilon(X)).$$

Taking X sufficiently large in the conclusion of [GS07, Prop. 4] shows that for any

$k \geq 0$ we have

$$\frac{1}{\#\mathcal{A}} \sum_{d \in \mathcal{A}} (\gamma_{\mathcal{P}}(d) - \mu_{\mathcal{P}}(\gamma))^k$$
$$\begin{cases} = (k-1)!! \sigma_{\mathcal{P}}(\gamma)^k + O_k\left(\sigma_{\mathcal{P}}(\gamma)^{k-2} + \log\log(X)^k X^{2k\varepsilon(X)-1/2}\right) & k \text{ even}, \\ \ll_k \sigma_{\mathcal{P}}(\gamma)^{k-1} + \log\log(X)^k X^{2k\varepsilon(X)-1/2} & k \text{ odd}. \end{cases}$$

In particular, the kth moments of $(\gamma_{\mathcal{P}} - \mu_{\mathcal{P}}(\gamma))/\sigma_{\mathcal{P}}(\gamma)$ converge to those of a normal random variable with mean 0 and variance 1. Note that for $n \leq X$ we have

$$\gamma(n) - \gamma_{\mathcal{P}}(n) \leq 2\#\left\{p \mid n \ : \ p > X^{\varepsilon(X)}\right\} \leq \frac{\log(n)}{\varepsilon(X)\log(X)} \leq \varepsilon(X)^{-1}.$$

Induction on k (cf. [GS07, Deduction of Theorem 1]) now shows that, taking $\varepsilon(X) = \log\log\log(X)^{-1}$, we have

$$\frac{1}{\#\mathcal{A}} \sum_{d \in \mathcal{A}} (\gamma(d) - 2\delta_{E,K}\log\log(X))^k = \frac{1}{\#\mathcal{A}} \sum_{d \in \mathcal{A}} (\gamma_{\mathcal{P}}(d) - \mu_{\mathcal{P}}(\gamma))^k + o(\log\log(X)^{k/2}).$$

Thus the kth moments of $(\gamma - 2\delta_{E,K}\log\log(X))/\sqrt{4\delta_{E,K}\log\log(X)}$ converge as $X \to \infty$ to those of the standard normal distribution. It then follows from [Bil95, Theorem 30.2, Example 30.1] that γ becomes normally distributed with mean $2\delta_{E,K}\log\log(X)$ and variance $4\delta_{E,K}\log\log(X)$ in the limit $X \to \infty$, i.e.

$$\lim_{X\to\infty} \frac{\#\left\{|d| \leq X \text{ squarefree} \ : \ \frac{g(d) - \delta_{E,K}\log\log(X)}{\sqrt{4\delta_{E,K}\log\log(X)}} \leq z\right\}}{\#\left\{|d| \leq X \text{ squarefree}\right\}} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-t^2/2} dt.$$

The result now follows. □

Remark 4.2.10. In the last step of the proof we have used the standard result that a function f becomes normal as $X \to \infty$ with mean $\mu(X) := C_0 \log\log(X)$ and variance $\sigma^2(X) := C_1 \log\log(X)$ for some constants $C_0, C_1 > 0$ if and only if the function $(f(d) - \mu(d))/\sigma(d)$ becomes normal as $X \to \infty$ with mean 0 and variance 1. This can be proved directly.

Remark 4.2.11. In the case that $K \subseteq \mathbb{Q}(E[2])$, the function $\gamma(d)$ in the proof of Proposition 4.2.9 is 0. In particular, by Proposition 4.2.7, we have that the kth moments of $g(d)$ are bounded.

We have the following basic corollary showing that, for 100% of d, $\dim \mathrm{Sel}_2(E_d/K)$ is larger than any fixed integer whenever the 2-torsion of E field does not interact with K. This is in stark contrast with the situation for the Selmer groups $\mathrm{Sel}_2(E_d/\mathbb{Q})$, whose distribution is determined by Kane in [Kan13, Thm. 3].

Corollary 4.2.12. *If $K \cap \mathbb{Q}(E[2]) = \mathbb{Q}$, then for any $z \in \mathbb{R}$ we have*

$$\lim_{X\to\infty} \frac{\#\left\{|d| \leq X \text{ squarefree} \ : \ \dim(\mathrm{Sel}_2(E_d/K)) \leq z\right\}}{\#\left\{|d| \leq X \text{ squarefree}\right\}} = 0.$$

Proof. By Lemma 4.1.3 we have $\dim \mathrm{Sel}_2(E_d/K) \geq g(d) - 2$. The result now follows from Proposition 4.2.9. □

§ 4.3 | Main Results

Recall that $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ is a quadratic extension with $G = \mathrm{Gal}(K/\mathbb{Q})$. From this section onwards, we make the restriction that our choice of elliptic curve $E/\mathbb{Q}$ has $E[2] \subseteq E(\mathbb{Q})$.

For a squarefree integer d, a consequence of Lemmas 2.3.11 and 4.1.2 is that, roughly speaking, the auxiliary Selmer group $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ controls the discrepancy between $\dim \mathrm{Sel}_2(E_d/K)$ and the function $g(d)$ of Notation 4.2.6. Thus to improve on Proposition 4.2.9 and gain full control of the Selmer groups $\mathrm{Sel}_2(E_d/K)$ as d varies, it suffices to control these auxiliary groups. We achieve this under the assumption that all 2-torsion of E is defined over $\mathbb{Q}$. Specifically, across Sections 4.4 and 4.5 we will prove that, under this assumption, the Selmer group $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ is trivial for 100% of d. That is:

Theorem 4.3.1. *We have*

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree} \quad : \quad |d| < X,\ \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) = 0\}}{\#\{d \text{ squarefree} \quad : \quad |d| < X\}} = 1.$$

Remark 4.3.2. We will in fact show that the number of squarefree d with $|d| < X$ for which $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) \neq 0$ is $\ll X \log(X)^{-0.0394}$. See Theorem 4.5.1. It is likely that with more work this bound could be improved significantly, however we have not attempted to do so.

Remark 4.3.3. By Proposition 4.1.1 we have

$$\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) = \mathrm{Sel}_2(E_d/\mathbb{Q}) \cap \mathrm{Sel}_2(E_{d\theta}/\mathbb{Q})$$

where the intersection is taken inside $H^1(\mathbb{Q}, E[2])$. Thus Theorem 4.3.1 shows that for 100% of squarefree d, the groups $\mathrm{Sel}_2(E_d/\mathbb{Q})$ and $\mathrm{Sel}_2(E_{d\theta}/\mathbb{Q})$ share only the identity element.

Before embarking on the proof, we use the results of previous sections to draw several consequences of this theorem.

§ 4.3.1 | Statistical Results for 2-Selmer Groups

An immediate consequence of Theorem 4.3.1 is that the conclusion of Corollary 4.1.4 holds for 100% of squarefree d when we have full 2-torsion.

Corollary 4.3.4. *For* 100% *of squarefree d (ordered by absolute value), the* $\mathrm{Gal}(K/\mathbb{Q})$*-action on* $\mathrm{Sel}_2(E_d/K)$ *is trivial, and we have*

$$\dim \mathrm{Sel}_2(E_d/K) = -2 + \sum_{v \text{ place of } \mathbb{Q}} \dim E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E_d(K_w). \tag{4.1}$$

As a consequence, we can upgrade Proposition 4.2.9 to the following Erdős–Kac type result determining the distribution of the full 2-Selmer group.

Corollary 4.3.5. *The quantity*

$$\frac{\dim \mathrm{Sel}_2(E_d/K) - \log\log|d|}{\sqrt{2\log\log|d|}}$$

follows a standard normal distribution. That is, for every $z \in \mathbb{R}$ we have

$$\lim_{X\to\infty} \frac{\#\left\{|d| \le X \text{ squarefree } : \frac{\dim \mathrm{Sel}_2(E_d/K)-\log\log|d|}{\sqrt{2\log\log|d|}} \le z\right\}}{\#\left\{|d| \le X \text{ squarefree }\right\}} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-t^2/2}dt.$$

Proof. By Corollary 4.3.4, amongst all squarefree integers d with $|d| < X$, outside a set of cardinality $o(X)$ we have

$$\dim \mathrm{Sel}_2(E_d/K) = -2 + \sum_{v \text{ place of } \mathbb{Q}} \dim E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v}E_d(K_w) = g(d) - 2.$$

The result now follows from Proposition 4.2.9 noting that since $E[2] \subseteq E(\mathbb{Q})$, we have that $\delta_{E,K} = 1/2$. □

§ 4.3.2 | Statistical Results for Shafarevich–Tate Groups

A consequence of Corollary 4.3.5 is that $\dim \mathrm{Sel}_2(E_d/K)$ typically has size around $\log\log|d|$. By contrast, the dimensions of the 2-Selmer groups of the E_d over $\mathbb{Q}$ are known to be bounded on average thanks to a result of Kane [Kan13, Thm. 3]. In particular, the majority of $\dim \mathrm{Sel}_2(E_d/K)$ is attributable to the Shafarevich–Tate group. Formalising this observation allows us to prove the analogue of Corollary 4.3.5 for Shafarevich–Tate groups also.

Corollary 4.3.6. *Assume that E has no cyclic 4-isogeny defined over $\mathbb{Q}$. Then the quantity*

$$\frac{\dim Ш(E_d/K)[2] - \log\log|d|}{\sqrt{2\log\log|d|}}$$

follows a standard normal distribution. That is, for all $z \in \mathbb{R}$ we have

$$\lim_{X\to\infty} \frac{\#\left\{|d| \le X \text{ squarefree } : \frac{\dim Ш(E_d/K)[2]-\log\log|d|}{\sqrt{2\log\log|d|}} \le z\right\}}{\#\left\{|d| \le X \text{ squarefree}\right\}} = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-t^2/2}dt.$$

Proof. Since $\dim Ш(E_d/K)[2] \le \dim \mathrm{Sel}_2(E_d/K)$ for all d, by Corollary 4.3.5 we need only show that the limit in the statement (or more precisely the limit superior of the left hand side of the statement) is bounded above by $\Phi(z) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{z} e^{-t^2/2}dt$.

This follows from Corollary 4.3.5 thanks to [Kan13, Thm. 3], which gives adequate control of the Mordell–Weil component of $\mathrm{Sel}_2(E_d/K)$. First, for any squarefree integer

d, the standard short exact sequence

$$0 \longrightarrow E_d(K)/2E_d(K) \longrightarrow \mathrm{Sel}_2(E_d/K) \longrightarrow Ш(E_d/K)[2] \longrightarrow 0$$

gives

$$\dim Ш(E_d/K)[2] = \dim \mathrm{Sel}_2(E_d/K) - \dim E_d(K)/2E_d(K).$$

Since $K = \mathbb{Q}(\sqrt{\theta})$ and $\dim E_d(K)[2] = 2$ we have

$$\dim E_d(K)/2E_d(K) = 2 + \mathrm{rk}(E_d/\mathbb{Q}) + \mathrm{rk}(E_{d\theta}/\mathbb{Q}),$$

giving the equality

$$\dim Ш(E_d/K)[2] = \dim \mathrm{Sel}_2(E_d/K) - \mathrm{rk}(E_d/\mathbb{Q}) - \mathrm{rk}(E_{d\theta}/\mathbb{Q}) - 2.$$

Now fix a real number z and a positive real number M. Partitioning into cases according to

$$\mathrm{rk}(E_d/\mathbb{Q}) + \mathrm{rk}(E_{d\theta}/\mathbb{Q}) \leq M \quad \text{or} \quad \mathrm{rk}(E_d/\mathbb{Q}) + \mathrm{rk}(E_{d\theta}/\mathbb{Q}) > M$$

we find

$$\begin{aligned}
&\#\left\{|d| \leq X \text{ squarefree } : \frac{\dim Ш(E_d/K)[2] - \log\log|d|}{\sqrt{2\log\log|d|}} \leq z\right\} \\
&\leq \#\left\{|d| \leq X \text{ squarefree } : \frac{\dim \mathrm{Sel}_2(E_d/K) - \log\log|d|}{\sqrt{2\log\log|d|}} \leq z + \frac{M+2}{\sqrt{2\log\log|d|}}\right\} \\
&\quad + \#\left\{|d| \leq X \text{ squarefree } : \mathrm{Sel}_2(E_d/\mathbb{Q}) > M/2\right\} \\
&\quad + \#\left\{|d| \leq X \text{ squarefree } : \mathrm{Sel}_2((E_\theta)_d/\mathbb{Q}) > M/2\right\}.
\end{aligned}$$

Dividing through by the number of squarefree integers d with $|d| \leq X$, taking the limsup $X \to \infty$, and applying Kane's theorem [Kan13, Thm. 3] to both E and E_θ (since E has no cyclic 4-isogeny defined over $\mathbb{Q}$ the same is true for E_θ, allowing us to apply Kane's result without further assumptions), we find as a consequence of Corollary 4.3.5 that

$$\limsup_{X\to\infty} \frac{\#\left\{|d| \leq X \text{ squarefree } : \frac{\dim Ш(E_d/K)[2] - \log\log|d|}{\sqrt{2\log\log|d|}} \leq z\right\}}{\#\left\{|d| \leq X \text{ squarefree}\right\}} \leq \Phi(z) + 2\sum_{r \geq M/2} \alpha_r,$$

where the α_r are defined in Kane's Theorem 2. Since the α_r determine a probability distribution on the set of $r \in \mathbb{Z}_{\geq 0}$, taking the limit $M \to \infty$ gives the result. □

Remark 4.3.7. It seems reasonable to expect that Corollary 4.3.6 remains true without the assumption that E has no cyclic 4-isogeny defined over $\mathbb{Q}$. However, since no

analogue of Kane's result is known in this setting we have not been able to prove this.

§ 4.3.3 | Statistical Results for Mordell–Weil Groups

We now give some consequences for the Mordell–Weil groups of the E_d/K. We begin with the following algebraic results. Write $G = \mathrm{Gal}(K/\mathbb{Q})$. Recall that the Mordell–Weil lattice of E_d over a number field F is the free abelian group

$$\Lambda(E_d/F) := E_d(F)/E_d(F)_{\mathrm{tors}}.$$

We will, in particular, be interested in the structure of $\Lambda(E_d/K)$ as a $\mathbb{Z}[G]$-lattice.

For a G-module M, we denote by $M(-1)$ the G-module which is isomorphic to M as an abelian group but with G-action twisted by multiplication by -1. That is, the new G-action of the generator σ of G is given by

$$m \longmapsto -\sigma(m).$$

Lemma 4.3.8. *If* $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) = 0$ *then there is an isomorphism of* $\mathbb{Z}[G]$*-modules*

$$\Lambda(E_d/K) \cong \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1).$$

Proof. By [CR81, Theorem 34.31], there exist unique $a, b, c \in \mathbb{Z}_{\geq 0}$ such that

$$\Lambda(E_d/K) \cong \mathbb{Z}^a \oplus \mathbb{Z}(-1)^b \oplus \mathbb{Z}[G]^c,$$

where $\mathbb{Z}$ denotes a rank 1 free $\mathbb{Z}$-module with trivial G-action. Note that we have an inclusion of G-modules

$$\Lambda(E_d/K)/2\Lambda(E_d/K) \subseteq \mathrm{Sel}_2(E_d/K)/\delta(E_d[2]).$$

The right hand side has trivial G-action, as follows from the vanishing of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ combined with Corollary 4.1.4 (iii). Thus $\Lambda(E_d/K)/2\Lambda(E_d/K)$ has trivial G-action also. Thus, $c = 0$. Via the natural K-isomorphism $E_d \cong E_{d\theta}$, we can identify the points of $E_d(K)$ on which the generator of G acts as multiplication by -1 with $E_{d\theta}(\mathbb{Q})$. The result follows. □

Proposition 4.3.9. *Suppose we have* $E_d(K)_{\mathrm{tors}} = E_d[2]$ *and* $\mathrm{Sel}_{\mathscr{C}_d}(\mathbb{Q}, E_d[2]) = 0$*. Then there is an isomorphism of* $\mathbb{Z}[G]$*-modules*

$$E_d(K) \cong \mathbb{F}_2^2 \oplus \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1).$$

Proof. By Lemma 4.3.8 we must have

$$\Lambda(E_d/K) \cong \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1). \tag{4.2}$$

As a consequence, take $\mathcal{B}$ to be a $\mathbb{Z}$-basis for $\Lambda(E_d/K)$ such that for all $v \in \mathcal{B}$ we have $\sigma(v) \in \{v, -v\}$. Let $\tilde{\mathcal{B}}$ be a lift of $\mathcal{B}$ to $E_d(K)$. Note that $E_d(K)/2E_d(K)$ has a basis

comprising of the images of the elements of $\tilde{\mathcal{B}}$ and two linearly independent vectors from the submodule $E_d(K)_{\text{tors}} = E_d[2] \cong \mathbb{F}_2^2$.

For each $v \in \tilde{\mathcal{B}}$, we have $\sigma(v) = \pm v + u$ for some $u \in E_d[2]$. Since $\text{Sel}_{\mathscr{C}_d}(\mathbb{Q}, E_d[2]) = 0$, the G-action on $E_d(K)/2E_d(K)$ is trivial by Corollary 4.1.4(iii). In particular $\pm v + u = \sigma(v) \equiv v$ in $E_d(K)/2E_d(K)$, and so $u \in 2E_d(K)$. Since $E_d(K)$ has no 4–torsion, $u = 0$ and so $\sigma(v) = \pm v$. Thus the morphism of abelian groups $\Lambda(E_d/K) \to E_d(K)$ induced by the lift $\tilde{\mathcal{B}}$ of $\mathcal{B}$ is one of $\mathbb{Z}[G]$–modules, so we have

$$E_d(K) \cong E_d[2] \oplus \Lambda(E_d/K).$$

The result then follows from (4.2). □

Corollary 4.3.10. *For* 100% *of squarefree d, there is an isomorphism of $\mathbb{Z}[G]$-modules*

$$E_d(K) \cong \mathbb{F}_2^2 \oplus \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1). \tag{4.3}$$

More precisely, we have

$$\lim_{X\to\infty} \frac{\#\{d \text{ squarefree } \mid\ |d| < X,\ (4.3) \text{ holds}\}}{\#\{d \text{ squarefree } \mid\ |d| < X\}} = 1.$$

Proof. Note that for each odd prime p, at most 2 quadratic twists of E have rational p-torsion (otherwise E would have at least 3 dimensional p-torsion over a multiquadratic extension, which is impossible). In particular, for each odd prime p, only finitely many twists of E can have p-torsion over K. Consequently, by Mazur's torsion theorem [Maz77, Theorem 8], amongst squarefree integers d with $|d| < X$, outwith a finite set of d we have $E_d(K)_{\text{tors}} \subseteq E[2^\infty]$. Moreover, by Lemma 4.2.2, only finitely many quadratic twists have a point of order 4. The result now follows from Theorem 4.5.1 and Proposition 4.3.9. □

§ 4.4 | Explicit Local Conditions for Full 2-Torsion

In this section we make preparations for the proof of Theorem 4.3.1 by making the results of §4.1 explicit in the case that E has full rational 2-torsion.

Recall that $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ is a quadratic extension and $E/\mathbb{Q}$ is a fixed elliptic curve with $E[2] \subseteq E(\mathbb{Q})$. Further, we fix a Weierstrass equation

$$E/\mathbb{Q} : y^2 = (x - a_1)(x - a_2)(x - a_3) \tag{4.4}$$

for E where, without loss of generality, $a_1, a_2, a_3 \in \mathbb{Z}$. Set $\alpha = a_1 - a_2$, $\beta = a_1 - a_3$, and $\gamma = a_2 - a_3$. Note that the primes of bad reduction for E all divide $2\alpha\beta\gamma$, and that $E[2] = \{O, P_1, P_2, P_3\}$ where $P_i = (a_i, 0)$.

As in Notation 4.2.1 we fix a finite set Σ of places of $\mathbb{Q}$ containing the real place, the prime 2, all primes which ramify in $K/\mathbb{Q}$, and all primes at which E has bad reduction. Note in particular that Σ contains all primes dividing $2\alpha\beta\gamma$.

§ 4.4.1 | Quadratic Twists

Let d be a squarefree integer. The quadratic twist $E_d/\mathbb{Q}$ is given by the Weierstrass equation

$$E_d : y^2 = (x - da_1)(x - da_2)(x - da_3).$$

We have $E_d[2] = \{O, P_{1,d}, P_{2,d}, P_{3,d}\}$ where $P_{i,d} = (da_i, 0)$.

The following lemma describes the local conditions $\mathscr{C}_v(K/\mathbb{Q}; E_d)$ of Definition 2.2.1 at primes $p \notin \Sigma$. For a place v of $\mathbb{Q}$, we denote by $\delta_{d,v} : E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \hookrightarrow H^1(\mathbb{Q}_v, E_d[2])$ the coboundary map associated to the sequence (2.1) with $F = \mathbb{Q}$.

Lemma 4.4.1. *Let p be a prime with $p \notin \Sigma$. Then*

(i) if $p \nmid d$, we have

$$\mathscr{C}_p(K/\mathbb{Q}; E_d) = \mathscr{S}_p(\mathbb{Q}; E_d) = H^1_{\mathrm{nr}}(\mathbb{Q}_p, E_d[2]),$$

(ii) if $p \mid d$ is split in $K/\mathbb{Q}$, we have

$$\mathscr{C}_p(K/\mathbb{Q}; E_d) = \mathscr{S}_p(\mathbb{Q}; E_d) = \delta_{d,p}(E_d[2]),$$

(iii) if $p \mid d$ is inert in $K/\mathbb{Q}$, we have

$$\mathscr{C}_p(K/\mathbb{Q}; E_d) = 0.$$

Proof. Let $\mathfrak{p}$ be a prime of K lying over p. (i): By Lemma 4.2.3 we have an equality $N_{K_\mathfrak{p}/\mathbb{Q}_p} E_d(K_\mathfrak{p}) = E_d(\mathbb{Q}_p)$. The first equality in Proposition 4.1.1(ii) thus gives

$$\mathscr{C}(E_d/\mathbb{Q}_p) = \delta_p(E_d(\mathbb{Q}_p)) = \mathscr{S}(E_d/\mathbb{Q}_p).$$

The second equality follows from the fact that p is odd and E_d has good reduction at p.

(ii): when p splits in $K/\mathbb{Q}$ the local extension $K_\mathfrak{p}/\mathbb{Q}_p$ is trivial, so $\mathscr{C}(E_d/\mathbb{Q}_p) = \mathscr{S}(E_d/\mathbb{Q}_p)$ by definition. For the second equality, since $p \nmid 2\infty$, $\dim \mathscr{S}(E_d/\mathbb{Q}_p) = \dim E_d[2]$. In particular, it suffices to show that the restriction of $\delta_{d,p}$ to $E_d[2]$ is injective, which follows from Lemma 4.2.2.

(iii): by Lemma 4.2.3 and the fact that E has full 2-torsion, it follows from a dimension count that $N_{K_\mathfrak{p}/\mathbb{Q}_p} E(K_\mathfrak{p}) = 2E(\mathbb{Q}_p)$. The result now follows from Proposition 4.1.1. □

Remark 4.4.2. Taking orthogonal complements, the above result also determines the local groups $\mathscr{F}(E_d/\mathbb{Q}_p)$ for $p \notin \Sigma$.

§ 4.4.2 | Explicit Local Conditions

We now use the fact that E_d has full rational 2-torsion to give an explicit description of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ as a subgroup of $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$.

Let $\lambda_{i,d} : E_d[2] \to \boldsymbol{\mu}_2$ be the map $P \mapsto (P, P_{i,d})_{e_2}$, where $(\ ,\ )_{e_2} : E_d[2] \times E_d[2] \to \boldsymbol{\mu}_2$ is the Weil pairing. This induces an isomorphism

$$(\lambda_{1,d}, \lambda_{2,d}) : E_d[2] \xrightarrow{\sim} \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2.$$

Via this map, we identify $H^1(\mathbb{Q}, E_d[2])$ with $H^1(\mathbb{Q}, \boldsymbol{\mu}_2) \oplus H^1(\mathbb{Q}, \boldsymbol{\mu}_2) = (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$ (cf. Example 2.1.2). We similarly identify $H^1(\mathbb{Q}_v, E_d[2])$ with $(\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2})^2$ for each place v of $\mathbb{Q}$. In this description, for each place v of $\mathbb{Q}$, the local Tate pairing

$$\langle\ ,\ \rangle_v : H^1(\mathbb{Q}_v, E_d[2]) \times H^1(\mathbb{Q}_v, E_d[2]) \to \mathbb{Q}/\mathbb{Z}$$

becomes the pairing $(\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2})^2 \times (\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2})^2 \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \boldsymbol{\mu}_2$ given by

$$((x_1, x_2), (y_1, y_2)) \mapsto (x_1, y_2)_v (x_2, y_1)_v, \tag{4.5}$$

where $(\ ,\ )_v$ denotes the quadratic Hilbert symbol. The Kummer map

$$\delta_{d,v} : E_d(\mathbb{Q}_v)/2E_d(\mathbb{Q}_v) \hookrightarrow H^1(\mathbb{Q}_v, E_d[2]),$$

then becomes the map

$$(x, y) \longmapsto \begin{cases} (x - da_1, x - da_2) & x \notin \{da_1, da_2\}, \\ (\alpha\beta, d\alpha) & (x, y) = (da_1, 0), \\ (-d\alpha, -\alpha\gamma) & (x, y) = (da_2, 0). \end{cases} \tag{4.6}$$

See, for example, [Sil09, Proposition X.1.4].

§ 4.4.3 | The Group $\mathbf{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$

We now define a further Selmer structure, whose associated Selmer group contains $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ as a subgroup, and which admits a cleaner explicit description.

Definition 4.4.3. Define the Selmer structure $\widetilde{\mathscr{C}_d}$ for $E_d[2]$ (viewed as a $G_\mathbb{Q}$-module) via the local conditions

$$\widetilde{\mathscr{C}_{d,v}} = \begin{cases} \mathscr{C}_v(K/\mathbb{Q}; E_d) & v \notin \Sigma, \\ H^1(\mathbb{Q}_v, E[2]) & v \in \Sigma. \end{cases}$$

Denote by $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$ the associated Selmer group.

Note that by construction, $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$ contains $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ as a subgroup. In particular, if $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$ is trivial, then so is $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$. The advantage of considering $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$ is that now Lemma 4.4.1 describes all non-trivial Selmer conditions.

Notation 4.4.4. Write N for the squarefree product of all (finite) primes $p \in \Sigma$. Further, write $d = ad'd''$, where d' is the product of all primes $p \mid d$ such that both

$p \notin \Sigma$ and p splits in $K/\mathbb{Q}$, and d'' is the product of all primes $p \mid d$ such that both $p \notin \Sigma$ and p is inert in $K/\mathbb{Q}$.

For $d \in \mathbb{Z}$ squarefree, we identify $H^1(\mathbb{Q}, E_d[2])$ with $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$ as in §4.4.2, and further identify $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$ with the set of pairs of squarefree integers. For a prime p and an integer n coprime to p, we write $\left(\frac{n}{p}\right)$ for the Legendre symbol taking value 1 if n is a square modulo p, and -1 else.

Proposition 4.4.5. *With the notation and identifications of Notation 4.4.4, the Selmer group* $\mathrm{Sel}_{\widetilde{\mathscr{C}}_d}(\mathbb{Q}, E_d[2])$ *consists of pairs* (x_1, x_2) *of squarefree integers such that the following conditions all hold:*

(i) we have $x_i \mid Nd'$ *for* $i = 1, 2$,

(ii) we have $\left(\frac{x_i}{p}\right) = 1$ *for all* $p \mid d''$ *and for* $i = 1, 2$,

(iii) for all $p \mid d'$ *we have*

$$(x_1, d\alpha)_p (x_2, \alpha\beta)_p = 1 = (x_1, -\alpha\gamma)_p (x_2, -d\alpha)_p.$$

Proof. By Lemma 4.4.1 and the definition of the local groups $\widetilde{\mathscr{C}}(E_d/\mathbb{Q}_v)$, we have $\widetilde{\mathscr{C}}(E_d/\mathbb{Q}_p) = 0$ for all primes p with $p \notin \Sigma$ such that both $p \mid d$ and p is inert in $K/\mathbb{Q}$, and $\widetilde{\mathscr{C}}(E_d/\mathbb{Q}_p) = H^1_{\mathrm{nr}}(\mathbb{Q}_p, E_d[2])$ for each prime p such that both $p \notin \Sigma$ and $p \nmid d$. These conditions are equivalent to conditions (i) and (ii) in the statement. Since in the definition of $\mathrm{Sel}_{\widetilde{\mathscr{C}}_d}(\mathbb{Q}, E_d[2])$ there are no conditions imposed at primes $p \in \Sigma$, in light of Lemma 4.4.1(ii) it suffices to show that condition (iii) is equivalent to the condition that

$$(x_1, x_2) \in \mathscr{S}_p(\mathbb{Q}; E_d) = \delta_{d,p}(E_d[2])$$

for each prime $p \mid d$ such that both $p \notin \Sigma$ and p splits in $K/\mathbb{Q}$. Since $\mathscr{S}_p(\mathbb{Q}; E_d)$ is its own orthogonal complement under the local Tate pairing, (x_1, x_2) is in $\mathscr{S}_p(\mathbb{Q}; E_d)$ if and only if it pairs trivially with each element of $\delta_{d,p}(E_d[2])$. Now $P_{d,1} = (da_1, 0)$ and $P_{d,2} = (da_2, 0)$ is a basis for $E_d[2]$, and by (4.6) we have

$$\delta_{d,p}(P_{d,1}) = (\alpha\beta, d\alpha) \in \left(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\right)^2 \quad \text{and} \quad \delta_{d,p}(P_{d,2}) = (-d\alpha, -\alpha\gamma) \in \left(\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\right)^2.$$

By (4.5), (x_1, x_2) pairs trivially with both of these elements under the local Tate pairing at p if and only if

$$(x_1, d\alpha)_p (x_2, \alpha\beta)_p = 1 = (x_1, -\alpha\gamma)_p (x_2, -d\alpha)_p.$$

The result follows. □

§ 4.5 | Proof of Theorem 4.3.1

Recall that $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ is a quadratic extension with Galois group G, and $E/\mathbb{Q}$ is an elliptic curve over $\mathbb{Q}$ with $E[2] \subseteq E(\mathbb{Q})$, and given by a Weierstrass equation

$$E/\mathbb{Q} : y^2 = (x - a_1)(x - a_2)(x - a_3) \tag{4.7}$$

for $a_1, a_2, a_3 \in \mathbb{Z}$. Recall also that we have defined integers $\alpha = a_1 - a_2$, $\beta = a_1 - a_3$, and $\gamma = a_2 - a_3$, and that the integer N is taken to be the product of all primes in the set Σ of Notation 4.2.1.

The aim of this section is to prove Theorem 4.3.1. Specifically, we will show the following, strictly stronger, result.

Theorem 4.5.1. *We have*

$$\#\{d \text{ squarefree} : \ |d| < X, \ \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) \neq 0\} \ll X \log(X)^{-0.0394}.$$

In particular

$$\lim_{X \to \infty} \frac{\#\{d \text{ squarefree} : \ |d| < X, \ \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2]) = 0\}}{\#\{d \text{ squarefree} : \ |d| < X\}} = 1.$$

§ 4.5.1 | First Reduction

In order to prove Theorem 4.5.1 it suffices to replace $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ with the slightly larger group $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$ (cf. Definition 4.4.3) in place of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$, since the latter is a subgroup of the former. We begin by defining a further group S_d determined by simpler local conditions. Specifically, we wish to 'decouple' the variables x_1 and x_2 appearing in Proposition 4.4.5. We first introduce some notation.

Notation 4.5.2. We introduce the following 3 sets of primes:

$$\mathcal{P}_0 := \{p \notin \Sigma, \ \ p \text{ split in } K/\mathbb{Q}, \text{ and } p \text{ non-split } \mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}\},$$

$$\mathcal{P}_1 := \{p \notin \Sigma, \ \ p \text{ split in } K/\mathbb{Q}, \text{ and } p \text{ split in } \mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}\},$$

$$\mathcal{P}_2 := \{p \notin \Sigma, \ \ p \text{ inert in } K/\mathbb{Q}\}.$$

(If $\alpha\beta$ is a square in $\mathbb{Q}$ we take $\mathcal{P}_0 := \emptyset$ and $\mathcal{P}_1$ the collection of primes not in Σ which split in $K/\mathbb{Q}$.) Note that the sets $\Sigma, \mathcal{P}_0, \mathcal{P}_1$ and $\mathcal{P}_2$ give a partition of the set of all primes into 4 pairwise disjoint subsets.

For $i = 0, 1, 2$, we define $\mathcal{F}_i$ to be the set of positive squarefree integers n all of whose prime factors lie in $\mathcal{P}_i$. Note that for $i \neq j$ we have $\mathcal{F}_i \cap \mathcal{F}_j = \{1\}$. We write $\mathcal{F}_i \cdot \mathcal{F}_j$ for the collection of squarefree integers n which can be written as a product $n = n_i n_j$ for some $n_i \in \mathcal{F}_i$ and $n_j \in \mathcal{F}_j$. Note that such a decomposition is necessarily unique.

Remark 4.5.3. Note that provided $\mathbb{Q}(\sqrt{\alpha\beta}) \not\subseteq K$, $\mathcal{P}_0$ and $\mathcal{P}_1$ have Dirichlet density 1/4, and $\mathcal{P}_2$ has density 1/2. If $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$ then $\mathcal{P}_0 = \emptyset$ and $\mathcal{P}_1$ and $\mathcal{P}_2$ both have Dirichlet density 1/2.

Definition 4.5.4. For d a squarefree integer, define the subgroup S_d of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ as follows. First, write (uniquely) $d = ad_0d_1d_2$ where $a \mid N$, $d_0 \in \mathcal{F}_0$, $d_1 \in \mathcal{F}_1$, and $d_2 \in \mathcal{F}_2$. Now define S_d to be the set of squarefree integers

$$S_d := \left\{ x \text{ sq. free} \ : \ \begin{smallmatrix} x \mid Nd_0d_1, \\ \left(\frac{x}{p}\right)=1 \text{ for all } p \mid d_2, \\ (x, d\alpha)_p = 1 \text{ for all } p \mid d_1. \end{smallmatrix} \right\}.$$

We allow x to be either positive or negative.

Lemma 4.5.5. *If a pair of squarefree integers (x_1, x_2) is in $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$, then $x_1 \in S_d$.*

Proof. Immediate from Proposition 4.4.5, noting that for $p \mid d_1$, since p is split in $\mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}$ by assumption, the condition $(x_1, d\alpha)_p(x_2, \alpha\beta)_p = 1$ is equivalent to having $(x_1, d\alpha)_p = 1$. □

We will show the following. As explained below, this is sufficient to prove Theorem 4.5.1.

Theorem 4.5.6. *We have*

$$\#\{d \text{ squarefree} \ \mid \ |d| < X, \ S_d \neq 0\} \ll X\log(X)^{-0.0394}.$$

Proof of Theorem 4.5.1 assuming Theorem 4.5.6. By Combining Theorem 4.5.6 with Lemma 4.5.5 we obtain that the x_1-coordinate of any element of $\mathrm{Sel}_{\widetilde{\mathscr{C}_d}}(\mathbb{Q}, E_d[2])$ is trivial for 100% of squarefree d. By symmetry, the same must then be true of the x_2-coordinate since we can relabel a_1 and a_2 in the equation (4.4) for our elliptic curve in order to interchange the roles of x_1 and x_2. This shows the limit statement of Theorem 4.5.1, and running the same argument but keeping track of error terms proves the general result. □

We now begin preparations for the proof of Theorem 4.5.6.

§ 4.5.2 | Notation and Preparations

Notation 4.5.7. Given a positive integer n we write $\omega(n)$ for the number of distinct prime factors of n. For $i = 0, 1, 2$ we write $\omega_i(n)$ for the number of distinct prime factors of n which lie in $\mathcal{P}_i$. We denote by μ the Möbius function.

We will use frequently the following lemma controlling generalised divisor sums.

Lemma 4.5.8. *Let a_0, a_1, and a_2 be non-negative real numbers. Then we have*

$$\sum_{\substack{X-Y<n\leq X \\ n \text{ sq. free}}} a_0^{\omega_0(n)} a_1^{\omega_1(n)} a_2^{\omega_2(n)} \ll \begin{cases} Y\log(X)^{\frac{a_0}{4}+\frac{a_1}{4}+\frac{a_2}{2}-1} & \mathbb{Q}(\sqrt{\alpha\beta}) \not\subseteq K, \\ Y\log(X)^{\frac{a_1}{2}+\frac{a_2}{2}-1} & \mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K, \end{cases}$$

uniformly for $2 \leq X\exp(-\sqrt{\log(X)}) \leq Y \leq X$.

Proof. This follows from a (significantly more general) result of Shiu [Shi80]. Define the multiplicative function $f : \mathbb{Z}_{>0} \to \mathbb{R}_{\geq 0}$ by setting, for any $k \geq 1$, $f(p^k) = a_i$ for $p \in \mathcal{P}_i$ $(i = 0, 1, 2)$, and taking $f(p) = 1$ for $p \in \Sigma$. We then wish to bound the sum $\sum_{X-Y<n\leq X} f(n)$. It follows from Remark 4.5.3, and the explicit form of the Chebotarev density theorem given in [LO77], that we have

$$\sum_{p\leq X} \frac{f(p)}{p} = \begin{cases} \left(\frac{a_0}{4} + \frac{a_1}{4} + \frac{a_2}{2}\right)\log\log(X) + O(1) & \text{if } \mathbb{Q}(\sqrt{\alpha\beta}) \subsetneq K, \\ \left(\frac{a_1}{2} + \frac{a_2}{2}\right)\log\log(X) + O(1) & \text{if } \mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K. \end{cases}$$

The result now follows from [Shi80, Theorem 1] (the conditions (i) and (ii) needed for that theorem follow in our setting from well known bounds on the divisor function). □

§ 4.5.3 | Reduction to Computing a Weighted Average

In order to prove Theorem 4.5.6 we will compute bounds for a certain weighted average of $\#(S_d \setminus \{1\})$. Specifically will we prove:

Proposition 4.5.9. *For any* $1 < \gamma < 7/8 + \sqrt{17}/8 = 1.3903...$*, we have*

$$\sum_{|d|<X,\ d \text{ sq. free}} \gamma^{\omega_2(d)-\omega_0(d)}(\#S_d - 1) = o(X). \tag{4.8}$$

Moreover, for $\gamma = 1/4 + \sqrt{17}/4$ *the left hand side of (4.8) is* $\ll X\log(X)^{-0.0394}$.

We begin by showing that this is sufficient to prove Theorem 4.5.6.

Proof of Theorem 4.5.6 assuming Proposition 4.5.9. We first show that the weights are at least 1 for 100% of squarefree d. That is, we claim that

$$\#\{d \text{ squarefree } \mid |d| \leq X,\ \omega_0(d) \geq \omega_2(d)\} \ll X\log(X)^{-0.042}.$$

To see this, fixing any $\lambda > 1$ we have

$$\#\{d \text{ squarefree } \mid |d| \leq X,\ \omega_0(d) \geq \omega_2(d)\} \leq 2\sum_{1\leq d\leq X} \lambda^{\omega_0(d)-\omega_2(d)}.$$

By Lemma 4.5.8 the right hand side is $\ll X\log(X)^{\lambda/4+1/(2\lambda)-3/4}$. Optimising over λ we find that when $\lambda = \sqrt{2}$ the exponent is $1/\sqrt{2} - 3/4 < -0.042$, giving the claim.

Now fix $1 < \gamma < 7/8 + \sqrt{17}/8$. By the claim we have

$$\begin{aligned} \#\left\{|d| \leq X \;\middle|\; S_d \neq 0\right\} &\leq \#\left\{|d| \leq X \;\middle|\; \omega_0(d) \geq \omega_2(d)\right\} + \\ &\quad \#\left\{|d| \leq X \;\middle|\; S_d \neq 0,\ \omega_2(d) > \omega_0(d)\right\} \\ &\ll X\log(X)^{-0.042} + \sum_{|d|\leq X} \gamma^{\omega_2(d)-\omega_0(d)}(\#S_d - 1) \end{aligned}$$

where above d is implicitly taken squarefree. The result now follows from Proposition 4.5.9. □

Remark 4.5.10. The reason for the introduction of the weight γ is that, in passing from the group $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ to the group S_d, we have thrown away the Selmer conditions coming from primes in $\mathcal{P}_0$ in favour of reducing the number of variables involved. This leads to twists having an abnormally large number of prime factors lying in $\mathcal{P}_0$ contributing a disproportionate amount to the average size of S_d. The weight γ is introduced to compensate for this.

§ 4.5.4 | Strategy of the Proof of Proposition 4.5.9

The proof of Proposition 4.5.9 follows closely the argument of [FK07, §5], which has its origins in the work of Heath-Brown [HB93, HB94]. There, Fouvry–Klüners determine asymptotics for the moments of 4-ranks of class groups of quadratic fields. Our first step is to express the sum in Proposition 4.5.9 as a sum of Jacobi symbols. We do this in Lemma 4.5.12 below, using ideas from [FK07, Lemma 16]. The resulting sum, given in (4.13), is structurally similar to the one in [FK07, Lemma 17]. We then adapt the techniques used by Fouvry–Klüners to bound this sum. There are a couple of points at which the argument we give diverges from that of Fouvry–Klüners. First, whilst they compute higher moments of the sizes of class groups, we need only compute a (weighted version of) the first moment of the size of S_d. Thus the intricate study of 'maximal unlinked subsets' undertaken in [FK07, §5.6] can be avoided. On the other had, the variables D_i in [FK07, §5] are allowed to vary over all positive squarefree integers, whilst ours are constrained to lie in the thin families $\mathcal{F}_j$. This necessitates changes to the argument in Fouvry–Klüners' first and fourth families, which correspond to our 'remaining families' and 'third family' respectively, below.

§ 4.5.5 | Expressing the Sum in Terms of Jacobi Symbols

We now begin preparations for the proof of Proposition 4.5.9 by expressing the relevant sum in terms of Jacobi symbols. We first define the following sums which will be ubiquitous in what follows.

Definition 4.5.11. Let λ and η be squarefree divisors (either positive or negative) of N. For a tuple $(D_i)_{0\leq i\leq 7}$ of coprime positive integers, write

$$\begin{aligned}\mathcal{J}_{\eta,\lambda}((D_i)_{0\leq i\leq 7}) \;:=\; &\left(\frac{\eta}{D_2}\right)\left(\frac{\lambda}{D_4}\right)\left(\frac{\lambda}{D_6}\right)\left(\frac{D_4}{D_2}\right)\left(\frac{D_2}{D_4}\right)\left(\frac{D_6}{D_2}\right)\left(\frac{D_2}{D_6}\right)\\ &\times\left(\frac{D_1}{D_2}\right)\left(\frac{D_5}{D_2}\right)\left(\frac{D_7}{D_2}\right)\left(\frac{D_0}{D_4}\right)\left(\frac{D_3}{D_4}\right)\left(\frac{D_0}{D_6}\right)\left(\frac{D_3}{D_6}\right).\end{aligned}$$

Now for any real number $X > 1$, and any positive real γ, define

$$\mathcal{S}_\gamma(\lambda,\eta,X) := \sum_{\substack{D_0,D_1\in\mathcal{F}_0\\ D_2,D_3,D_4,D_5\in\mathcal{F}_1\\ D_6,D_7\in\mathcal{F}_2\\ \prod_i D_i\leq X\\ D_i \text{ coprime}}} \gamma^{-\omega(D_0D_1)}2^{-\omega(D_2D_3D_4D_5)}(2/\gamma)^{-\omega(D_6D_7)}\mathcal{J}_{\eta,\lambda}((D_i)_{0\leq i\leq 7}),$$

with the additional condition that, if $\lambda = 1$, then not all of D_0, D_2 and D_3 are equal

to 1 in the range of summation.

Lemma 4.5.12. *For any positive real number γ we have*

$$\sum_{|d|<X,\ d \text{ sq. free}} \gamma^{\omega_2(d)-\omega_0(d)}(\#S_d - 1) = \sum_{a|N} \sum_{x_N|N} \mathcal{S}_\gamma(x_N, -ax_N\alpha, X/a) \tag{4.9}$$

where the right hand sums run over both positive and negative divisors of N.

Proof. Fix d squarefree. As in Definition 4.5.4 we write $d = ad_0d_1d_2$ where $d_i \in \mathcal{F}_i$ for $i = 0, 1, 2$, so that

$$S_d = \left\{ x \text{ sq. free} \ : \ \begin{smallmatrix} x|Nd_0d_1, \\ \left(\frac{x}{p}\right)=1 \text{ for all } p|d_2, \\ (x,d\alpha)_p=1 \text{ for all } p|d_1. \end{smallmatrix} \right\}.$$

Now fix $x \mid Nd_0d_1$ and note that we have

$$2^{-\omega(d_2)} \sum_{z_2|d_2} \left(\frac{x}{z_2}\right) = 2^{-\omega(d_2)} \prod_{p|d_2} \left(1 + \left(\frac{x}{p}\right)\right) = \begin{cases} 1 & \left(\frac{x}{p}\right) = 1 \ \text{ for all } p \mid d_2 \\ 0 & \text{else,} \end{cases} \tag{4.10}$$

where in the sum above z_2 runs over all *positive* divisors of d_2.

To deal with the conditions at primes dividing d_1, we write x uniquely as $x = x_N x_0 x_1$ where $x_N \mid N$ (and may be negative) $x_0 \mid d_0$ and $x_1 \mid d_1$. Say $d_0 = x_0y_0$ and $d_1 = x_1y_1$. Then for $p \mid d_1$, we have (noting that d_1 and α are coprime and that all $p \mid d_1$ are odd)

$$(x, d\alpha)_p = \begin{cases} \left(\frac{x}{p}\right) & p \mid y_1 \\ (x, -xd\alpha)_p = \left(\frac{-ax_Ny_0y_1d_2\alpha}{p}\right) & p \mid x_1. \end{cases}$$

Thus, similarly to (4.10), we have

$$2^{-\omega(x_1y_1)} \sum_{\substack{w_1|x_1 \\ z_1|y_1}} \left(\frac{x}{z_1}\right) \left(\frac{-ax_Ny_0y_1d_2\alpha}{w_1}\right) = \begin{cases} 1 & (x, d\alpha)_p = 1 \ \text{ for all } p \mid d_1 \\ 0 & \text{else.} \end{cases} \tag{4.11}$$

We now multiply (4.10) and (4.11), write $d_2 = z_2z_2'$, $x_1 = w_1w_1'$, and $y_1 = z_1z_1'$, and sum over all $x = x_Nx_0x_1$ dividing Nd_0d_1 to find that $\#S_d$ is equal to

$$\sum_{x_N|N} \sum_{\substack{x_0y_0=d_0 \\ w_1w_1'z_1z_1'=d_1 \\ z_2z_2'=d_2}} 2^{-\omega(w_1w_1'z_1z_1'z_2z_2')} \left(\frac{x_Nx_0w_1w_1'}{z_2}\right) \left(\frac{x_Nx_0w_1w_1'}{z_1}\right) \left(\frac{-ax_Ny_0z_1z_1'z_2z_2'\alpha}{w_1}\right)$$

where x_N may be negative but all other variables are positive and coprime. Note that we necessarily have $x_0, y_0 \in \mathcal{F}_0$, $w_1, w_1', z_1, z_1' \in \mathcal{F}_1$ and $z_2, z_2' \in \mathcal{F}_2$, so that in particular $\omega_0(d) = \omega(x_0y_0)$ and $\omega_2(d) = \omega(z_2z_2')$. Moreover, the identity element in S_d corresponds to $x_N = x_0 = w_1 = w_1' = 1$, so that restricting the range of summation so that not all of these variables are 1 counts $\#S_d - 1$ instead. To conclude we sum the resulting expression for $\#S_d - 1$ over all squarefree $d = ad_0d_1d_2$ with $|d| \le X$, weighted by $\gamma^{\omega_2(d)-\omega_0(d)}$, and relabel variables $(x_0, y_0, w_1, w_1', z_1, z_1', z_2, z_2') = (D_0, D_1, D_2, D_3, D_4, D_5, D_6, D_7)$. □

Remark 4.5.13. The proof above shows that the reason for excluding the terms where $\lambda = D_0 = D_2 = D_3 = 1$ in the definition of $\mathcal{S}_\gamma(\lambda, \eta, X)$ above is to remove the identity element of S_d from the count.

Now fix $1 < \gamma < 7/8 + \sqrt{17}/8$ as in the statement of Proposition 4.5.9 . In light of Lemma 4.5.12 we want to study the sums $\mathcal{S}_\gamma(\lambda, \eta, X)$.

Definition 4.5.14. As a book-keeping device, we define the function $\Phi(i, j)$ $(0 \leq i \neq j \leq 7)$ by setting $\Phi(i, j) = 1$ if the Jacobi symbol $\left(\frac{D_i}{D_j}\right)$ appears in the definition of $\mathcal{J}_{\eta,\lambda}((D_i)_{0\leq i\leq 7})$, and 0 else. We say that two indices i and j are *linked* if $\Phi(i, j) + \Phi(j, i) = 1$.

Note that the sets of linked indices are

$$\{1, 2\}, \{2, 5\}, \{2, 7\}, \{0, 4\}, \{3, 4\}, \{0, 6\}, \{3, 6\}. \tag{4.12}$$

Notation 4.5.15. To write the sums $\mathcal{S}_\gamma(\lambda, \eta, X)$ in a manageable way, set μ_i to be 1 if $\left(\frac{\eta}{D_i}\right)$ appears in $\mathcal{J}_{\eta,\lambda}((D_i)_{0\leq i\leq 7})$ and 0 else, and set ν_i to be 1 if $\left(\frac{\lambda}{D_i}\right)$ appears in $\mathcal{J}_{\eta,\lambda}((D_i)_{0\leq i\leq 7})$ and 0 else. Further, define

$$\kappa_i := \begin{cases} \gamma & i = 0, 1 \\ 2 & i = 2, 3, 4, 5 \\ \frac{2}{\gamma} & i = 6, 7. \end{cases}$$

Finally, we let $\mathscr{D}(X)$ denote the set of tuples of pairwise coprime positive integers $(D_0, ..., D_7)$ such that all of the following hold:

- we have $D_0, D_1 \in \mathcal{F}_0$, $D_2, D_3, D_4, D_5 \in \mathcal{F}_1$, and $D_6, D_7 \in \mathcal{F}_2$,
- we have $\prod_{i=0}^{7} D_i \leq X$,
- if $\lambda = 1$, then D_0, D_2 and D_3 are not all 1.

We thus write

$$\mathcal{S}_\gamma(\lambda, \eta, X) = \sum_{(D_i)\in\mathscr{D}(X)} \prod_i \kappa_i^{-\omega(D_i)} \prod_i \left(\frac{\eta}{D_i}\right)^{\mu_i} \left(\frac{\lambda}{D_i}\right)^{\nu_i} \prod_{i\neq j} \left(\frac{D_i}{D_j}\right)^{\Phi(i,j)}. \tag{4.13}$$

We also define n_i $(0 \leq i \leq 7)$ so that the D_i are required to lie in $\mathcal{F}_{n_i}$ (e.g. $n_0 = n_1 = 0$).

§ 4.5.6 | Bounds on the Sums $\mathcal{S}_\gamma(\lambda, \eta, X)$

Proposition 4.5.16. *For any $1 < \gamma < 7/8 + \sqrt{17}/8$, and for any (positive or negative) divisors λ and η of N, we have $\mathcal{S}_\gamma(\lambda, \eta, X) = o(X)$. Moreover, when $\gamma = 1/4 + \sqrt{17}/4$ we have*

$$\mathcal{S}_\gamma(\lambda, \eta, X) \ll X \log(X)^{-0.0394}.$$

It's immediate from Lemma 4.5.12 that Proposition 4.5.16 implies Proposition 4.5.9 and so, via Theorem 4.5.6, we obtain Theorem 4.5.1. The rest of the section is occupied with the proof of Proposition 4.5.16.

The contribution from $D_0, D_2, D_3 = 1$ and $\lambda = \theta$

Recall that $K = \mathbb{Q}(\sqrt{\theta})$ for some squarefree integer θ (necessarily dividing N). We first show that the contribution to $\mathcal{S}_\gamma(\theta, \eta, X)$ coming from $D_0 = D_2 = D_3 = 1$ is negligible, since leaving this in would prevent a uniform argument at a later point. Note that when $D_0 = D_2 = D_3 = 1$ all Jacobi symbols appearing in (4.13) are equal to 1 except those that involve $\lambda = \theta$. Moreover, since elements of $\mathcal{F}_2$ are products of primes inert in K, any $n \in \mathcal{F}_2$ has $\left(\frac{\theta}{n}\right) = \mu(n)$. On the other hand, we similarly have $\left(\frac{\theta}{n}\right) = 1$ for all $n \in \mathcal{F}_1$. Consequently, the contribution to $\mathcal{S}_\gamma(\theta, \eta, X)$ from tuples with $D_0 = D_2 = D_3 = 1$ is given by

$$\sum_{\substack{(D_i)\in\mathscr{D}(X)\\ D_0,D_2,D_3=1}} \mu(D_6) \prod_{i\neq 0,2,3} \kappa_i^{-\omega(D_i)} = \sum_{\substack{r\in\mathcal{F}_0\cdot\mathcal{F}_1\\ r\leq X}} \gamma^{-\omega_0(r)} \sum_{\substack{n\in\mathcal{F}_2\\ n\leq X/r}} \gamma^{\omega(n)} \sum_{m|n} \mu(m). \tag{4.14}$$

In the above, to pass from the left hand side to the right hand side we have set $r = D_1D_4D_5$ and $n = D_6D_7$, noting that e.g. given $r \in \mathcal{F}_0 \cdot \mathcal{F}_1$ there are $2^{\omega_1(r)}$ ways or writing r as a product $D_1D_4D_5$ where $D_1 \in \mathcal{F}_0$ and $D_4, D_5 \in \mathcal{F}_1$, and that this multiplicity cancels the contribution of $\kappa_4^{-\omega(D_4)}\kappa_5^{-\omega(D_5)}$. Now since $\sum_{m|n} \mu(m)$ is equal to 0 if $n > 1$, and 1 if $n = 1$, we find

$$|\text{RHS of (4.14)}| = \sum_{\substack{r\in\mathcal{F}_0\cdot\mathcal{F}_1\\ r\leq X}} \gamma^{-\omega_0(r)} \ll X \log(X)^{-1/2} \tag{4.15}$$

where for the bound we are using Lemma 4.5.8.

Number of prime factors of the variables

We now show that the contribution coming from D_i with a large number of prime factors is negligible. This will be important for dealing with our third family below. Set $\Omega = 4e \cdot (\log\log(X) + B_0)$ with B_0 as in [FK07, Lemma 11], and let Σ_1 be the contribution to $\mathcal{S}_\gamma(\lambda, \eta, X)$ from the tuples $(D_i) \in \mathscr{D}(X)$ satisfying

$$\omega(D_i) \geq \Omega \quad \text{for some } 0 \leq i \leq 7. \tag{4.16}$$

Writing $n = \prod_i D_i$ we have

$$\begin{aligned} |\Sigma_1| &\ll \sum_{\substack{n\leq X\\ \omega(n)\geq\Omega}} \frac{2^{\omega_0(n)}4^{\omega_1(n)}2^{\omega_2(n)}}{\gamma^{\omega_0(n)}2^{\omega_1(n)}(2/\gamma)^{\omega_2(n)}}\mu^2(n) \\ &\ll \sum_{\substack{n\leq X\\ \omega(n)\geq\Omega}} \mu^2(n)2^{\omega(n)}. \end{aligned}$$

Applying the Cauchy–Schwarz inequality and arguing using [HR00, Lemma A] as in [FK07, §5.3] (paragraph above Equation (30)) we find $\Sigma_1 \ll X \log(X)^{-1}$.

Ranges of the variables

We now divide the ranges of summation into intervals, and treat these intervals separately. Specifically, we set

$$\Delta := 1 + \frac{1}{\log(X)^2} \tag{4.17}$$

and divide the ranges of the variables into intervals $[\Delta^n, \Delta^{n+1}]$ for $n = 0, 1, 2, ...$, noting that 1 is the only integer in the $n = 0$ interval. For $i = 0, ..., 7$ we let A_i denote a number of the form Δ^n with $1 \leq \Delta^n \leq X$, let $\mathbf{A} = (A_i)_{0 \leq i \leq 7}$, and define

$$\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A}) = \sum_{\substack{(D_i) \in \mathscr{D}'(X) \\ A_i \leq D_i \leq \Delta A}} \prod_i \kappa_i^{-\omega(D_i)} \prod_i \left(\frac{\eta}{D_i}\right)^{\mu_i} \left(\frac{\lambda}{D_i}\right)^{\nu_i} \prod_{i \neq j} \left(\frac{D_i}{D_j}\right)^{\Phi(i,j)}, \tag{4.18}$$

where, in light of there being negligible contribution from D_i with a large number of prime factors, and (4.15), we define $\mathscr{D}'(X)$ to be the subset of $\mathscr{D}(X)$ consisting of tuples $(D_i)_i$ such that $\omega(D_i) \leq \Omega$ for each i, and such that, if $\lambda = \theta$, then not all of D_0, D_2 and D_3 are equal to 1. Since for α small positive we have $\log(1 + \alpha) \approx \alpha$, for X large $\log(X)/\log(\Delta) \approx \log(X)^3$, so there are order $\log(X)^{24}$ expressions (4.18) as $\mathbf{A}$ varies.

Following [FK07, §5.4] we split the collection of all $\mathbf{A}$ into families and treat each in turn.

First family: $\prod_i A_i$ large.

In order to exploit oscillations of the Jacobi symbols it will be necessary to allow the variables D_i to range (essentially) freely in the interval $[A_i, \Delta A_i]$. To this end, we first deal with the case where the product of the A_i is large, where the condition $\Pi_i D_i \leq X$ is relevant. Specifically, the first family of the $\mathbf{A}$ is defined by the condition

$$\prod_{0 \leq i \leq 7} A_i \geq \Delta^{-8} X. \tag{4.19}$$

The argument here is essentially identical to that occurring between Equations (33) and (34) of [FK07]: we have

$$\begin{aligned}
\sum_{\mathbf{A} \text{ satisfies (4.19)}} |\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| &\leq \sum_{\mathbf{A} \text{ satisfies (4.19)}} \sum_{\substack{(D_i) \in \mathscr{D}'(X) \\ A_i \leq D_i \leq \Delta A_i}} \prod_i \kappa_i^{-\omega(D_i)} \\
&\leq \sum_{\Delta^{-8} X \leq n \leq X} 2^{\omega(n)} \\
&\ll (1 - \Delta^{-8}) X \log(X) \\
&\ll X \log(X)^{-1}
\end{aligned}$$

where for the last inequality we are using that

$$1 - \Delta^{-8} = 1 - (1 + \log(X)^{-2})^{-8} = 1 - (1 - 8\log(X)^{-2} + O(\log(X)^{-4})) \ll \log(X)^{-2}.$$

Note that if $\mathbf{A}$ does not satisfy (4.19) then the condition $\prod_i D_i \leq X$ is made automatic by the restrictions on the intervals the D_i lie in, and may henceforth be dropped.

Second family: two large factors corresponding to linked indices

We introduce the parameter $X^\dagger := \log(X)^{78}$, and consider the $\mathbf{A}$ such that

$$\prod_{0\leq k\leq 7} A_k \leq \Delta^{-8}X, \text{ and there exist linked indices } i \neq j \text{ with } A_i, A_j \geq X^\dagger. \tag{4.20}$$

Here the argument is almost identical to that given between Equations (40) and (42) in [FK07], ultimately relying on a result of Heath-Brown exploiting double oscillations of characters [HB95, Corollary 4]. For such $\mathbf{A}$, since i and j are linked we have (swapping i and j if necessary)

$$\begin{aligned}&|\mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A})|\\ &\ll \sum_{\substack{A_k\leq D_k\leq \Delta A_k\\ k\neq i,j}} \prod_{k\neq i,j} \kappa_k^{-\omega(D_k)} \Big| \sum_{\substack{1\leq D_i\leq \Delta A_i\\ 1\leq D_j\leq \Delta A_j}} f(D_i;(D_k)_{k\neq i,j}) g(D_j;(D_k)_{k\neq i,j}) \left(\frac{D_i}{D_j}\right)\Big|,\end{aligned}$$

where in the inner sum D_i and D_j are odd coprime integers with no further constraints,

$$f(D_i;(D_k)_{k\neq i,j}) = \mathbb{1}_{\substack{D_i\in\mathcal{F}_{n_i},\\ D_i\geq A_i,\\ \omega(D_i)\leq\Omega}} \cdot \kappa_i^{-\omega(D_i)} \left(\frac{\eta}{D_i}\right)^{\mu_i} \left(\frac{\lambda}{D_i}\right)^{\nu_i} \prod_{k\neq i,j} \left(\frac{D_i}{D_k}\right)^{\Phi(i,k)} \left(\frac{D_k}{D_i}\right)^{\Phi(k,i)}$$

and $g(D_j;(D_k)_{k\neq i,j})$ is defined in the same way but with i and j switched. The coefficients $f(D_i;(D_k)_{k\neq i,j})$ and $g(D_j;(D_k)_{k\neq i,j})$ are complex numbers with absolute value < 1, so applying [FK07, Lemma 15] (with $\varepsilon = 1/6$) to the inner sum above gives

$$|\mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A})| \ll \frac{A_iA_j}{\log(X)^{26}} \sum_{\substack{A_k\leq D_k\leq \Delta A_k\\ k\neq i,j}} \prod_{k\neq i,j} \kappa_k^{-\omega(D_k)} \leq \frac{A_iA_j}{\log(X)^{26}} \sum_{n\leq \Delta^6} \frac{2^{\omega(n)}}{\prod_{k\neq i,j} A_k}. \tag{4.21}$$

Since $\prod_i A_i \leq \Delta^{-8}X$ this gives

$$|\mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A})| \ll \frac{X}{\log(X)^{25}}. \tag{4.22}$$

Summing over each of the $\ll \log(X)^{24}$ possibilities for $\mathbf{A}$ we find

$$\sum_{\mathbf{A} \text{ satisfies (4.20)}} |\mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A})| \ll X\log(X)^{-1}. \tag{4.23}$$

Third family: one large and one small factor corresponding to linked indices

We introduce a further parameter $X^\ddagger = \exp(\log(X)^\varepsilon)$ for fixed $\varepsilon > 0$ (to be chosen later). Note that for X sufficiently large we have $X^\ddagger > X^\dagger$. The family of $\mathbf{A}$ we now

consider is given by

$$\text{Neither (4.19) nor (4.20) hold, and } \exists\ i \neq j \text{ linked with } 1 < A_j < X^{\dagger} \text{ and } A_i \geq X^{\ddagger}. \tag{4.24}$$

This section of the argument corresponds to the treatment of Fouvry–Klüners fourth family [FK07, Equations (43) to (47)], and we similarly obtain cancellation from the Siegel–Walfisz theorem. However, the conditions that the D_i lie in the thin families $\mathcal{F}_{n_i}$ necessitate some changes and the resulting argument is modelled on [FK10, §7.5].

Fix such an $\mathbf{A}$. In the definition of $\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})$ we group all terms involving D_i. Since η and λ divide N, for fixed $(D_k)_{k\neq i}$ there is a Dirichlet character $\chi_{i,(D_k)_{k\neq i}}$ modulo $4N$ with

$$\left(\frac{\eta}{D_i}\right)^{\mu_i}\left(\frac{\lambda}{D_i}\right)^{\nu_j}\prod_{k\neq i}\left(\frac{D_i}{D_k}\right)^{\Phi(i,k)}\left(\frac{D_k}{D_i}\right)^{\Phi(k,i)} = \chi_{i,(D_k)_{k\neq i}}(D_i)\prod_{k\neq i}\left(\frac{D_i}{D_k}\right)^{\Phi(i,k)+\Phi(k,i)} \tag{4.25}$$

where in the above we are using quadratic reciprocity for Jacobi symbols. From the definition of linked indices, writing $d := d((D_k)_{k\neq i}) = \prod_{k \text{ linked to } i} D_k$ (which is at least 3 by assumption), we have

$$|\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \leq \sum_{\substack{A_k \leq D_k \leq \Delta A_k \\ k\neq i}} \prod_{k\neq i} \kappa_k^{-\omega(D_k)} \left| \sum_{A_i \leq D_i \leq \Delta A_i} \kappa_i^{-\omega(D_i)} \chi_{i,(D_k)_{k\neq i}}(D_i)\left(\frac{D_i}{d}\right)\right| \tag{4.26}$$

where in the inner sum D_i is in $\mathcal{F}_{n_i}$ and is coprime to the D_k in the outer sum, and $\omega(D_i) \leq \Omega$. Now d is odd and coprime to N so

$$D_i \mapsto \chi_{i,(D_k)_{k\neq i}}(D_i)\left(\frac{D_i}{d}\right)$$

is a primitive Dirichlet character modulo q for some q divisible by d, and dividing $4Nd$. In particular, $3 \leq q \ll (\Delta X^{\dagger})^7$ since (4.20) does not hold.

Replacing the inner sum in (4.26) with its maximum possible value we have

$$|\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \ll \frac{X}{\Delta A_i} \cdot \max_{a,\chi,q} \Big| \sum_{\substack{A_i \leq D_i \leq \Delta A_i \\ (a, D_i)=1 \\ D_i \in \mathcal{F}_{n_i},\ \omega(D_i)\leq\Omega}} \kappa_i^{-\omega(D_i)} \chi(D_i)\Big|, \tag{4.27}$$

where the maximum is taken over all $1 \leq a \leq X$, all $3 \leq q \ll (\Delta X^{\dagger})^7$ which contain at least one prime factor coprime to N , and all primitive Dirichlet characters χ modulo q. Here the condition $(a, D_i) = 1$ takes care of the coprimality of D_i with the remaining D_k . We now partition the inner sum according to the number $1 \leq l \leq \Omega$ of prime factors of D_i, write $D_i = np$ where p is the largest prime factor of D_i, and denote by

$P^+(n)$ the largest prime factor of the remaining integer n, giving

$$\max_{a,\chi,q}\Big|\sum_{\substack{A_i\le D_i\le \Delta A_i\\(a,D_i)=1\\D_i\in\mathcal{F}_{n_i},\ \omega(D_i)\le\Omega}}\kappa_i^{-\omega(D_i)}\chi(D_i)\Big|\le\sum_{1\le l\le\Omega}\sum_{\substack{n\\\omega(n)=l-1}}\max_{a,\chi,q}\Big|\sum_{\substack{\max(P^+(n),A_i/n)<p<\Delta A_i/n\\(a,p)=1\\p\in\mathcal{P}_{n_i}}}\chi(p)\Big|, \tag{4.28}$$

where we allow n to range over arbitrary positive integers with $l-1$ factors. To treat the innermost sum, first note that we can drop the condition $(a,p)=1$ at the expense of adding

$$|\sum_{p|a}\mathbb{1}_{\mathcal{P}_{n_i}}(p)\chi(p)|\le\omega(a)\ll\log(X)$$

to its value. Next, since $K/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}$ ramify only at primes dividing N, a prime p is in $\mathcal{P}_{n_i}$ if and only if $p \pmod{4N}$ lies in a certain subset of $(\mathbb{Z}/4N\mathbb{Z})^\times$. In particular we may express the indicator function $\mathbb{1}_{\mathcal{P}_i}$ as a finite sum $\sum_s a_s\chi_s$ where each χ_s is a Dirichlet character modulo $4N$, and the a_s are real numbers. Since the modulus q of any χ appearing in (4.28) contains at least one prime not dividing N (coming from D_j), each $\chi_s\chi$ is a primitive Dirichlet character modulo q' for some $3\le q'\ll(\Delta X^\dagger)^7$ also. By the triangle inequality and [FK07, Lemma 13] (a consequence of the Siegel–Walfisz theorem) we conclude that for all constants $A>0$ we have

$$\begin{aligned}\max_{a,\chi,q}\Big|\sum_{\substack{\max(P^+(n),A_i/n)<p<\Delta A_i/n\\(a,p)=1\\p\in\mathcal{P}_{n_i}}}\chi(p)\Big|\ll&\quad\max_{a,\chi,q}\Big|\sum_{\max(P^+(n),A_i/n)<p<\Delta A_i/n}\chi(p)\Big|+\log(X)\\ \ll_A&\quad(X^\dagger)^4\cdot\frac{\Delta A_i}{n}\cdot\log(A_i/n)^{-A}+\log(X).\end{aligned} \tag{4.29}$$

Now n has at most Ω prime factors, so the sum on the left of (4.29) is non-empty only if $n\le\Delta A_i^{1-1/\Omega}$, in which case

$$\log(A_i/n)^{-A}\ll\log(A_i^{1/\Omega})^{-A}\ll\left(\frac{1}{\Omega}\log(X)^\varepsilon\right)^{-A}\ll\log(X)^{-\varepsilon A}.$$

We now insert this into (4.29), and insert the result into (4.28) and finally (4.27), to find

$$\begin{aligned}|\mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A})|\ &\ll_A\ \frac{X}{\Delta A_i}\cdot\sum_{1\le n\le\Delta A_i^{1-1/\Omega}}\left[(X^\dagger)^4\cdot\frac{\Delta A_i}{n}\cdot\log(X)^{-\varepsilon A}+\log(X)\right]\\ &\ll_A\ X\log(X)^{1-\varepsilon A}(X^\dagger)^4+\frac{X\log(X)^1}{(X^\ddagger)^{1/\Omega}}.\end{aligned}$$

Summing over the $\ll\log(X)^{24}$ possibilities for $\mathbf{A}$ and recalling that $\Omega\ll\log\log(X)$,

we find

$$\sum_{\mathbf{A} \text{ satisfies (4.24)}} |\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \ll X \log(X)^{-1}$$

provided A is chosen large enough (compared to ε).

Remaining families

We now consider those $\mathbf{A}$ such that

$$\text{None of (4.19), (4.20), or (4.24) hold.} \tag{4.30}$$

Here the argument deviates significantly from that in [FK07]. Fix such an $\mathbf{A}$, and define

$$\mathcal{I}_{\mathbf{A}} := \{0 \leq i \leq 7 \quad | \, A_i \geq X^{\ddagger}\}.$$

Recalling that $X^{\ddagger} > X^{\dagger}$ (for sufficiently large X), it follows from the conditions on $\mathbf{A}$ that

- $\mathcal{I}_{\mathbf{A}}$ is unlinked,
- if $j \notin \mathcal{I}_{\mathbf{A}}$ is linked to an element of $\mathcal{I}_{\mathbf{A}}$ then $A_j = 1$ (so in particular, if D_j is such that $A_j \leq D_j \leq \Delta A_j$, then $D_j = 1$).

We begin by discarding as many options for $\mathcal{I}_{\mathbf{A}}$ as we can simply using the trivial bound

$$|\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \leq \sum_{\substack{(D_i) \in \mathscr{D}'(X) \\ A_i \leq D_i \leq \Delta A_i}} \prod_i \kappa_i^{-\omega(D_i)}. \tag{4.31}$$

Specifically, let I be any (possibly empty) set of unlinked indices, and let $i_0 = |I \cap \{0,1\}|$, $i_1 = |\{2,3,4,5\} \cap I|$, and $i_2 = |I \cap \{6,7\}|$. Then

$$\sum_{\substack{\mathbf{A} \text{ satisfies (4.30)} \\ \mathcal{I}_{\mathbf{A}} = I}} |\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \leq \sum_{n \leq (\Delta X^{\ddagger})^8} 2^{\omega(n)} \sum_{m \leq X/n} \frac{i_0^{\omega_0(m)}}{\gamma^{\omega_0(m)}} \cdot \frac{i_1^{\omega_1(m)}}{2^{\omega_1(m)}} \cdot \frac{i_2^{\omega_2(m)}}{(2/\gamma)^{\omega_2(m)}}. \tag{4.32}$$

Here in the above sum, if $i_j = 0$ then we interpret $i_j^{\omega_j(m)}$ as being equal to 1 when m has no prime factors in $\mathcal{P}_j$. The right hand side is derived from the left by setting $n = \prod_{i \notin I} D_i$ and $m = \prod_{i \in I} D_i$. To treat the sum on the right hand side of (4.32) we apply Lemma 4.5.8. Here the argument diverges according to whether $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$ or not. Since the former, somewhat degenerate, case is easier we make the following assumption, consigning the case $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$ to Remark 4.5.19.

Assumption 4.5.17. *Assume henceforth that* $\mathbb{Q}(\sqrt{\alpha\beta}) \nsubseteq K$.

Applying Lemma 4.5.8 to the right hand side of (4.32) we obtain

$$\begin{aligned}\sum_{\substack{\mathbf{A} \text{ satisfies (4.30)} \\ \mathcal{I}_{\mathbf{A}}=I}} \mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A}) &\ll \sum_{n\leq(\Delta X^\ddagger)^8} 2^{\omega(n)}\frac{X}{n}\log(X/n)^{i_0/(4\gamma)+i_1/8+\gamma i_2/4-1} \\ &\ll X\log(X)^{i_0/(4\gamma)+i_1/8+\gamma i_2/4-1}\sum_{n\leq(\Delta X^\ddagger)^8}\frac{2^{\omega(n)}}{n} \\ &\ll X\log(X)^{i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon}\end{aligned}$$

with the last $\ll$ following from the bound $\sum_{n\leq Y}\frac{2^{\omega(n)}}{n}\ll\log(Y)^2$ (to prove this e.g. square the bound $\sum_{n\leq Y}\frac{1}{n}\ll\log(Y)$). We now study the exponent $i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon$ as we vary over unlinked sets I. Note that I is contained in one of the maximal unlinked sets of indices

$$\mathcal{I}_1:=\{2,4,6\},\ \mathcal{I}_2:=\{0,2,3\},\ \mathcal{I}_3:=\{0,1,3,5,7\},\ \mathcal{I}_4:=\{1,4,5,6,7\}.$$

We then have (recall that we've fixed $1<\gamma<7/8+\sqrt{17}/8$):

- $I\subseteq\mathcal{I}_1$. Here $i_0=0$, $i_1\leq 2$, $i_2\leq 1$ so that
$$i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon\leq -1/4+2\varepsilon.$$
- $I\subseteq\mathcal{I}_2$. Here $i_0\leq 1$, $i_1\leq 2$ and $i_2=0$ so that
$$i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon\leq -1/2+2\varepsilon.$$
- $I\subseteq\mathcal{I}_3$. Here $i_0\leq 2$, $i_1\leq 2$ and $i_2\leq 1$. Then
$$i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon\leq 1/(2\gamma)+\gamma/4-3/4+2\varepsilon=\frac{(\gamma-1)(\gamma-2)}{4\gamma}+2\varepsilon.$$
Note that as $1<\gamma<2$ this is strictly negative for sufficiently small ε.
- $I\subsetneq\mathcal{I}_4$. Since I is properly contained in $\mathcal{I}_4$ we have $i_0\leq 1$, $i_1\leq 2$, $i_2\leq 2$, and at least one of these inequalities is strict. This leads to 3 cases. First assume that $i_0=0$. Then
$$i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon\leq\gamma/2-3/4+2\varepsilon.$$
This is strictly negative for sufficiently small $\varepsilon>0$ since $\gamma<3/2$. Next, assume that $i_1\leq 1$. Then
$$i_0/(4\gamma)+i_1/8+\gamma i_2/4-1+2\varepsilon\leq 1/(4\gamma)+\gamma/2-7/8+2\varepsilon=\frac{4\gamma^2-7\gamma+2}{8\gamma}+2\varepsilon.$$
The numerator has roots at $\gamma=7/8\pm\sqrt{17}/8\approx 0.36, 1.39$. This is strictly negative for sufficiently small $\varepsilon>0$ since $\gamma<7/8+\sqrt{17}/8$ (which is why we have

chosen this upper bound on γ). The final case is when $i_2 \leq 1$ where we have

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\varepsilon \leq 1/(4\gamma) + \gamma/4 - 3/4 + 2\varepsilon = \frac{\gamma^2 - 3\gamma + 1}{4\gamma} + 2\varepsilon.$$

In the range considered, the function $\frac{\gamma^2-3\gamma+1}{4\gamma}$ is always less that its value at e.g. 2, where it is equal to $-1/8$.

In conclusion, for all unlinked sets $I \neq \{1,4,5,6,7\}$, choosing ε sufficiently small, we have

$$\sum_{\substack{\mathbf{A} \text{ satisfies (4.30)} \\ \mathcal{I}_{\mathbf{A}} = I}} |\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \ll X \log(X)^{-r_\gamma} \tag{4.33}$$

for some $r_\gamma > 0$, provided that $1 < \gamma < 7/8 + \sqrt{17}/8$.

Remark 4.5.18. Optimising the exponent r_γ over $1 < \gamma < 7/8 + \sqrt{17}/8$, we find that the best uniform upper bound for $i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\varepsilon$ as we range over all unlinked sets $I \neq \{1,4,5,6,7\}$ is obtained when $(\gamma-1)(\gamma-2)/4\gamma = (4\gamma^2 - 7\gamma + 2)/8\gamma$, which yields $\gamma = 1/4 + \sqrt{17}/4$. At this choice of γ we have

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\varepsilon = \frac{1}{16}(3\sqrt{17} - 13) + 2\varepsilon = 2\varepsilon - 0.0394...$$

Completing the argument

Finally, it remains to consider $\mathbf{A}$ satisfying (4.30) such that $\mathcal{I}_{\mathbf{A}} = \{1,4,5,6,7\}$. Since $\mathcal{I}_{\mathbf{A}}$ is a maximal unlinked subset, the assumptions on $\mathbf{A}$ force $A_0 = A_2 = A_3 = 1$ so that also $D_0 = D_2 = D_3 = 1$. Note that the definition of $\mathscr{D}'(X)$ then excludes $\lambda = 1$ or $\lambda = \theta$. Putting $D_0 = D_2 = D_3 = 1$ into the definition of $\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})$ we find

$$\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A}) = \sum_{\substack{(D_i) \in \mathscr{D}'(X) \\ A_i \leq D_i \leq \Delta A}} \left(\frac{\lambda}{D_4}\right)\left(\frac{\lambda}{D_6}\right) \prod_i \kappa_i^{-\omega(D_i)}, \tag{4.34}$$

where $A_4, A_6 \geq X^\ddagger$ by assumption. We get cancellation in this sum via the Siegel–Walfisz theorem as in our third family, although unlike the previous case we must be careful of potential interaction between the conditions defining the sets $\mathcal{F}_i$ and the Dirichlet characters appearing. Specifically, arguing as in our third family, we find

$$|\mathcal{S}_\gamma(\lambda, \eta, X, \mathbf{A})| \ll \frac{X \log(X)}{\Delta A_6} \max_{1 \leq a \leq X} \Big| \sum_{\substack{A_6 \leq D_6 \leq \Delta A_6 \\ (a, D_6) = 1}} \kappa_6^{-\omega(D_6)} \left(\frac{\lambda}{D_6}\right) \Big|$$

and that the inner sum satisfies

$$\Big| \sum_{\substack{A_6 \leq D_6 \leq \Delta A_6 \\ (a, D_6) = 1}} \kappa_6^{-\omega(D_6)} \left(\frac{\lambda}{D_6}\right) \Big| \leq \sum_{1 \leq l \leq \Omega} \sum_{\substack{n \\ \omega(n) = l-1}} \Big| \sum_{\substack{\max(P^+(n), A_6/n) < p < \Delta A_6/n \\ (a,p)=1 \\ p \in \mathcal{P}_3}} \left(\frac{\lambda}{p}\right) \Big|. \tag{4.35}$$

As before we may remove the condition $(a,p)=1$ at the expense of an acceptable error term. To treat the condition that $p \in \mathcal{P}_2$, recall that $\mathcal{P}_2$ is the set of primes coprime to N which are inert in $K/\mathbb{Q}$. In particular, the indicator function $\mathbb{1}_{\mathcal{P}_2}(p)$ is given by $\frac{1}{2}(1-\left(\frac{\theta}{p}\right))$. Inserting this into the sum, we may apply [FK07, Lemma 13] as in our third family since $\lambda \neq 1, \theta$ means that both $D \mapsto \left(\frac{\lambda}{D}\right)$ and $D \mapsto \left(\frac{\lambda\theta}{D}\right)$ are non-principal. Continuing to argue as in our third family yields

$$\sum_{\substack{\mathbf{A} \text{ satisfies (4.30)} \\ \mathcal{I}_{\mathbf{A}}=\{1,4,5,6,7\}}} |\mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A})| \ll X\log(X)^{-1}, \tag{4.36}$$

which completes the proof of Proposition 4.5.16.

Remark 4.5.19. Suppose instead (of Assumption 4.5.17) we have $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$. This time applying Lemma 4.5.8 to the right hand side of (4.32) gives the bound

$$\sum_{\substack{\mathbf{A} \text{ satisfies (4.30)} \\ \mathcal{I}_{\mathbf{A}}=I}} \mathcal{S}_\gamma(\lambda,\eta,X,\mathbf{A}) \ll X\log(X)^{i_1/4+i_2\gamma/4-1+2\varepsilon}.$$

Splitting into cases according to which maximal unlinked subset I is contained in, one finds that in the first 3 cases, namely $I \subseteq \mathcal{I}_i$ for $i=1,2,3$, the exponent satisfies

$$i_1/4 + i_2\gamma/4 - 1 + 2\varepsilon \leq -1/8 + 2\varepsilon$$

provided $\gamma < 3/2$. In the final case where $I \subseteq \mathcal{I}_4$, we note that $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$ forces $\mathcal{F}_0 = \emptyset$, so that D_1 (and also D_0) is necessarily equal to 1. Thus $I \subseteq \{4,5,6,7\}$. Now provided $I \neq \{4,5,6,7\}$, the exponent is strictly negative (for sufficiently small ε) for $\gamma < 3/2$, and is e.g. equal to $(\sqrt{17}-5)/8 = -0.1096...$ if one takes $\gamma = 1/4 + \sqrt{17}/4$ as in Remark 4.5.18. We are thus left to deal with the case $I = \{4,5,6,7\}$. This forces $D_2 = D_3 = 1$ (since they are both linked to elements of I), in addition to $D_0 = D_1 = 1$. One may conclude as we did for the third family.

§ 4.6 | Prime Twists with Nontrivial Action

In this section we provide an example of a thin subfamily of quadratic twists for which the statistical behaviour of the 2-Selmer group differs from that of the family of all twists. In particular, there is a non-trivial Galois action in a positive proportion of cases so that, by Corollary 4.1.4, $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_d[2])$ is non-trivial for a positive proportion of d in our thin subfamily.

We restrict our quadratic field $K = \mathbb{Q}(\sqrt{\theta})$ to be an imaginary quadratic number field which has class number 1 and in which 2 is inert (so $-\theta \in \{3,11,19,43,67,163\}$). Write $\mathcal{O}_K$ for the ring of integers of K, and note that the only prime which ramifies in K is $-\theta$. We take

$$E : y^2 = x^3 - x = x(x-1)(x+1),$$

to be the congruent number curve. This has good reduction away from 2. Taking

$p \nmid 2\theta$ to be a rational prime, we will explicitly describe the group $\mathrm{Sel}_2(E_p/K)$ as a $G = \mathrm{Gal}(K/\mathbb{Q})$-module.

For a place v of K, we will identify the local Kummer images $\mathscr{S}_v(E_p/K)$ of Definition 2.1.6 with their image under the 2-descent map (4.6) (in our case, $a_1 = 0, a_2 = 1, a_3 = -1$), so that

$$\mathscr{S}_v(E_p/K) \subseteq K_v^\times/K_v^{\times 2} \times K_v^\times/K_v^{\times 2}.$$

We view the Selmer group $\mathrm{Sel}_2(E_p/K)$ as a subgroup of $K^\times/K^{\times 2}$ similarly, noting that this identification respects the G-action.

For a vector space V and $v_1, \ldots, v_n \in V$ we write $\langle v_1, v_2, ..., v_n \rangle$ for the subspace generated by $v_1, \ldots, v_n$.

§ 4.6.1 | 2-Descent

Our primary goal is to characterise the groups $\mathrm{Sel}_2(E_p/K)$ for p prime, which we do via 2-Descent. We first begin by identifying the local Kummer images at each prime.

Lemma 4.6.1. *Let $p \nmid 2\theta$ be a prime, and let v be a place of K. Then the local Kummer image at v for E_p is given by:*

(i) If $v \mid \infty$ then

$$\mathscr{S}_v(E_p/K) = 0.$$

(ii) If $v \nmid 2p$ then

$$\mathscr{S}_v(E_p/K) = \langle (1, u), (u, 1) \rangle$$

where u is any nonsquare unit in K_v.

(iii) If $v \mid p$, then

$$\mathscr{S}_v(E_p/K) = \langle (-1, -p), (p, 2) \rangle .$$

(iv) If $v = 2$ and $\zeta \in K_2$ is a primitive third root of unity, then

$$\mathscr{S}_2(E_p/K) = \langle T_1, T_2, T_3, T_4 \rangle$$

where

$$T_1 := (-1, -p), \qquad T_3 := (\zeta + 3, \zeta + 3(1 + p)),$$
$$T_2 := (1, 2), \qquad T_4 := (1, 4\zeta + 5).$$

Proof. Since K is imaginary, if $v \mid \infty$ the group $H^1(K_v, E[2])$ is trivial and so (i) holds. Lemma 4.4.1 then provides (ii) as $p \notin \Sigma$. In order to prove (iii), it is enough to note that by Lemma 4.2.2, since $\dim \mathscr{S}_v(E_p/K) = 2$, $\mathscr{S}_v(E_p/K) = \delta_v(E_p[2])$.

For $v = 2$, note firstly that $\dim((K_2^\times/K_2^{\times 2})^2) = 8$, so since $\mathscr{S}_p(E_p/K)$ is self-dual with respect to the local Tate pairing (see Lemma 2.3.2) we have $\dim \mathscr{S}_2(E_p/K) = 4$.

Let $x_3 = -(\zeta+3)/3$ and $x_4 = -(3\zeta+2)/3$. It is elementary to compute that

$$x_3^3 - p^2 x_3 \equiv -3\zeta \mod 8 \qquad x_4^3 - p^2 x_4 \equiv \zeta^2 \mod 8.$$

Since $-3, \zeta$ and ζ are all square in K_2, by Hensel's lemma each $x_i^3 - p^2 x_i$ is then also a square in K_2. In particular, there are y_3, y_4 in K_2 such that $P_i = (x_i, y_i)$ lies in $E_p(K_2)$ for $i = 3, 4$. We then have $\delta_2(P_3) = T_3$ since -3 is square in K_2 and moreover

$$\delta_2(P_4) = (3\zeta + 2, 3\zeta + 2 + 3p)\,.$$

Moreover, the space generated by the $\delta_2(P)$ for $P \in E_p[2]$ is $\langle (p,2), (-1,-p) \rangle$. Since $K_2/\mathbb{Q}_2$ is unramified of degree 2, p is congruent to ± 1 modulo $K_2^{\times 2}$, so this space is spanned by T_1 and T_2. One then checks that

$$T_1 \cdot T_2 \cdot T_4 = \delta_2(P_4)$$

inside $(K_2^\times / K_2^{\times 2})^2$, so that T_4 is in $\mathscr{S}_2(E_p/K)$. Since T_1, T_2, T_3 and T_4 are readily checked to be linearly independent, the result follows. □

In the case that p is split in $K/\mathbb{Q}$, we will need to understand the image of the primes over p in the localisation at 2, for which we will use the following result. As in Lemma 4.6.1, $p \nmid 2\theta$ is a prime, and we denote by ζ a fixed primitive 3rd root of unity in K_2. For x in K we denote its conjugate under the action of G as $\overline{x}$.

Lemma 4.6.2. *Suppose that p splits in $K/\mathbb{Q}$, and write $p = \varepsilon\overline{\varepsilon}$ for some $\varepsilon \in \mathcal{O}_K$. Then in $K_2^\times$ we have*

$$\varepsilon \equiv \pm(\zeta + 2 - p) \pmod{K_2^{\times 2}}.$$

(Since -1 is not a square in K_2, precisely one of these two possibilities occurs.)

Proof. The ring of integers of K_2 is $\mathbb{Z}_2[\zeta]$ and by Hensel's lemma, an element of $\mathbb{Z}_2[\zeta_3]^\times$ is a square if and only if it is a square modulo 8. Now using the fact that both 5 and $\zeta = \zeta^4$ are squares in K_2, we find that any element of $\mathbb{Z}_2[\zeta]^\times / \mathbb{Z}_2[\zeta]^{\times 2}$ can be written uniquely in the form $a \pm \zeta$ for some $a \in \{\pm 1, \pm 5\}$ (in this representation, the trivial class is $-1-\zeta = \zeta^2$). Now writing $\varepsilon \pmod{K_2^{\times 2}}$ in this form we find that, in $K_2^\times / K_2^{\times 2}$, we have

$$p = N_{K_2/\mathbb{Q}_2}(\varepsilon) = (a \pm \zeta)(a \pm \zeta^2) = 2 \mp a.$$

Thus $a \equiv \pm(2-p) \pmod 8$ and the result follows. □

We are now ready to describe the Selmer groups. In the statement, all isomorphisms are as $\mathbb{F}_2[G]$-modules.

Proposition 4.6.3. *Let p be an odd prime not dividing θ. Then*

(i) If p is inert in $K/\mathbb{Q}$ we have

$$\mathrm{Sel}_2(E_p/K) \cong \mathbb{F}_2^4.$$

(ii) If p is split in $K/\mathbb{Q}$ and $\varepsilon \in \mathcal{O}_K$ has norm p, we have

$$\mathrm{Sel}_2(E_p/K) \cong \begin{cases} \mathbb{F}_2^2 \oplus \mathbb{F}_2[G] & p \equiv 5,7 \pmod 8, \\ \mathbb{F}_2^2 & p \equiv 3 \pmod 8, \\ \mathbb{F}_2^2 \oplus \mathbb{F}_2[G]^2 & p \equiv 1 \pmod 8 \text{ and } \overline{\varepsilon} \in K_\varepsilon^{\times 2}, \\ \mathbb{F}_2^4 & p \equiv 1 \pmod 8 \text{ and } \overline{\varepsilon} \notin K_\varepsilon^{\times 2}. \end{cases}$$

Proof. Let $p \neq 2$ be inert in $K/\mathbb{Q}$. Since E_p has good reduction outside 2 and p, the 2-Selmer elements are units outside $2, p$. As K has class number 1 we thus want to find all $a_i, b_i \in \{0,1\}$ for which

$$((-1)^{a_1} 2^{a_2} p^{a_3}, (-1)^{b_1} 2^{b_2} p^{b_3}) \tag{4.37}$$

lies in both of the local groups $\mathscr{S}_p(E_p/K)$ and $\mathscr{S}_2(E_p/K)$ described in Lemma 4.6.1. As $K_p/\mathbb{Q}_p$ is unramified of degree 2, both -1 and 2 are squares in K_p. Thus all elements of the form (4.37) lie in $\mathscr{S}_p(E_p/K)$. We now apply the Selmer conditions at 2. Since p is odd we have $p \equiv \pm 1 \pmod{K_2^{\times 2}}$. Consequently, a global element of the form (4.37) which lies in $\mathrm{Sel}_2(E_p/K)$ necessarily maps to the subspace of $\mathscr{S}_2(E_p/K)$ generated by $T_1 = (-1,-p)$ and $T_2 = (1,2)$. Restricting to elements of the form (4.37) which do map to this space gives

$$\mathrm{Sel}_2(E_p/K) = \left\langle (p,2), (-1,-p), (1,(-1)^\delta p), ((-1)^\delta p, 1) \right\rangle \cong \mathbb{F}_2^4$$

where $\delta = 1$ if $p \notin K_2^{\times 2}$ and $\delta = 0$ otherwise.

Now suppose p splits in $K/\mathbb{Q}$, and fix $\varepsilon \in K^\times$ such that $\varepsilon\overline{\varepsilon} = p$. As above, the 2-Selmer elements are unramified outside $\{2, \varepsilon, \overline{\varepsilon}\}$, so we want to find all $a_i, b_i \in \{0,1\}$ for which

$$((-1)^{a_1} 2^{a_2} \varepsilon^{a_3} \overline{\varepsilon}^{a_4}, (-1)^{b_1} 2^{b_2} \varepsilon^{b_3} \overline{\varepsilon}^{b_4}) \tag{4.38}$$

lies in each of the groups $\mathscr{S}_\varepsilon(E_p/K)$, $\mathscr{S}_{\overline{\varepsilon}}(E_p/K)$ and $\mathscr{S}_2(E_p/K)$ described in Lemma 4.6.1. This is an elementary computation, which we do by treating each possibility for $p \pmod 8$ separately. We repeat the local Kummer images from Lemma 4.6.1:

$$\begin{aligned} \mathscr{S}_2(E_p/K) &= \langle (-1,-p), (1,2), (\zeta+3, \zeta+3(1+p)), (1, 4\zeta+5) \rangle \\ \mathscr{S}_\varepsilon(E_p/K) &= \langle (-1, -\varepsilon\overline{\varepsilon}), (\varepsilon\overline{\varepsilon}, 2) \rangle, \\ \mathscr{S}_{\overline{\varepsilon}}(E_p) &= \langle (-1, -\varepsilon\overline{\varepsilon}), (\varepsilon\overline{\varepsilon}, 2) \rangle. \end{aligned}$$

We now break into cases.

$\underline{\mathbf{p \equiv -1 \pmod 8}}$: Here -1 is nonsquare in K_ε. Replacing ε with $-\varepsilon$ if necessary, we assume $\overline{\varepsilon} \in K_\varepsilon^{\times 2}$. Note also that 2 is a square in K_ε. By symmetry, this gives $2, \varepsilon \in K_{\overline{\varepsilon}}^{\times 2}$. The elements of the form (4.38) which lie in $\mathscr{S}_\varepsilon(E_p/K)$ are then those of the shape

$$\left((-1)^{a_1} 2^{a_2} \varepsilon^{a_3} \overline{\varepsilon}^{a_4}, (-\varepsilon)^{a_1} 2^{b_2} \overline{\varepsilon}^{b_4}\right).$$

Reducing further to those that satisfy the conditions of $\mathscr{S}_{\overline{\varepsilon}}(E_p)$ we are left with elements of the shape

$$\left((-1)^{a_1}2^{a_2}\varepsilon^{a_3}\overline{\varepsilon}^{a_4}, (-\varepsilon\overline{\varepsilon})^{a_1}2^{b_2}\right). \tag{4.39}$$

Finally, as $p \equiv -1 \pmod 8$ we have

$$\mathscr{S}_2(E_p/K) = \langle (-1,1), (1,2), (\zeta+3,1), (1,4\zeta+5)\rangle.$$

Since the first coordinate of each of these basis vectors has valuation 0, we must have $a_2 = 0$. Further, Lemma 4.6.2 gives $\varepsilon \equiv \pm(\zeta+2-p) \equiv \pm(\zeta+3)$ in $K_2^\times/K_2^{\times 2}$, and since $\varepsilon\overline{\varepsilon} = p \equiv -1 \pmod{K_2^{\times 2}}$ we have $\overline{\varepsilon} \equiv \mp(\zeta+3)$. It follows that each of the elements

$$(\varepsilon,1), (\overline{\varepsilon},1), (1,2), (-1,-\varepsilon\overline{\varepsilon})$$

are in $\mathrm{Sel}_2(E_p/K)$. Since each element of the form (4.39) with $a_2 = 0$ can be written as a linear combination of these Selmer elements, we have

$$\begin{aligned}\mathrm{Sel}_2(E_p/K) &= \langle (1,2), (-1,-\varepsilon\overline{\varepsilon}), (\varepsilon,1), (\varepsilon\overline{\varepsilon},1)\rangle \\ &\cong \mathbb{F}_2^2 \oplus \mathbb{F}_2[G].\end{aligned}$$

$\underline{\mathbf{p \equiv 3 \pmod 8}}$: Again, -1 is nonsquare in K_ε so we assume $\overline{\varepsilon} \in K_\varepsilon^{\times 2}$. Additionally, 2 is nonsquare in K_ε, hence -2 is a square. With ε and $\overline{\varepsilon}$ swapped this all remains true.

The elements of the form (4.38) which lie in $\mathscr{S}_\varepsilon(E_p/K)$ are thus those of the shape

$$\left((-2)^{a_2}\overline{\varepsilon}^{a_4}(-1)^{b_3}\varepsilon^{a_3}, (-2)^{b_2}\overline{\varepsilon}^{b_4}(-1)^{a_3}(-\varepsilon)^{b_3}\right).$$

Reducing further to those that satisfy the conditions of $\mathscr{S}_{\overline{\varepsilon}}(E_p)$ we are left with

$$\left((-2)^{a_2}(-1)^{b_3}(\varepsilon\overline{\varepsilon})^{a_3}, (-2)^{b_2}(-\varepsilon\overline{\varepsilon})^{b_3}(-1)^{a_3}\right). \tag{4.40}$$

Finally, we apply the conditions at 2. By Lemma 4.6.2 we have $\varepsilon \equiv \pm(\zeta-1) \pmod{K_2^{\times 2}}$. As $p \equiv 3 \pmod 8$ we have

$$\mathscr{S}_2(E_p/K) = \langle (-1,1), (1,2), (\zeta+3,\zeta+4), (1,4\zeta+5)\rangle.$$

Since the first coordinate of each basis element is a unit, we must have $a_2 = 0$. Considering the second coordinate, and noting that $\varepsilon\overline{\varepsilon} \equiv -1 \pmod{K_2^{\times 2}}$, we find $a_3 = b_2$. This leaves a 2-dimensional space of candidate Selmer elements. However, since the elements $(p,2)$ and $(-1,-p)$ (which correspond to the 2-torsion points) lie in the Selmer group, we have

$$\begin{aligned}\mathrm{Sel}_2(E_p/K) &= \langle (-1,-p), (p,2)\rangle \\ &\cong \mathbb{F}_2^2.\end{aligned}$$

$\underline{\mathbf{p \equiv 5 \pmod 8}}$: Here -1 is square in both K_ε and $K_{\overline{\varepsilon}}$, and 2 is a nonsquare unit in both K_ε and $K_{\overline{\varepsilon}}$. We now split into two cases according to whether $\overline{\varepsilon}$ is in $(K_\varepsilon^\times)^2$. To capture this, we fix

$$\delta = \begin{cases} 1 & \overline{\varepsilon} \notin K_\varepsilon^{\times 2} \\ 0 & \text{else.} \end{cases}$$

Note that if $\overline{\varepsilon} \notin K_\varepsilon^{\times 2}$ then we necessarily have $2 \equiv \overline{\varepsilon} \pmod{K_\varepsilon^{\times 2}}$. Acting by $\mathrm{Gal}(K/\mathbb{Q})$, we see that $\overline{\varepsilon}$ is in $(K_\varepsilon^\times)^2$ if and only if ε is in $(K_{\overline{\varepsilon}}^\times)^2$.

The elements of the form (4.38) which lie in $\mathscr{S}_\varepsilon(E_p/K)$ are thus those of the shape

$$\left((-1)^{a_1}(2^\delta\overline{\varepsilon})^{a_4}(2^\delta\varepsilon)^{a_3}, (-1)^{b_1}(2^\delta\overline{\varepsilon})^{b_4}2^{a_3}(2^\delta\varepsilon)^{b_3}\right).$$

Reducing further to those that lie in $\mathscr{S}_{\overline{\varepsilon}}(E_p)$ forces $a_3 = a_4$, leaving those of the shape

$$\left((-1)^{a_1}(\varepsilon\overline{\varepsilon})^{a_3}, (-1)^{b_1}(2^\delta\overline{\varepsilon})^{b_4}2^{a_3}(2^\delta\varepsilon)^{b_3}\right). \tag{4.41}$$

Finally, we apply the conditions at 2. By Lemma 4.6.2 we have $\varepsilon \equiv \pm(\zeta-3) \equiv \mp(4\zeta+5) \pmod{K_2^{\times 2}}$. Moreover, as $p \equiv 5 \pmod 8$ we have

$$\mathscr{S}_2(E_p/K) = \langle (-1,-1), (1,2), (\zeta+3, \zeta+2), (1, 4\zeta+5)\rangle.$$

Since $\varepsilon\overline{\varepsilon} = p \equiv 1 \pmod{K_2^{\times 2}}$, we have $\overline{\varepsilon} \equiv \varepsilon \equiv \mp(4\zeta+5)$. Thus the elements

$$(-1,-1), (\varepsilon\overline{\varepsilon}, 2), (1, \mp 2^\delta\varepsilon), (1, \mp 2^\delta\overline{\varepsilon})$$

all lie in $\in \mathrm{Sel}_2(E/K)$, and are visibly linearly independent. Noting that $(1,-1)$ is not in $\mathscr{S}_2(E_p/K)$, we conclude that

$$\begin{aligned} \mathrm{Sel}_2(E_p/K) &= \left\langle (-1,-1), (\varepsilon\overline{\varepsilon}, 2), (1, \mp 2^\delta\varepsilon), (1, \mp 2^\delta\overline{\varepsilon})\right\rangle \\ &\cong \mathbb{F}_2^2 \oplus \mathbb{F}_2[G]. \end{aligned}$$

$\underline{\mathbf{p \equiv 1 \pmod 8}}$: Here both -1 and 2 are squares in both K_ε and $K_{\overline{\varepsilon}}$. As before, set

$$\delta = \begin{cases} 1 & \overline{\varepsilon} \notin K_\varepsilon^{\times 2} \\ 0 & \text{else.} \end{cases}$$

The elements of the form (4.38) which lie in $\mathscr{S}_\varepsilon(E_p/K)$ are those of the shape

$$\left((-1)^{a_1}2^{a_2}(\varepsilon\overline{\varepsilon}^\delta)^{c_1}\overline{\varepsilon}^{(1-\delta)c_2}, (-1)^{b_1}2^{b_2}(\varepsilon\overline{\varepsilon}^\delta)^{d_1}\overline{\varepsilon}^{(1-\delta)d_2}\right), \tag{4.42}$$

for some c_1, c_2, d_1, d_2 in $\{0,1\}$. For either value of δ these elements all lie in $\mathscr{S}_{\overline{\varepsilon}}(E_p)$.

Finally, we apply the conditions at 2. By Lemma 4.6.2 we have

$$\varepsilon \equiv \pm(-\zeta-1) \equiv \pm\zeta^2 \equiv \pm 1 \pmod{K_2^{\times 2}},$$

and as $\varepsilon\overline{\varepsilon} = p$ with have $\varepsilon \equiv \overline{\varepsilon} \pmod{K_2^{\times 2}}$. Moreover, with $p \equiv 1 \pmod 8$ we have

$$\mathscr{S}_2(E_p/K) = \langle (-1,-1), (1,2), (\zeta+3, \zeta+6), (1, 4\zeta+5) \rangle .$$

As the first coordinate of each of these basis elements has trivial valuation, we have $a_2 = 0$.

Suppose that $\delta = 1$. Then we see that an element of the form(4.42) is in the Selmer group if and only if, in addition to $a_2 = 0$, we have $a_1 = b_1$. Thus we find

$$\begin{aligned} \mathrm{Sel}_2(E_p/K) &= \langle (-1,-1), (1,2), (1, \varepsilon\overline{\varepsilon}), (\varepsilon\overline{\varepsilon}, 1) \rangle \\ &\cong \mathbb{F}_2^4. \end{aligned}$$

Now suppose that $\delta = 0$. Setting $a_2 = 0$ in (4.42) leaves a 7-dimensional space of candidate Selmer elements. Further, one readily checks that $(-1, 1)$, which has the form (4.42) for $a_1 = 1$ and all other variables 0, is not in $\mathscr{S}_2(E_p/K)$. Thus $\mathrm{Sel}_2(E_p/K)$ is at most 6 dimensional. However, using the fact that $\varepsilon \equiv \overline{\varepsilon} \equiv \pm 1 \pmod{K_2^{\times 2}}$, one readily checks that the 6 linearly independent elements

$$\{(-1,-1), (1,2), (1, \pm\varepsilon), (\pm\varepsilon, 1), (1, \pm\overline{\varepsilon}), (\pm\overline{\varepsilon}, 1)\},$$

each of which are of the form (4.42), map to $\mathscr{S}_2(E_p/K)$ after localising at 2. Thus,

$$\begin{aligned} \mathrm{Sel}_2(E_p/K) &= \langle (-1,-1), (1,2), (1, \pm\varepsilon), (\pm\varepsilon, 1), (1, \pm\overline{\varepsilon}), (\pm\overline{\varepsilon}, 1) \rangle \\ &\cong \mathbb{F}_2^2 \oplus \mathbb{F}_2[G]^2. \end{aligned}$$

This completes the proof. □

Remark 4.6.4. The proof of part (i) shows that the conditions at inert primes impose no restrictions. Using this observation, one sees similarly that if d is odd and divisible only by inert primes, then

$$\mathrm{Sel}_2(E_d/K) \cong \mathbb{F}_2^{2+2\omega(d)}.$$

This gives a concrete instance of the growth of $\mathrm{Sel}_2(E_d/K)$ seen also in e.g. Proposition 4.2.7.

§ 4.6.2 | Statistics

Here we use Rédei symbols alongside the Chebotarev density theorem to determine the statistical behaviour of $\mathrm{Sel}_2(E_p/K)$ from Proposition 4.6.3. We refer the reader to [Ste18] for definitions concerning Rédei symbols.

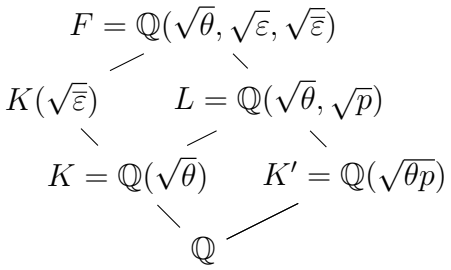
Lemma 4.6.5. *Let $p \equiv 1 \pmod 8$ be a prime which splits in $K/\mathbb{Q}$, and let $\varepsilon \in \mathcal{O}_K$ have norm p. Then $\overline{\varepsilon} \in (K_\varepsilon^\times)^2$ if and only if the Rédei symbol $[\theta, -\theta, p]$ is trivial.*

Proof. Note that -1 is a square in K_ε since $p \equiv 1 \pmod 8$. In particular, the statement is unchanged upon replacing ε with $-\varepsilon$. By Lemma 4.6.2 we may thus assume that we

have

$$\overline{\varepsilon} \equiv -(\zeta+1) = \zeta^2 \equiv 1 \pmod{K_2^{\times 2}}.$$

Now consider the diagram of fields



Since ε ramifies in L/K, we see that $\overline{\varepsilon} \in (K_\varepsilon^\times)^2$ if and only if the unique prime of L lying over ε splits in F/L. Let $\mathfrak{p}$ denote the unique prime of K' lying over p. Since p splits in $K/\mathbb{Q}$, we see that $\mathfrak{p}$ splits in L/K'. Further, $\overline{\varepsilon}$ ramifies in L/K and hence has even valuation (either 0 or 2) at any prime $\mathfrak{p}' \mid \mathfrak{p}$ of L. In particular, the extension $F = L(\sqrt{\overline{\varepsilon}})/L$ is unramified at such $\mathfrak{p}'$. Thus F/K' is unramified at $\mathfrak{p}$. We now conclude that $\overline{\varepsilon} \in (K_\varepsilon^\times)^2$ if and only if the Artin symbol $\left(\frac{F/K'}{\mathfrak{p}}\right)$ is trivial. Before relating this to a Rédei symbol, it will be useful to prove the following two claims.

Claim 1: The field F/K' is everywhere unramified. That F'/K' is unramified at primes not dividing $2p\theta$ is clear, and we have already shown that the unique prime of K' dividing p is unramified in F'/K'. For primes over 2 note that K and K' are unramified at 2, and so $L/\mathbb{Q}$ is unramified at 2 also. Further, having chosen $\overline{\varepsilon}$ to be a square in K_2, the extension $K(\sqrt{\overline{\varepsilon}})/K$ is split at 2. Thus, as the compositum of $K(\sqrt{\overline{\varepsilon}})$ and L, the full extension $F/\mathbb{Q}$ is unramified at 2. Now note that $\ell = -\theta$ is an odd prime. Since p has trivial l-adic valuation, the extension $F = K'(\sqrt{p}, \sqrt{\varepsilon})/K'$ is unramified at (the unique prime of K' over) l. This proves the claim.

Claim 2: For each prime q, the Hilbert symbols $(p,\theta)_q$ and $(p,p)_q$ are trivial. By assumption, p is a norm from $K = \mathbb{Q}(\sqrt{\theta})$, so that $(p,\theta)_q$ is trivial for all q. Next, for each prime q we have $(p,p)_q = (p,-1)_q$. That this latter symbol is trivial for $q \neq 2, p$ is immediate, whilst for $q = 2, p$ it is trivial since $p \equiv 1 \pmod 8$. This proves the claim.

Returning to the proof, by Claim 2 the Rédei symbol $[\theta, p, p]$ exists (see [Ste18, Definition 7.8]). Writing $\varepsilon = x + y\sqrt{\theta}$ for x, y in $\mathbb{Q}$, we have $x^2 - \theta y^2 = p$ by assumption. The field F is then given by adjoining to L the element

$$\sqrt{\varepsilon} = \sqrt{x + y\sqrt{\theta}}.$$

Further, by Claim 1 the extension F/K' is minimally ramified in the sense of [Ste18, Definition 7.6]. Thus we may take $a = \theta$, $b = p$ and $F_{a,b} = F$ in [Ste18, Definition 7.8], giving $[\theta, p, p] = \left(\frac{F/K'}{\mathfrak{p}}\right)$. Consequently, we see that $\overline{\varepsilon} \in K_\varepsilon^{\times 2}$ if and only if the Rédei symbol $[\theta, p, p]$ is trivial.

By [Ste18, Proposition 7.10] the Rédei symbol $[p, \theta, -\theta p]$ exists and is trivial (to see that θp is a second kind decomposition, use [Ste18, Prop 4.2 (4)] and our computations of Hilbert symbols above). Now, using the trilinearity and reciprocity of Rédei symbols [Ste18, Theorem 1.1] we have

$$\begin{aligned}[\theta, p, p] &= [p, \theta, p] + [p, \theta, -\theta p] \\ &= [p, \theta, -\theta] \\ &= [\theta, -\theta, p]\end{aligned}$$

as required. □

This allows us to give a complete statistical description of the $\mathbb{F}_2[G]$-module structure of $\mathrm{Sel}_2(E_p/K)$. First we introduce some notation.

Notation 4.6.6. For p a prime, we define $e_1(E_p/K), e_2(E_p/K) \in \mathbb{Z}_{\geq 0}$ to be the unique positive inters (by Lemma 2.2.12) for which there is an $\mathbb{F}_2[G]$-module isomorphism

$$\mathrm{Sel}_2(E_p/K) \cong \mathbb{F}_2^{e_1(E_p/K)} \oplus \mathbb{F}_2[G]^{e_2(E_p/K)}.$$

Theorem 4.6.7 (Theorem 1.2.5)**.** *For each pair $(e_1, e_2) \in \mathbb{Z}^2_{\geq 0}$, the natural density of primes p for which $e_1(E_p/K) = e_1$ and $e_2(E_p/K) = e_2$ is as follows:*

$$\lim_{X\to\infty} \frac{\#\left\{p \leq X \text{ prime} \ : \ \begin{smallmatrix} e_1(E_p/K)=e_1 \text{ and} \\ e_2(E_p/K)=e_2 \end{smallmatrix}\right\}}{\#\{p \leq X \text{ prime}\}} = \begin{cases} 9/16 & \text{if } (e_1, e_2) = (4, 0), \\ 1/16 & \text{if } (e_1, e_2) = (2, 2), \\ 4/16 & \text{if } (e_1, e_2) = (2, 1), \\ 2/16 & \text{if } (e_1, e_2) = (2, 0). \end{cases}$$

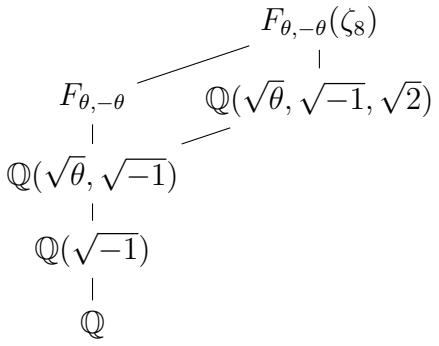
Proof. As a consequence of Lemma 4.6.5, and the Chebotarev density theorem applied to Proposition 4.6.3, it suffices to show that $[\theta, -\theta, p]$ is trivial for precisely half of the primes $p \equiv 1 \pmod 8$ which split in $K/\mathbb{Q}$ (with respect to the natural density).

Fix a prime $p \nmid 2\theta$. In the notation of [Ste18, Definitions 7.6, 7.8], let $F_{\theta,-\theta}$ be minimally ramified over $\mathbb{Q}(\sqrt{\theta}, \sqrt{-1})$, so that by definition the Rédei symbol $[\theta, -\theta, p]$ is equal to the Artin symbol

$$\left(\frac{F_{\theta,-\theta}/\mathbb{Q}(\sqrt{-1})}{\mathfrak{p}}\right), \tag{4.43}$$

where $\mathfrak{p}$ is any ideal of $\mathbb{Q}(\sqrt{-1})$ of norm p. The field $F_{\theta,-\theta}$ is a cyclic degree 4 extension of $\mathbb{Q}(\sqrt{-1})$ fitting into the diagram below. It is dihedral of degree 8 over $\mathbb{Q}$ and contains

$\mathbb{Q}(\sqrt{\theta}, \sqrt{-1})$ as a subfield.



The field $F_{\theta,-\theta}(\zeta_8)/\mathbb{Q}$ is Galois of degree 16. Now p both splits in $K/\mathbb{Q}$ and is congruent to 1 modulo 8 if and only if it splits completely in $\mathbb{Q}(\sqrt{\theta}, \sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\sqrt{\theta}, \zeta_8)$. On the other hand, the Artin symbol (4.43) is trivial if and only if p splits completely in $F_{\theta,-\theta}$.

Consequently, we wish to compute the density of primes which split completely in $F_{\theta,-\theta}(\zeta_8)$, amongst those that split completely in $\mathbb{Q}(\sqrt{\theta}, \zeta_8)$. By the Chebotarev density theorem, this is equal to $1/2$. □

Part III

The Family of All Elliptic Curves

Chapter 5

Elliptic Curves Over Galois Extensions

In this chapter we study the family of all elliptic curves ordered by the natural height, and prove the results presented in §1.3. We begin in §5.1 by studying the statistical behaviour of the Galois representation given by the n-torsion of E. Using the large sieve we show that, for each fixed number field K and integer n, for 100% of $E/\mathbb{Q}$ the image of G_K in $\mathrm{Aut}(E[n])$ is as large as it is able to be. This material is novel, though it is an application of the large sieve much like other results in the literature.

Next, in §5.2, we study p-Selmer groups of elliptic curves over a finite Galois extension of number fields K/F when p is "good" (i.e. $p \nmid [K : F]$). In this setting we can decompose the p-Selmer group over K as a sum of p-Selmer groups of other abelian varieties, so-called twists, over F. We conclude the section by applying these results in the case that $F = \mathbb{Q}$ and $K/\mathbb{Q}$ is multiquadratic to extend results of Bhargava–Shankar [BS15b, BS13] and Hypothesis 1 on average sizes of p-Selmer groups over $\mathbb{Q}$ to ones on average sizes of p-Selmer groups over K.

In §5.3 we return to the generality that K/F is finite Galois, and bound the difference between the average size of the Galois fixed space in $\mathrm{Sel}_p(E/K)$ and the average size of $\mathrm{Sel}_p(E/F)$. In §5.4 and §5.5 we then apply the previous results to bound the average dimension of p-Selmer groups, with additional assumptions on K/F, and to bound average multiplicities of certain lattices in the Mordell–Weil lattices of elliptic curves. At the end of the chapter we present an example of a class of modules covered by our result for lattices.

This chapter is solely the work of the author, with the exception of cited results, and everything except for §5.1 appears in [Pat21].

§ 5.1 | Torsion Modules

For every elliptic curve $E/\mathbb{Q}$ and integer $n \geq 2$ let

$$\rho_{E,n} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

for the Galois representation given by the natural action of $G_{\mathbb{Q}}$ on n-torsion points. It is natural to ask how often the maps $\rho_{E,n}$ are surjective. This question was answered by Duke [Duk97, Theorem 1], who in fact showed that showed that for 100% of $E/\mathbb{Q}$, all of the maps $\{\rho_{E,n} \ : \ n \geq 2\}$ are surjective. Equivalently, for 100% of $E/\mathbb{Q}$ every field extension $\mathbb{Q}(E[n])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. For a fixed number field K and integer $n \geq 2$, a natural follow-on question is to ask how often $\rho_{E,n}$ remains surjective on restriction to G_K.

Sometimes the answer to this question is simply never, as, for some K and n, there are some constraints which apply to $\rho_{E,n}(G_K)$ for every elliptic curve $E/\mathbb{Q}$ and force it to be non-maximal. Recall that for each positive integer n we have an isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ given by mapping an automorphism σ to the class m_σ such that

$$\sigma(\zeta_n) = \zeta_n^{m_\sigma}.$$

Definition 5.1.1. For each finite Galois extension $K/\mathbb{Q}$ and positive integer n, we write $D_{K,n} \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ for the image of the subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K \cap \mathbb{Q}(\zeta_n)) \leq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ under the isomorphism above. We then define

$$\Gamma_{K,n} = \{g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \ : \ \det(g) \in D_{K,n}\}.$$

Lemma 5.1.2. *For every elliptic curve $E/\mathbb{Q}$, every integer $n \geq 2$ and every finite extension $K/\mathbb{Q}$ we have an inclusion*

$$\rho_{E,n}(G_K) \subseteq \Gamma_{K,n}$$

Proof. The set $D_{K,n}$ functions as our set of allowed determinants, since $\det \circ \rho_{E,n} = \chi_n$ where χ_n is the cyclotomic character cutting out the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. In particular, elements of $\rho_{E,n}(G_K)$ can only have determinants inside of $D_{K,n}$ and so certainly $\rho_{E,N}(G_K) \subseteq \Gamma_{K,n}$. □

Remark 5.1.3. Note that if n_1, n_2 are coprime integers then the Chinese remainder theorem induces natural isomorphisms

$$\Gamma_{K,n_1n_2} \cong \Gamma_{K,n_1} \times \Gamma_{K,n_2}$$

which commute with the analogous splittings of $\mathrm{GL}_2(\mathbb{Z}/n_1n_2\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/n_1n_2\mathbb{Z})$

One can then restrict our question above to a more sensible one: how often is $\rho_{E,n}(G_K)$ actually equal to the subgroup $\Gamma_{K,n}$? In this section we will will show that,

for fixed n and K, equality holds for 100% of $E/\mathbb{Q}$. For this, we will use the large sieve in much the same way as Duke [Duk97], with adaptations similar to those found in later work of Zywina [Zyw10].

§ 5.1.1 | Large Sieve

We now state the version of the large sieve that we will use. Let Ω be a function which associates to each prime number p a subset $\Omega(p) \subseteq \mathbb{F}_p^2$. Moreover, for every $X > 0$ and every pair $(r, s) \in \mathbb{Z}^2$ we then define

$$P_\Omega(X) = \sum_{p \leq X} \frac{\Omega(p)}{p^2},$$
$$P_\Omega(X; (r,s)) = \#\left\{p \leq X \ : \ (r,s) \bmod p \in \Omega(p)\right\}.$$

Lemma 5.1.4. *There exists a uniform constant $c \in \mathbb{R}$ such that the following is true. Let $\mathcal{B} = [-N_1, N_1] \times [-N_2, N_2] \subset \mathbb{R}^2$ for some $N_i \in \mathbb{R}_{>0}$, and Ω be a function as above. For all real numbers X such that $\min_i \{N_i\} \geq X^2$ we have that*

$$\sum_{\mathbf{m} \in \mathbb{Z}^2 \cap \mathcal{B}} \left(P_\Omega(X; \mathbf{m}) - P_\Omega(X)\right)^2 \leq c N_1 N_2 P_\Omega(X).$$

Proof. This is an elementary extension of [Gal73, Lemma A] by using the estimate in [Hux68, Theorem 1] to bound the exponential sums in the proof (see also [Duk97, Lemma 1]). □

We then apply this to our specific counting problem in a manner similar to, for example, [Gal73, Lemma B].

Proposition 5.1.5. *There exists a uniform constant c such that the following holds. Let Ω be a function as above, and X a real number such that there is a prime number $p \leq X^{1/6}$ with $\#\Omega(p) \neq 0$. Write*

$$\mathcal{E}(X; \Omega) := \left\{(A,B) \in \mathcal{E}(X) \ : \ (A,B) \bmod p \notin \Omega(p) \ \forall p\right\}.$$

Then

$$\#\mathcal{E}(X; \Omega) \leq \frac{c X^{5/6}}{P_\Omega(X^{1/6})}$$

Proof. Note that for $(A, B) \in \mathcal{E}(X; \Omega)$, we have that $P_\Omega(X^{1/6}; (A, B)) = 0$, so that

$$\sum_{(A,B) \in \mathcal{E}(X;\Omega)} 1 \leq P_\Omega(X^{1/6})^{-2} \sum_{(A,B) \in \mathcal{E}(X)} \left(P_\Omega(X^{1/6}; (A,B)) - P_\Omega(X^{1/6})\right)^2.$$

Let $\mathcal{B} = \left\{(a,b) \in \mathbb{R}^2 \ : \ |a|^3, b^2 \leq X\right\}$, which clearly contains the lattice points $\mathcal{E}(X)$ and has minimal width $X^{1/3}$. In light of Lemma 5.1.4, we then have that

$$P_\Omega(X^{1/6})^{-2} \sum_{(A,B) \in \mathcal{E}(X)} \left(P_\Omega(X^{1/6}; \mathbf{m}) - P_\Omega(X^{1/6})\right)^2 \leq c P_\Omega(X^{1/6})^{-1} X^{5/6}.$$

□

§ 5.1.2 | Sieving for Conjugacy Classes

We now apply the large sieve in the form presented in §5.1.1 to study $\rho_{E,n}(K)$ for $E/\mathbb{Q}$ ordered by height. Our approach, similar to that of Zywina, is to show that for each fixed conjugacy class C in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, the image $\rho_{E,n}(G_K)$ must meet $C \cap \Gamma_{K,n}$ almost always. Then since there are only finitely many conjugacy classes we are able to conclude that the image must actually be $\Gamma_{K,n}$ almost always.

Definition 5.1.6. For each finite Galois extension $K/\mathbb{Q}$, positive integer n and $d \in D_{K,n}$ we write

$$\mathcal{P}_{K,n}^{(d)} = \left\{ p \text{ prime number } : \begin{smallmatrix} p>3 \\ p \equiv d \bmod n \\ p \text{ totally split in } K/\mathbb{Q} \end{smallmatrix} \right\}.$$

Moreover, we write for each $X \in \mathbb{R}$,

$$\mathcal{P}_{K,n}^{(d)}(X) := \left\{ p \in \mathcal{P}_{K,n}^{(d)} \mid p \leq X \right\}.$$

Remark 5.1.7. Since $d \in D_{K,n}$, the set $\mathcal{P}_{K,n}(d)$ is infinite by the Chebotarev density theorem, since if $L_{K,n} = K \cap \mathbb{Q}(\zeta_n)$

$$\mathcal{P}_{K,n}^{(d)} = \left\{ p \text{ prime number } : \begin{smallmatrix} p \text{ unramified in } K\cdot\mathbb{Q}(\zeta_n)/\mathbb{Q} \\ \mathrm{Frob}_p=(\mathrm{Id},d)\in \mathrm{Gal}(K/L_{K,n})\times\mathrm{Gal}(\mathbb{Q}(\zeta_n)/L_{K,n})\subseteq\mathrm{Gal}(K\cdot\mathbb{Q}(\zeta_n)/\mathbb{Q}) \end{smallmatrix} \right\}.$$

In fact, this shows that as $X \to \infty$ we have

$$\#\mathcal{P}_{K,n}^{(d)}(X) \sim \frac{1}{[K \cdot \mathbb{Q}(\zeta_n) : \mathbb{Q}]} \frac{X}{\log(X)}$$

For an integer $n > 0$, a finite Galois extension $K/\mathbb{Q}$, a conjugacy class $C \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and a real number X we define, in analogue to [Zyw10, §5.1],

$$Y_{K,n}(X; C) = \left\{ (A, B) \in \mathcal{E}(X) \ : \ \rho_{E_{A,B},n}(G_K) \cap C = \emptyset \right\}.$$

We note that this is not the same set as in [Zyw10, §5.1], indeed we are considering elliptic curves over $\mathbb{Q}$ but the image of G_K.

Proposition 5.1.8. *There exist uniform constants c_0, c_1 such that the following holds. Let $K/\mathbb{Q}$ be a finite Galois extension, n be a positive integer, $d \in D_{K,n}$ and $C \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a conjugacy class of elements with determinant d. Then for all $X \in \mathbb{R}_{>0}$ such that $\mathcal{P}_{K,n}^{(d)}(X) \neq \emptyset$ we have that*

$$\#Y_{K,n}(X; C) \leq c_0 X^{5/6} \left(\frac{|C|}{\#\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})} \mathcal{P}_{K,n}^{(d)}(X^{1/6}) - c_1 n^5 X^{1/12} \right)^{-1}.$$

Proof. We will use the large sieve. For $p \in \mathcal{P}_{K,n}(d)$ define

$$\Omega(p) = \left\{ (r, s) \in \mathbb{F}_p^2 \ : \ 4r^3 + 27s^2 \neq 0 \text{ and } \rho_{E_{r,s},n}(\mathrm{Frob}_p) \in C \right\}.$$

If $(A, B) \in \mathcal{E}(X)$ lies (modulo p) in $\Omega(p)$ for such a prime, then $E_{A,B}$ has good reduction at p and $\rho_{E_{A,B},n}(G_K) \cap C$ contains the image of the frobenius element over p, so in

particular $(A,B) \notin Y_{K,n}(X;C)$. For the remaining prime numbers we set $\Omega(p) = \emptyset$. Thus we have

$$\#Y_{K,n}(X;C) \leq \#\mathcal{E}(X;\Omega) \leq \frac{c_0 X^{5/6}}{P_\Omega(X^{1/6})},$$

where the second inequality is by Proposition 5.1.5 and c_0 is an absolute constant. By [Jon10, Theorem 8] we have that there is an absolute constant c_1' such that

$$\left|\frac{\Omega(p)}{p^2} - \frac{|C|}{\#\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})}\right| \leq c_1' \frac{m^5}{p^{1/2}},$$

and so in particular, estimating this error by the integral, we obtain that there is an absolute constant c_1 such that

$$P_\Omega(X^{1/6}) \geq \frac{|C|}{\#\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})}\mathcal{P}_{K,n}^{(d)}(X^{1/6}) - c_1 n^5 X^{1/12},$$

completing the result. □

§ 5.1.3 | Galois Image

Immediately we know that, for a fixed extension field $K/\mathbb{Q}$ and integer $n \geq 2$, 100% of elliptic curves over $\mathbb{Q}$ retain the largest possible Galois image on n-torsion.

Theorem 5.1.9. *Let $K/\mathbb{Q}$ be a finite Galois extension and $n \geq 2$ be an integer. Recall the group $\Gamma_{K,n}$ of Definition 5.1.1. Then*

$$\frac{\#\left\{(A,B) \in \mathcal{E}(X) \ : \ \rho_{E_{A,B},n}(G_K) \neq \Gamma_{K,n}\right\}}{\#\mathcal{E}(X)} \ll_{n,K} \frac{\log(X)}{X^{1/6}}$$

Proof. By [Zyw10, Lemma A.10] we have that if $H \leq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is a subgroup which meets every conjugacy class with determinant 1 nontrivially, then $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z}) \leq H$. Moreover, it then follows that if $D_{K,n} = \det(H)$ then we must have that $H = \Gamma_{K,n}$.

Let $C_1, \ldots, C_k$ be a complete list of conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with determinant in $D_{K,n}$, then by the above discussion (and Lemma 5.1.2)

$$\left\{(A,B) \in \mathcal{E}(X) \ : \ \rho_{E_{A,B},n}(G_K) \neq \Gamma_{K,n}\right\} \subseteq \bigcup_{i=1}^{k} Y_{K,n}(X;C_i),$$

so that by Proposition 5.1.8 we have

$$\begin{aligned}&\left\{(A,B) \in \mathcal{E}(X) \ : \ \rho_{E_{A,B},n}(G_K) \neq \Gamma_{K,n}\right\} \\ &\quad \ll X^{5/6} \sum_{i=1}^{k} \left(\frac{|C_i|}{\#\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})}\mathcal{P}_{K,n}^{(d)}(X^{1/6}) - c_1 n^5 X^{1/12}\right)^{-1}.\end{aligned}$$

Now, note that for all i we have by the Chebotarev density theorem as in Remark 5.1.7

$$\left|\frac{|C_i|}{\#\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})}\mathcal{P}_{K,n}^{(d)}(X^{1/6}) - c_1 n^5 X^{1/12}\right| \gg_{n,K} \frac{X^{1/6}}{\log(X)},$$

completing the result. □

In particular, this shows that almost no elliptic curves have nontrivial n-torsion over a fixed extension, which will be of use to us later in this thesis.

Corollary 5.1.10. *Let n be a positive integer and let $K/\mathbb{Q}$ be a finite Galois extension. Then*

$$\frac{\#\left\{(A,B)\in\mathcal{E}(X)\ :\ E_{A,B}(K)[n] \text{ is nontrivial}\right\}}{\#\mathcal{E}(X)} \ll_{n,K} \frac{\log(X)}{X^{1/6}}.$$

Proof. Since the action of $\Gamma_{K,n} \supseteq \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ on $(\mathbb{Z}/n\mathbb{Z})^2$ has no fixed points, this follows from Theorem 5.1.9. □

§ 5.2 | Good Characteristic: Weil Restriction

For the duration of this section, fix a finite Galois extension of number fields K/F and an elliptic curve $E/\mathbb{Q}$, and write $G = \mathrm{Gal}(K/F)$. We begin in §5.2.1 with expository material on twists of elliptic curves and the Weil restriction. In §5.2.2 we then go on to survey some results on p-Selmer groups in extensions of degree coprime to p. This material is closely related to, and inspired by, that appearing in [MR07, §3]. Finally, in §5.2.3, we explain how this material allows us to extend the results of Bhargava and Shankar [BS15b, BS13] on the average dimension of 3- and 5-Selmer groups over $\mathbb{Q}$ to a bound for the average dimension of 3- and 5-Selmer groups over any multiquadratic number field.

§ 5.2.1 | Twists of Elliptic Curves

As in Milne [Mil72, §2] (see also [MRS07]), there is a general construction of twists of powers of an elliptic curve, which we now recall.

Definition 5.2.1. Let $n \geq 1$. To each matrix $M = (m_{i,j})$ in $\mathrm{Mat}_n(\mathbb{Z})$ we can associate an endomorphism of E^n given by

$$(P_1, ..., P_n) \longmapsto \left(\sum_{j=1}^{n} m_{1,j}P_j, ..., \sum_{j=1}^{n} m_{n,j}P_j\right).$$

In this way we view $\mathrm{GL}_n(\mathbb{Z})$ as a subgroup of $\mathrm{Aut}_{\mathbb{Q}}(E^n)$. Now suppose that Λ is a free rank-n $\mathbb{Z}$-module equipped with a continuous $G_{\mathbb{Q}}$-action. Choosing a basis for Λ gives rise to a homomorphism

$$\rho_\Lambda : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_n(\mathbb{Z}),$$

which we view as a 1-cocycle valued in $\mathrm{Aut}_{\overline{\mathbb{Q}}}(E^n)$. The class of ρ_Λ in $H^1(\mathbb{Q}, \mathrm{Aut}_{\overline{\mathbb{Q}}}(E^n))$ does not depend on the choice of basis. Associated to this cocycle class is a twist of E^n, which we denote $\Lambda \otimes E$. This is an abelian variety over $\mathbb{Q}$ of dimension n, equipped with a $\overline{\mathbb{Q}}$-isomorphism $\varphi_\Lambda : E^n \to \Lambda \otimes E$ satisfying $\varphi_\Lambda^{-1}\varphi_\Lambda^\sigma = \rho_\Lambda(\sigma)$ for all $\sigma \in G_{\mathbb{Q}}$.

The Weil restriction of E can now be defined as a specific example of such a twist.

Definition 5.2.2. The Weil restriction of E from K to F is the abelian variety

$$\mathrm{Res}_{K/F}E = \mathbb{Z}[G] \otimes E.$$

Remark 5.2.3. The Weil restriction $\mathrm{Res}_{K/F}E$ is classically defined as the unique scheme over F representing the functor on F-schemes

$$T \longmapsto E(T \times_F K).$$

As in [MRS07, Theorem 4.1], this is equivalent to the construction given above.

§ 5.2.2 | Selmer Groups in Good Characteristic

Here we remark on the structure of n-Selmer groups in the case that n is coprime to $\#G$, the case of so–called "good characteristic". In this case, the n-Selmer group splits as a sum over twists of E. This can be viewed as a finite-level explication of the results in [MR07, §3], where similar results are shown for Pontryagin dual p^∞–Selmer vector spaces without our restriction on p.

Lemma 5.2.4. *For every positive integer n,*

(i) there is a natural isomorphism of $\mathbb{Z}[G_F]$–modules

$$\mathrm{Res}_{K/F}E[n] \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} E[n],$$

where $\sigma \in G_F$ acts on the right hand side diagonally,

(ii) the above isomorphism induces an isomorphism of $\mathbb{Z}[G]$–modules

$$\mathrm{Sel}_n(\mathrm{Res}_{K/F}E/F) \cong \mathrm{Sel}_n(E/K),$$

where the action of G on the left hand side is induced by the action of G on $\mathbb{Z}[G]$ by left multiplication.

Proof. (i) is found in [MRS07, Theorem 2.2(ii)], see also [Mil72, §1(a)]. For (ii), we give an analogous argument to that in [MR07, proof of Proposition 3.1(iii)], see also [Mil72, Proof of Theorem 1] for an similar result for Shafarevich–Tate groups. Indeed, by (i), Shapiro's lemma (see, e.g. [Neu13, Theorem 4.9]) provides a $\mathbb{Z}[G]$ isomorphism

$$H^1(F, (\mathrm{Res}_{K/F}E)[n]) \cong H^1(K, E[n]),$$

where the action of G on the left hand side is induced by left multiplication on $\mathbb{Z}[G]$ in the isomorphism of (i). It is then elementary to check that this isomorphism commutes with the corresponding isomorphisms at the local extensions, and thus restricts to one of Selmer groups. □

Definition 5.2.5. Let ρ be an irreducible finite dimensional $\mathbb{Q}[G]$–module. As in [MRS07, Definition 4.3] we define the twist of E by ρ to be

$$E_\rho = (\mathbb{Q}[G]_\rho \cap \mathbb{Z}[G]) \otimes E,$$

where $\mathbb{Q}[G]_\rho$ is the ρ-isotypic component of $\mathbb{Q}[G]$, that is, the sum of all left ideals of $\mathbb{Q}[G]$ isomorphic to ρ.

Example 5.2.6. *If K/F is multiquadratic then these twists are extremely concrete. Let $\Delta \in F$ be an element such that $F(\sqrt{\Delta}) \subseteq K$, and let χ_Δ be the corresponding at–most–quadratic character of G_F. Identifying χ_Δ with its corresponding one dimensional $\mathbb{Q}[G]$-module, this construction gives rise to all irreducible finite-dimensional $\mathbb{Q}[G]$-modules. Moreover, it is clear that $\mathbb{Q}[G]_{\chi_\Delta} \cap \mathbb{Z}[G]$ is a rank one free abelian group with action of $\sigma \in G$ given by multiplication by $\chi_\Delta(\sigma)$. In particular, by* [MRS07, Theorem 2.2(i)] *we obtain that $E_{\chi_\Delta} = E^{(\Delta)}$ is just the usual quadratic twist of E by Δ.*

We can then split the n-Selmer group of the Weil restriction into those of these twists. This result is analogous to [MR07, Corollary 3.7], where they study the Pontryagin dual Selmer vector spaces.

Proposition 5.2.7. *If n is an integer which is coprime to $\#G$, then we have an isomorphism of $\mathbb{Z}[G]$-modules*

$$\mathrm{Sel}_n(E/K) \cong \bigoplus_\rho \mathrm{Sel}_n(E_\rho/F),$$

where the sum is over isomorphism classes of irreducible finite dimensional $\mathbb{Q}[G]$-modules and the action of G on the summands on the right hand side is induced by the action of G on $\mathbb{Q}[G]_\rho \cap \mathbb{Z}[G]$ via the isomorphism in Lemma 5.2.4(i).

Proof. By Lemma 5.2.4 we need only show that $\mathrm{Sel}_n(\mathrm{Res}_{K/F}E/F)$ splits in this way. The natural map

$$f : \bigoplus_\rho (\mathbb{Z}[G] \cap \mathbb{Q}[G]_\rho) \to \mathbb{Z}[G],$$

is injective with finite cokernel, so by [MRS07, Theorem 4.5, see also Lemma 2.4] induces an F–isogeny

$$f_E : \bigoplus_\rho E_\rho \to \mathrm{Res}_{K/F}E.$$

Moreover, since the cokernel of f is $\#G$–torsion, the degree of the isogeny f_E must be a divisor of some power of $\#G$ [MRS07, proof of Lemma 2.4] and so coprime to n. In particular, f_E induces an isomorphism of n–Selmer groups, and moreover since f_E is an F–isogeny the isomorphism is one of $\mathbb{Z}[G]$–modules. □

Remark 5.2.8. In [MR07, Corollary 3.7] the authors do not need to make assumptions about coprimality, since the error that occurs when $p \mid \#G$ contributes an additional torsion module to the p^∞-Selmer groups. This in turn vanishes when taking the tensor product with $\mathbb{Q}_p$ to form the Pontryagin dual Selmer vector space $\mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/K), \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathbb{Q}_p$.

§ 5.2.3 | Average Selmer Ranks in Good Characteristic over Multiquadratic Fields

In this subsection, we will restrict our interest to multiquadratic number fields. We use the Weil restriction as in §5.2 to give a bound for Selmer ranks in good characteristic using results of Bhargava and Shankar [BS15b, BS13]. Their ordering is slightly

different to the one that we are working with, so for the purposes of using their results we define for each $X \in \mathbb{R}$ the set

$$\mathcal{E}'(X) = \left\{(A,B) \in \mathcal{E} \ : \ \max\left\{4\left|A\right|^3, 27B^2\right\} \leq X\right\}.$$

Now, we adapt the results of Bhargava–Shankar for quadratic twists.

Proposition 5.2.9. *For each squarefree integer D and $p \in \{2,3,5\}$, we have*

$$\lim_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}'(X)} \#\mathrm{Sel}_p(E_{A,B}^{(D)}/\mathbb{Q})}{\#\mathcal{E}'(X)} = (p+1).$$

Moreover, assuming Hypothesis 1 the conclusion holds for every prime number p.

Proof. Fix a squarefree integer D. Note that the quadratic twist $E_{A,B}^{(D)}$ has a (possibly not minimal) Weierstrass equation given by $E_{AD^2,BD^3} : y^2 = x^3 + AD^2x + BD^3$. Thus there is a bijection between $\left\{E_{A,B}^{(D)} \ : \ (A,B) \in \mathcal{E}'(X)\right\}$ and the set

$$\mathcal{E}'_D(X) = \left\{(A,B) \in \mathbb{Z}^2 \ : \ \begin{array}{c} 4|A|^3, 27B^2 \leq D^6X; \\ D^2|A, D^3|B; \\ 4A^3+27B^2\neq 0; \\ \forall \ell\nmid D \text{ prime, if } \ell^4|A \text{ then } \ell^6\nmid B; \\ \forall \ell|D \text{ prime, if } \ell^6|A \text{ then } \ell^9\nmid B \end{array}\right\},$$

given by identifying $(A,B) \in \mathcal{E}'_D(X)$ with the curve $E_{A,B}$. We now partition $\mathcal{E}'_D(X)$ into parts, so as to identify with minimal Weierstrass models. For each pair (d_1,d_2) of positive squarefree integers such that $D = \pm d_1d_2$, we define

$$\mathcal{E}'_{d_1,d_2}(X) = \left\{(A,B) \in \mathcal{E}'(D^6X) \ : \ \begin{array}{c} 4|A|^3, 27B^2 \leq \left(\frac{d_1}{d_2}\right)^6 X; \\ 4A^3+27B^2\neq 0; \\ \forall \ell\nmid d_1d_2 \text{ prime, if } \ell^4|A \text{ then } \ell^6\nmid B; \\ \forall \ell|d_1 \text{ prime: } \ell^2|A,\ \ell^3|B, \text{ and if } \ell^4|A \text{ then } \ell^6\nmid B; \\ \forall \ell|d_2 \text{ prime: if } \ell^2|A \text{ then } \ell^3\nmid B. \end{array}\right\}.$$

Note that $\mathcal{E}'_{d_1,d_2}(X) \subseteq \mathcal{E}'\left((\frac{d_1}{d_2})^6X\right)$, and moreover $\mathcal{E}'_{d_1,d_2}(X)$ parametrises a large family of elliptic curves ordered by naïve height in the sense of Bhargava–Shankar [BS15a, BS15b, BS13]. Further, we have that

$$\mathcal{E}'_D(X) = \bigsqcup_{D=\pm d_1d_2} \left\{(d_2^4A, d_2^6B) \ : \ (A,B) \in \mathcal{E}'_{d_1,d_2}(X)\right\},$$

where the disjoint union is over pairs of squarefree positive integers d_1, d_2 satisfying $D = \pm d_1d_2$.

Note that for any fixed pair of squarefree positive integers d_1, d_2 we have by [BS15a,

Theorem 3.17] that

$$\lim_{X\to\infty}\frac{\#\mathcal{E}'_{d_1,d_2}(X)}{\#\mathcal{E}'(X)}=\left(\prod_{\substack{\ell\mid d_1\\ \text{prime}}}\frac{(\ell^2-1)\ell^3+(\ell^3-1)}{\ell^{10}-1}\right)\left(\prod_{\substack{\ell\mid d_2\\ \text{prime}}}\frac{\ell^2(\ell^2-1)\ell^6+\ell^2(\ell^3-1)\ell^3}{\ell^{10}-1}\right)$$
$$=d_2^5\left(\prod_{\substack{\ell\mid D\\ \text{prime}}}\frac{\ell^5-1}{\ell^{10}-1}\right).$$

Thus,

$$\begin{aligned}
&\lim_{X\to\infty}\frac{1}{\#\mathcal{E}'(X)}\sum_{(A,B)\in\mathcal{E}'(X)}\#\mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})\\
&=\lim_{X\to\infty}\frac{1}{\#\mathcal{E}'(X)}\sum_{(A,B)\in\mathcal{E}'_D(X)}\#\mathrm{Sel}_p(E_{A,B}/\mathbb{Q})\\
&=\lim_{X\to\infty}\frac{1}{\#\mathcal{E}'(X)}\sum_{D=\pm d_1d_2}\sum_{(A,B)\in\mathcal{E}'_{d_1,d_2}(X)}\#\mathrm{Sel}_p(E_{A,B}/\mathbb{Q})\\
&=(p+1)\left(\prod_{\substack{\ell\mid D\\ \text{prime}}}\frac{\ell^5-1}{\ell^{10}-1}\right)\sum_{d\mid D}d^5\\
&=(p+1),
\end{aligned}$$

where the penultimate equality follows from the large family average Selmer group sizes in [BS15a, BS15b, BS13] and the computation above, and the final follows from an elementary identity for power-of-divisor sums.

Assuming Hypothesis 1, since the families $\mathcal{E}'_{d_1,d_2}(X)$ are defined by finitely many congruence conditions, the argument above holds for all prime numbers p. □

We can then relate this to our ordering via elementary estimates, and similarly obtain a bound for the average Selmer rank.

Proposition 5.2.10. *For each squarefree integer D and $p\in\{2,3,5\}$, we have*

$$\limsup_{X\to\infty}\frac{\sum_{(A,B)\in\mathcal{E}(X)}\dim\mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}(X)}\leq\left(\frac{27}{4}\right)^{5/6}\frac{(p+1)}{p}.$$

Moreover, assuming Hypothesis 1 the same is true for every prime number p.

Proof. For every real number X, there are clear inclusions

$$\mathcal{E}'(4X)\subseteq\mathcal{E}(X)\subseteq\mathcal{E}'\left(27X\right).$$

In particular

$$\frac{\sum_{(A,B)\in\mathcal{E}(X)}\dim\mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}(X)}\leq\frac{\sum_{(A,B)\in\mathcal{E}'(27X)}\dim\mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}'(4X)}.$$

For each $r \geq 0$ there is an elementary inequality $p^r \geq pr$, so for each $E/\mathbb{Q}$ we have $\dim \mathrm{Sel}_p(E/\mathbb{Q}) \leq \#\mathrm{Sel}_p(E/\mathbb{Q})/p$. Hence

$$\frac{\sum_{(A,B)\in\mathcal{E}'(27X)} \dim \mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}'(4X)} \leq \frac{1}{p}\frac{\sum_{(A,B)\in\mathcal{E}'(27X)} \#\mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}'(4X)}.$$

Finally, by [BS15a, Theorem 3.17] $\#\mathcal{E}'(X) \sim cX^{5/6}$ for some absolute constant c, and so using Proposition 5.2.9 we obtain

$$\lim_{X\to\infty} \frac{1}{p}\frac{\sum_{(A,B)\in\mathcal{E}'(27X)} \#\mathrm{Sel}_p(E^{(D)}_{A,B}/\mathbb{Q})}{\#\mathcal{E}'(4X)} = \left(\frac{27}{4}\right)^{5/6} \frac{(p+1)}{p},$$

providing the required bound. □

Remark 5.2.11. In fact, the way that Conjecture 1 is stated in [PR12] (and indeed that Hypothesis 1 is stated) suggests that we should expect to be able to remove the $\left(\frac{27}{4}\right)^{5/6}$ factor in our bound. However this does not contribute to the general shape of our bounds, so in the interests of maintaining uniformity with what is currently known we shall use the weaker bound.

Definition 5.2.12. For a squarefree integer D, we write χ_D for the quadratic character of $G_\mathbb{Q}$ cutting out $\mathbb{Q}(\sqrt{D})$, and for an abelian group M we write M^{χ_D} for the discrete $G_\mathbb{Q}$-module M with action by $\sigma \in G_\mathbb{Q}$ given by multiplication by $\chi_D(\sigma) \in \{\pm 1\}$.

Lemma 5.2.13. *Let F be a field contained in a multiquadratic number field, write $G = \mathrm{Gal}(F/\mathbb{Q})$, and let $E/\mathbb{Q}$ be an elliptic curve. Then for every odd prime number p there is an isomorphism of $\mathbb{Z}[G]$-modules*

$$\mathrm{Sel}_p(E/F) \cong \bigoplus_{D\in\mathcal{Q}(F)} \mathrm{Sel}_p(E^{(D)}/\mathbb{Q})^{\chi_D},$$

where $\mathcal{Q}(F)$ is the set of squarefree integers D such that $\mathbb{Q}(\sqrt{D}) \subseteq F$ and $E^{(D)}$ is the quadratic twist of E by D.

Proof. This follows by applying Proposition 5.2.7 to multiquadratic extensions as in Example 5.2.6. □

Now we can state an easy statistical consequence of Lemma 5.2.13.

Proposition 5.2.14. *Let F be either $\mathbb{Q}$ or a multiquadratic number field. Then for $p \in \{3, 5\}$,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/F)}{\#\mathcal{E}(X)} \leq 3^{5/2}\frac{p+1}{p}[F:\mathbb{Q}],$$

Moreover, assuming Hypothesis 1 the same holds for all odd prime numbers p.

Proof. Let p be an odd prime number. Using the decomposition in Lemma 5.2.13 we have that

$$\dim \mathrm{Sel}_p(E/F) = \sum_{D\in Q(F)} \dim \mathrm{Sel}_p(E^{(D)}/\mathbb{Q}),$$

where $E^{(D)}$ is the quadratic twist of E by D and $\mathcal{Q}(F)$ is the set of squarefree integers D such that $\mathbb{Q}(\sqrt{D}) \subseteq F$. The result now follows from Proposition 5.2.10, noting that the size of $\mathcal{Q}(F)$ is precisely $[F : \mathbb{Q}]$. □

§ 5.3 | Galois Descent for p-Selmer Groups

We will now use the algebraic results of §3.1 and §2.2 to obtain our statistical results. This will culminate in a proof of Theorem 1.3.8 which tells us that, for a finite Galois extension of number fields K/F and a prime number p, as we vary over the E parametrised by $\mathcal{E}(X)$, the average value of

$$\left|\dim \mathrm{Sel}_p(E/K)^{\mathrm{Gal}(K/F)} - \dim \mathrm{Sel}_p(E/F)\right|,$$

which we refer to as the failure of Galois descent, is bounded as $X \to \infty$. We use Lemma 2.2.72.3 to relate the Selmer group $\mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])$ to the Galois fixed space, which allows us to use Lemma 2.2.11 to bound this failure of Galois descent by the genus theory invariant $g_p(K/F; E)$. The remainder of the proof is then showing that the function $g_p(K/F; E)$ has bounded average as E varies in $\mathcal{E}$.

§ 5.3.1 | Preliminary Counting Lemmas

We begin by recalling the description, afforded by Tate's algorithm, of the reduction type of the curves $E_{A,B}$ in terms of the pair $(A, B) \in \mathcal{E}$ at almost all places.

Lemma 5.3.1. *For a prime number $\ell \geq 5$ and $(A, B) \in \mathcal{E}$, the reduction type of $E_{A,B}/\mathbb{Q}_\ell$ is*

- *I_n for $n > 0$ if and only if $v_\ell(4A^3 + 27B^2) = n$ and $v_\ell(AB) = 0$,*
- *additive if and only if $v_\ell(\gcd(A, B)) > 0$,*

where v_ℓ is the normalised valuation on $\mathbb{Q}_\ell$.

Proof. This is a consequence of Tate's algorithm, see Appendix A. □

Proposition 5.3.2. *There exists a constant $C > 0$ such that for all real numbers $X \in \mathbb{R}_{\geq 2}$,*

$$\sum_{(A,B)\in\mathcal{E}(X)} \#\left\{\ell \geq \log(X) \ : \ \begin{array}{c}\ell \text{ is prime;} \\ E_{A,B}/\mathbb{Q}_\ell \text{ has bad reduction of type different from } I_1.\end{array}\right\} \leq C\left(\frac{X^{5/6}}{\log(X)}\right).$$

Proof. We split the summand into counts of additive and multiplicative primes.

By Lemma 5.3.1, primes of additive reduction for $E_{A,B}$ divide $\gcd(A, B)$, so are

bounded by the absolute values of A and B. Therefore, we have

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}(X)} \#\left\{\ell \geq \log(X) \ : \ \substack{\ell \text{ is prime;} \\ E_{A,B}/\mathbb{Q}_\ell \text{ has additive reduction.}}\right\} \\
&\leq \sum_{\substack{\log(X)\leq\ell\leq X^{1/3} \\ \text{prime}}} \sum_{\substack{|A|\leq X^{1/3} \\ \ell|A}} \sum_{\substack{|B|\leq X^{1/2} \\ \ell|B}} 1 \\
&\ll \sum_{\substack{\log(X)\leq\ell\leq X^{1/3} \\ \text{prime}}} \left(\frac{4X^{5/6}}{\ell^2} + O\left(\frac{X^{1/2}}{\ell}\right)\right) \\
&\ll \left(X^{5/6}\int_{\log(X)}^{X^{1/3}} \frac{1}{y^2}dy\right) + X^{1/2}\log\log(X) \\
&\ll \frac{X^{5/6}}{\log(X)},
\end{aligned}$$

where the penultimate inequality uses an integral estimate for the main term, that the sum of reciprocals of prime numbers has order $\log\log(X)$ and the prime number theorem for the error term.

For the multiplicative primes: Lemma 5.3.1 shows that if ℓ is multiplicative of type different from I_1 for $E_{A,B}$ then $\ell^2 \mid (4A^3 + 27B^2)$ but $\ell \nmid AB$. Hence we have

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}(X)} \#\left\{\ell \geq \log(X) \ : \ \substack{\ell \text{ is prime;} \\ E_{A,B}/\mathbb{Q}_\ell \text{ has multiplicative reduction of type different from } I_1.}\right\} \\
&\leq \sum_{\substack{\log(X)\leq\ell\leq\sqrt{31X} \\ \text{prime}}} \sum_{\substack{|A|\leq X^{1/3} \\ \ell\nmid A}} \sum_{\substack{|B|\leq X^{1/2} \\ \ell^2|4A^3+27B^2}} 1 \\
&\ll \sum_{\substack{\log(X)\leq\ell\leq\sqrt{31X} \\ \text{prime}}} \left(\frac{X^{5/6}}{\ell^2} + O\left(X^{1/3}\right)\right) \\
&\ll \frac{X^{5/6}}{\log(X)}.
\end{aligned}$$

The result follows. □

§ 5.3.2 | Bounding the Genus Theory Invariant

We begin by noting some elementary bounds on the norm indices which occur as summands in the genus theory invariant (as in Definition 2.2.8).

Lemma 5.3.3. *Let F be a number field, K/F be a finite extension, p be a prime number and E/F be an elliptic curve. For every $v \in \Omega_F$ and each $w \in \Omega_K$ extending v we have that*

$$\dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right) \leq \begin{cases} 2 + [F_v : \mathbb{Q}_p] & \text{if } v|p, \\ 2 & \text{if } v \text{ is a finite place and } v\nmid p, \\ 1 & \text{if } v \text{ is a real place and } p=2, \\ 0 & \text{otherwise.} \end{cases} \tag{5.1}$$

Proof. We note that these norm indices are bounded above by $\dim E(F_v)/pE(F_v)$, so we estimate this instead.

For each finite place $\mathfrak{p} \in \Omega_F$ and each $E/\mathbb{Q}$, there is a finite index subgroup, arising from the filtration by formal groups, of $E(F_\mathfrak{p})$ which is isomorphic to the additive group of integers $\mathcal{O}_\mathfrak{p}$ of $F_\mathfrak{p}$ (see e.g. [Sil09, VII Prop. 6.3]). Thus these norm indices are bounded by

$$\#E(F_\mathfrak{p})/pE(F_\mathfrak{p}) = (\#E(F_\mathfrak{p})[p])(\#\mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}) \leq \begin{cases} p^{2+[F_\mathfrak{p}:\mathbb{Q}_p]} & \mathfrak{p} \mid p, \\ p^2 & \text{else.} \end{cases} \tag{5.2}$$

Moreover, for archimedean places $v \in \Omega_F$, if p is odd or v is complex then we have $\dim E(F_v)/pE(F_v) \leq \dim H^1(F_v, E[p]) = 0$. If, on the other hand, $p = 2$ and v is real then elementary computations show that the dimension of the quotient at v is at most 1. □

We are now mathematically ready to bound the average of the genus theory invariant, but first we require a small amount of notation.

Notation 5.3.4. For a number field F, we define the function ω_F on the set of ideals of the integers of F to send the ideal I to

$$\omega_F(I) := \#\left\{\mathfrak{p} \in \Omega_F \ : \ \mathfrak{p} \mid I\right\}.$$

We also define $r_1(F)$ to be the number of real embeddings of F. Moreover, δ_2 is the function which takes each prime number p to 1 if $p = 2$ and 0 otherwise.

We now bound the average of the genus theory invariant.

Proposition 5.3.5. *For every number field F, finite Galois extension K/F, prime number p and real number $X \in \mathbb{R}_{>0}$ we have*

$$\frac{\sum\limits_{(A,B)\in\mathcal{E}(X)} g_p(K/F; E_{A,B})}{\#\mathcal{E}(X)} \leq C_p(K/F) + O\left(\frac{[F:\mathbb{Q}]}{\log(X)}\right),$$

where

$$C_p(K/F) = 2\omega_F(6p\Delta_K) + [F:\mathbb{Q}] + \delta_2(p)r_1(F) + 2\sum_{\substack{\ell \text{ prime} \\ \ell \nmid 6p\Delta_K}} \omega_F(\ell)\frac{2\ell^8 - \ell^7 - 1}{\ell^{10} - 1}.$$

Proof. For each elliptic curve $E/\mathbb{Q}$, number field F and finite Galois extension K/F, define

$$g_p^{(0)}(K/F; E) = \sum_{\substack{v\in\Omega_F \\ v\mid 6p\infty\Delta_K}} \dim E(F_v)/\left(N_{K_w/F_v}E(K_w) + pE(F_v)\right),$$

$$g_p^{(1)}(K/F; E) = \sum_{\substack{\mathfrak{p}\in\Omega_F \\ \mathfrak{p}\nmid 6p\infty\Delta_K \\ \mathfrak{p}\mid N(E/F)}} \dim E(F_\mathfrak{p})/\left(N_{K_\mathfrak{P}/F_\mathfrak{p}}E(K_\mathfrak{P}) + pE(F_\mathfrak{p})\right),$$

where in each summand, w (resp. $\mathfrak{P}$) is a place of K above v (resp. $\mathfrak{p}$), and $N(E/F)$ is the conductor of E/F. By [Maz72, Corollary 4.4], the norm map is surjective at primes of good reduction which are unramified in K/F, so the norm indices at such primes are trivial. Thus

$$g_p(K/F;E) = g_p^{(0)}(K/F;E) + g_p^{(1)}(K/F;E),$$

so we bound the average of $g_p^{(i)}(K/F;E)$ for $i \in \{0,1\}$.

If $i = 0$ then by Lemma 5.3.3 we have that if $p > 2$ then

$$\sum_{(A,B)\in\mathcal{E}(X)} g_p^{(0)}(K/F;E_{A,B}) \leq (2\#\left\{\mathfrak{p}\in\Omega_F : \mathfrak{p} \mid 6p\Delta_K\right\} + [F:\mathbb{Q}] + \delta_2(p)r_1(F))\,\#\mathcal{E}(X).$$

We now deal with the case that $i = 1$. By Propositions 3.1.2, 3.1.3 and 3.1.4, the norm index at primes of reduction type I_1 is trivial. Thus, for each elliptic curve $E/\mathbb{Q}$, the sum $g_p^{(1)}(K/F;E)$ is the sum of norm indices at unramified primes of bad reduction of type different from I_1 over F. By [CJ20, Theorem 1.4], for each prime number $\ell \in [5, X^{1/6}]$ one has

$$\#\left\{(A,B)\in\mathcal{E}(X) \ : \ \substack{E_{A,B}/\mathbb{Q}_\ell \text{ has bad reduction}\\ \text{of type different from } I_1}\right\} = \frac{4X^{5/6}}{\zeta(10)}\frac{2\ell^8-\ell^7-1}{\ell^{10}-1} + O\left(\ell X^{1/2}\right). \quad (5.3)$$

Since we are looking at unramified local extensions $F_\mathfrak{p}/\mathbb{Q}_\ell$, curves with bad reduction of type different from I_1 over $F_\mathfrak{p}$ must satisfy the same condition over $\mathbb{Q}_\ell$. We then have

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}(X)} g_p^{(1)}(K/F;E_{A,B})\\
&\leq 2\sum_{\substack{5\leq\ell\leq 31X\\ \text{prime}\\ \ell\nmid p\Delta_K}}\ \sum_{\substack{\mathfrak{p}\in\Omega_F\\ \mathfrak{p}\mid\ell}} \#\left\{(A,B)\in\mathcal{E}(X) \ : \ \substack{E_{A,B} \text{ has bad reduction}\\ \text{of type different from } I_1 \text{ at } \ell}\right\}\\
&\leq 2\sum_{\substack{5\leq\ell\leq\log(X)\\ \text{prime}\\ \ell\nmid p\Delta_K}}\ \sum_{\substack{\mathfrak{p}\in\Omega_F\\ \mathfrak{p}\mid\ell}} \left(\frac{4X^{5/6}}{\zeta(10)}\frac{2\ell^8-\ell^7-1}{\ell^{10}-1} + O\left(\ell X^{1/2}\right)\right) + O\left(\frac{X^{5/6}[F:\mathbb{Q}]}{\log(X)}\right)\\
&\leq \frac{8X^{5/6}}{\zeta(10)}\sum_{\substack{\ell \text{ prime}\\ \ell\nmid 6p\Delta_K}} \#\left\{\mathfrak{p}\in\Omega_F \ : \ \mathfrak{p}\mid\ell,\ \mathfrak{p}\nmid\Delta_K\right\}\frac{2\ell^8-\ell^7-1}{\ell^{10}-1} + O\left(\frac{X^{5/6}[F:\mathbb{Q}]}{\log(X)}\right),
\end{aligned}$$

where in the first inequality we bound the norm index by Lemma 5.3.3, and in the second we discount large primes using Proposition 5.3.2 and then apply (5.3). The bound then follows from the well known fact that $\#\mathcal{E}(X) \sim \frac{4X^{5/6}}{\zeta(10)}$. □

§ 5.3.3 | Proof of Theorem 1.3.8

We first use the Selmer structures of §2.2 to approximate the dimension of the corresponding fixed space. To begin, almost no elliptic curves defined over $\mathbb{Q}$ have nontrivial n-torsion over a fixed number field K. The proof of this is obtained verbatim from the

argument of Duke [Duk97, Lemma 5] in the case $K = \mathbb{Q}$, applying the relevant sieve conditions only at totally split primes as performed by Zywina [Zyw10, Proposition 5.7].

Lemma 5.3.6. *Let n be a positive integer and let $K/\mathbb{Q}$ be a finite extension. Then*

$$\frac{\#\{(A,B) \in \mathcal{E}(X) \ : \ E_{A,B}(K)[n] \text{ is nontrivial}\}}{\#\mathcal{E}(X)} \ll_{n,K} \frac{\log(X)}{X^{1/6}}.$$

Using this result, we can prove the following.

Lemma 5.3.7. *Let p be a prime number, F be a number field and K/F be a finite Galois extension. We have that*

$$\frac{\sum\limits_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])\right|}{\#\mathcal{E}(X)} \ll_{K,p} \frac{\log(X)}{X^{1/6}},$$

where $G = \mathrm{Gal}(K/F)$ is the Galois group.

Proof. Let $D_p(G)$ be a positive integer such that, for every $\mathbb{F}_p[G]$-module M of dimension at most 2 and every $i \in \{1, 2\}$, we have

$$\dim H^i(G, M) \leq D_p(G).$$

Since there are only finitely many such M, $D_p(G)$ certainly exists. By Lemma 2.2.7, for every elliptic curve $E/\mathbb{Q}$ we have

$$\left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E[p])\right| \leq \begin{cases} 0 & \text{if } E(K)[p] \text{ is trivial,} \\ D_p(G) & \text{else.} \end{cases}$$

The result then follows from Lemma 5.3.6. □

We now combine this with Proposition 5.3.5 to prove Theorem 1.3.8, namely that the average failure of Galois descent is bounded.

Theorem 5.3.8. *Let p be a prime number, F be a number field and K/F be a finite Galois extension. Writing $G = \mathrm{Gal}(K/F)$, we have that*

$$\limsup_{X\to\infty} \frac{\sum\limits_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)} \leq C_p(K/F),$$

where $C_p(K/F)$ is the constant in §1.3.2.

Proof. By Lemma 5.3.7, we immediately have

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_p(E_{A,B}/K)^G - \dim \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)}$$
$$\leq \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \left|\dim \mathrm{Sel}_{\mathscr{F}(K)}(F, E_{A,B}[p]) - \dim \mathrm{Sel}_p(E_{A,B}/F)\right|}{\#\mathcal{E}(X)}.$$

Since by Lemma 2.2.11 this average is bounded by that of the genus theory invariant, the result follows from Proposition 5.3.5. □

From this we derive an immediate consequence.

Corollary 5.3.9. *Let $p \in \{2,3,5\}$ and let $K/\mathbb{Q}$ be a finite Galois extension. Then, writing $G = \mathrm{Gal}(K/\mathbb{Q})$, we have*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/K)^G}{\#\mathcal{E}(X)} \leq C_p(K/\mathbb{Q}) + \left(\frac{27}{4}\right)^{5/6} \frac{p+1}{p},$$

where $C_p(K/\mathbb{Q})$ is as in §1.3.2. Assuming Hypothesis 1 the same is true if p is any prime number.

Proof. This follows from Theorem 5.3.8 and Proposition 5.2.10 □

Example 5.3.10. *Consider the splitting field $K/\mathbb{Q}$ of $x^3 - 2$, which is a degree 6 extension with Galois group $G \cong S_3$.*

If $p = 2$, it follows from Corollary 5.3.9 that the average dimension of $\mathrm{Sel}_2(E/K)^G$ is at most $C_2(K/\mathbb{Q}) + \left(\frac{27}{4}\right)^{5/6} \frac{3}{2}$. The primes dividing $6p\Delta_K$ are 2 and 3, so that

$$C_2(K/\mathbb{Q}) = 6 + 2 \sum_{\substack{\ell\neq 2,3 \\ \text{prime}}} \frac{2\ell^8 - \ell^7 - 1}{\ell^{10} - 1} \approx 6.339.$$

Thus, the average of $\dim \mathrm{Sel}_2(E/K)^G$ is less than 13.71.

Similarly, if $p = 3$, the average of $\dim \mathrm{Sel}_3(E/K)^G$ is less than 12.89.

For every prime number p different from 2 and 3, and every elliptic curve $E/\mathbb{Q}$, we have that $\mathrm{Sel}_p(E/K)^G \cong \mathrm{Sel}_p(E/\mathbb{Q})$ by Proposition 5.2.7 (one can also note this by the vanishing of the finite group cohomology in the inflation restriction sequence). Moreover, for $p = 5$ the average of the dimension of this fixed space is at most 6/5 by [BS13].

§ 5.4 | Boundedness of Selmer Ranks

In this section we use the modular representation theory of p–groups to leverage the result of Theorem 5.3.8 to obtain a bound for the average dimension of the entire p–Selmer group, not just that of the fixed space. Combining this with estimates for p–Selmer groups over multiquadratic extensions from Proposition 5.2.14 we then prove

explicit upper bounds for average p–Selmer ranks over Galois p–extensions of $\mathbb{Q}$ and of multiquadratic number fields.

§ 5.4.1 | General p-Selmer Ranks for p-Extensions

Using the results so far we can, when the Galois group is a p-group, bound the entire p-Selmer group using only the fixed space.

Theorem 5.4.1. *Let p be a prime number, F be a number field and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/K)}{\#\mathcal{E}(X)} \leq [K:F]\left(C_p(K/F) + \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/F)}{\#\mathcal{E}(X)}\right),$$

where $C_p(K/F)$ is as in §1.3.2.

Proof. By Lemma 2.2.13 we know that

$$\dim \mathrm{Sel}_p(E/K) \leq [K:F] \dim \mathrm{Sel}_p(E/K)^{\mathrm{Gal}(K/F)},$$

so the result follows from Theorem 5.3.8. □

We can then combine the bound in Theorem 5.4.1 with the bound already established in Proposition 5.2.14 to obtain the full statement of Theorem 1.3.9 and so Theorem 1.3.5 via the inclusion $E(K)/pE(K) \subseteq \mathrm{Sel}_p(E/K)$.

Corollary 5.4.2. *Let $p \in \{2,3,5\}$, F be either $\mathbb{Q}$ or a multiquadratic number field, and K/F be a Galois p–extension. Then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/K)}{\#\mathcal{E}(X)} \leq \begin{cases} [K:F]C_2(K/F) + [K:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3^{7/2}}{2^{8/3}}\right) & \text{if } p=2 \text{ and } F\neq\mathbb{Q}, \\ [K:F]\left(C_p(K/F) + \left(\frac{27}{4}\right)^{5/6}\frac{p+1}{p}[F:\mathbb{Q}]\right) & \text{else,} \end{cases}$$

where $C_p(K/F)$ is the explicit constant in §1.3.2. Moreover, assuming Hypothesis 1 the same is true if p is any prime number.

Proof. If p is odd, then this is immediate from Theorem 5.4.1 and Proposition 5.2.14. If both $p=2$ and $F=\mathbb{Q}$ then it is immediate from Theorem 5.4.1 and Proposition 5.2.10. If $p=2$ and F is a multiquadratic extension, then we apply Theorem 5.4.1 twice: first to the extension K/F, then to $F/\mathbb{Q}$, since both are Galois 2–extensions. The result in this case then follows from Proposition 5.2.10. □

§ 5.5 | Mordell–Weil Lattices over Galois Extensions

§ 5.5.1 | Mordell–Weil Lattices

Our main object of study here will be the Mordell–Weil lattice, which is the "free part" of the Mordell-Weil group.

Definition 5.5.1. For a number field K and an elliptic curve E/K, the Mordell–Weil lattice is the quotient

$$\Lambda(E/K) := E(K)/E(K)_{\text{tors}}.$$

When K/F is a Galois extension of number fields and E is defined over F, this is evidently a finitely generated $\mathbb{Z}$-free $\mathbb{Z}[\mathrm{Gal}(K/F)]$-module. We refer to such modules as $\mathbb{Z}[\mathrm{Gal}(K/F)]$-lattices. We begin by giving a precise notion of "multiplicity" for indecomposable lattices in Mordell–Weil lattices.

Definition 5.5.2. Let p be a prime number, K/F be a finite Galois extension of number fields and E/F be an elliptic curve. For each finitely generated $\mathbb{Z}$-free $\mathbb{Z}[\mathrm{Gal}(K/F)]$-module Λ, define the multiplicity of Λ in $E(K)$ to be

$$e_\Lambda(K/F;E) := \max\left\{e \in \mathbb{Z}_{\geq 0} \ : \ \begin{smallmatrix}\Lambda^{\oplus e} \text{ is isomorphic to a direct summand} \\ \text{of } \Lambda(E/K) \text{ as } \mathbb{Z}[\mathrm{Gal}(K/F)]\text{-lattices}\end{smallmatrix}\right\}.$$

Example 5.5.3. *Let $K/\mathbb{Q}$ be the splitting field of the polynomial x^3-3x-1. Note that $K/\mathbb{Q}$ is Galois and has degree 3, and write $G = \mathrm{Gal}(K/\mathbb{Q})$. There are two irreducible $\mathbb{Q}[G]$-modules: the line $\mathbb{Q}$, with trivial G-action, and the third cyclotomic field $\mathbb{Q}(\zeta_3)$, where a generator of G acts by multiplication by ζ_3. Moreover, Maschke's theorem tells us that finite dimensional $\mathbb{Q}[G]$-modules are semisimple, so are isomorphic to direct sums of these irreducible modules.*

Let $E/\mathbb{Q}$ be the elliptic curve described by the Weierstrass equation

$$E : y^2 + xy = x^3 - x^2 - 42x - 19.$$

The computer algebra program `MAGMA` [BCP97] *can compute that $E(K)$ is torsion–free of rank 2 and $E(\mathbb{Q})$ is trivial. Since there are no points fixed by the Galois action, $e_{\mathbb{Z}} = 0$ where $\mathbb{Z}$ is the set of integers acted on trivially by G. Moreover, $E(K)\otimes\mathbb{Q} \cong \mathbb{Q}(\zeta_3)$, so the Mordell–Weil group is isomorphic to a $\mathbb{Z}[\zeta_3]$-stable lattice inside of $\mathbb{Q}(\zeta_3)$. Such lattices are precisely the fractional ideals, and since scaling such a lattice gives an isomorphic module and the class group of $\mathbb{Q}(\zeta_3)$ is trivial, $\Lambda(E/K) = E(K)$ is isomorphic to $\mathbb{Z}[\zeta_3]$ as $\mathbb{Z}[G]$-lattices. In particular, $e_{\mathbb{Z}[\zeta_3]}(E/K) = 1$.*

We shall give upper bounds for the averages of some of these exponents by considering the lattice modulo p, and then estimating the various exponents in terms of the fixed space in the p-Selmer group.

Lemma 5.5.4. *Let p be a prime number, K/F be a finite Galois extension of number fields, and E/F be an elliptic curve. Writing $G = \mathrm{Gal}(K/F)$, we have that*

$$\dim(\Lambda(E/K)/p\Lambda(E/K))^G \leq \dim \mathrm{Sel}_p(E/K)^G + \dim H^1\left(G, E(K)[p^\infty]/pE(K)[p^\infty]\right).$$

Proof. There is a short exact sequence of $\mathbb{F}_p[G]$-modules

$$0 \longrightarrow E(K)[p^\infty]/pE(K)[p^\infty] \longrightarrow E(K)/pE(K) \longrightarrow \Lambda(E/K)/p\Lambda(E/K) \longrightarrow 0,$$

so that, taking cohomology over G, we obtain

$$\dim\left(\frac{\Lambda(E/K)}{p\Lambda(E/K)}\right)^G \leq \dim\left(\frac{E(K)}{pE(K)}\right)^G + \dim H^1(G, E(K)[p^\infty]/pE(K)[p^\infty]).$$

Moreover, the short exact sequence induced by multiplication by p gives an inclusion of $\mathbb{F}_p[G]$-modules

$$\delta : E(K)/pE(K) \hookrightarrow \mathrm{Sel}_p(E/K),$$

completing the result. □

Proposition 5.5.5. *Let p be a prime number, K/F be a finite Galois extension of number fields, and E/F be an elliptic curve. Writing $G = \mathrm{Gal}(K/F)$, then for every $\mathbb{Z}[G]$-lattice Λ such that $\dim(\Lambda/p\Lambda)^G \geq 1$, we have that*

$$e_\Lambda(K/F; E) \leq \frac{1}{\dim(\Lambda/p\Lambda)^G}\left(\dim \mathrm{Sel}_p(E/K)^G + \dim H^1(G, E(K)[p^\infty]/pE(K)[p^\infty]\right).$$

Proof. If $\Lambda^{\oplus e}$ is a direct summand of $\Lambda(E/K)$, then

$$\left((\Lambda/p\Lambda)^G\right)^{\oplus e} \subseteq \left(\Lambda(E/K)/p\Lambda(E/K)\right)^G,$$

so that, since $\dim \Lambda/p\Lambda^G \geq 1$, we have

$$e_\Lambda(K/F; E) \leq \frac{\dim(\Lambda(E/K)/p\Lambda(E/K))^G}{\dim(\Lambda/p\Lambda)^G}. \tag{5.4}$$

Thus the result follows from Lemma 5.5.4. □

§ 5.5.2 | Average Multiplicities

We now use Theorem 5.3.8 to obtain the average multiplicity of certain lattices in Mordell–Weil lattices of elliptic curves.

Theorem 5.5.6. *Let K/F be a finite Galois extension of number fields, write $G = \mathrm{Gal}(K/F)$ and let p be a prime number. Assume that Λ is a $\mathbb{Z}[G]$-lattice satisfying*

$\dim(\Lambda/p\Lambda)^G \geq 1$, *then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} e_\Lambda(K/F; E_{A,B})}{\#\mathcal{E}(X)} \leq \frac{1}{\dim(\Lambda/p\Lambda)^G}\left(C_p(K/F) + \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_p(E_{A,B}/F)}{\#\mathcal{E}(X)}\right),$$

where $C_p(K/F)$ *is as in §1.3.2.*

Proof. Let $D_p(G)$ be an integer such that for every elliptic curve $E/\mathbb{Q}$ we have that

$$\dim H^1\left(G, E(K)[p^\infty]/pE(K)[p^\infty]\right) \leq D_p(G).$$

Note that this exists, since there are only finitely many $\mathbb{F}_p[G]$-modules of dimension at most 2. Now, by Lemma 5.3.6

$$\frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim H^1\left(G, E(K)[p^\infty]/pE(K)[p^\infty]\right)}{\#\mathcal{E}(X)} \ll_{K,p} D_p(G)\frac{\log(X)}{X^{1/6}},$$

and the result follows from Proposition 5.5.5 and Theorem 5.3.8. □

Remark 5.5.7. The requirement that $(\Lambda/p\Lambda)^G$ is non-trivial for some prime number p is rather easy to check. If $\Lambda^G \neq 0$ then already this is non-trivial for every prime number, and if $\Lambda^G = 0$ then via the short exact sequence induced by multiplication by p, $(\Lambda/p\Lambda)^G$ is isomorphic to the p-torsion of the finite cohomology group $H^1(G, \Lambda)$. Computing this cohomology group in any given instance is a purely mechanical task.

We then immediately obtain Theorem 1.3.11.

Corollary 5.5.8. *Let* $p \in \{2, 3, 5\}$*,* F *be either* $\mathbb{Q}$ *or a multiquadratic number field, and* K/F *be a finite Galois extension. Write* $G = \mathrm{Gal}(K/F)$*, then for every* $\mathbb{Z}[G]$*-lattice* Λ *such that* $\dim(\Lambda/p\Lambda)^G \geq 1$*,*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} e_\Lambda(K/F; E_{A,B})}{\#\mathcal{E}(X)} \leq \frac{1}{\dim(\Lambda/p\Lambda)^G} \cdot \begin{cases} C_2(K/F) + [F:\mathbb{Q}]\left(C_2(F/\mathbb{Q}) + \frac{3^{7/2}}{2^{8/3}}\right) & \text{if } p = 2 \text{ and } F \neq \mathbb{Q}, \\ C_p(K/F) + \left(\frac{27}{4}\right)^{5/6} \frac{p+1}{p}[F:\mathbb{Q}] & \text{else,} \end{cases}$$

where $C_p(K/F)$ *is the explicit constant in §1.3.2. Moreover, under Hypothesis 1 the same is true if* p *is any prime number.*

Proof. Applying Theorem 5.5.6, it is sufficient to replace the nominator in the left hand side with $\dim \mathrm{Sel}_p(E_{A,B}/F)$ and bound the average appropriately in each case.

If $p \in \{3, 5\}$, then this follows from Proposition 5.2.14; if $p = 2$ and $F = \mathbb{Q}$ then it follows from Proposition 5.2.10; and finally, if $p = 2$ and F is a multiquadratic number field then it follows from Corollary 5.4.2. □

§ 5.5.3 | An Example: Semidirect Products

We conclude by providing a family of examples of lattices which satisfy the hypotheses of Theorem 5.5.6 and generalise Example 1.3.13 from the introduction. Let $K/\mathbb{Q}$ be a finite Galois extension such that $G = \mathrm{Gal}(K/\mathbb{Q})$ is an inner semidirect product $N \rtimes H$. Consider the augmentation ideal $\Lambda \subseteq \mathbb{Z}[N]$, which is defined by the short exact sequence of $\mathbb{Z}[N]$–modules:

$$0 \longrightarrow \Lambda \longrightarrow \mathbb{Z}[N] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0, \tag{5.5}$$

where the augmentation map ε is given explicitly by $\sum_{n\in N} a_n \cdot n \mapsto \sum_{n\in N} a_n$.

Identifying each $n \in N$ with the coset $nH \in G/H$ provides an isomorphism of $\mathbb{Z}[N]$–modules $\mathbb{Z}[N] \cong \mathbb{Z}[G/H]$. This identification allows us to induce a G–action on $\Lambda \subseteq \mathbb{Z}[G/H]$, and to upgrade (5.5) to a short exact sequence of $\mathbb{Z}[G]$–modules. Taking cohomology over N we obtain an exact sequence of $\mathbb{Z}[G/N]$–modules

$$0 \longrightarrow \Lambda^N \longrightarrow \mathbb{Z}[G/H]^N \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow H^1(N,\Lambda) \longrightarrow 0. \tag{5.6}$$

In particular, as $\mathbb{Z}[G/H]^N = \mathbb{Z} \cdot (\sum_{n\in N} nH)$ so that ε is injective on the fixed points, we have that $\Lambda^N = 0$. By Remark 5.5.7, since $\Lambda^G \subseteq \Lambda^N = 0$, we have that for every prime number p

$$(\Lambda/p\Lambda)^G \cong H^1(G,\Lambda)[p].$$

It follows from the inflation restriction short exact sequence that $H^1(G,\Lambda) \cong H^1(N,\Lambda)^{G/N}$. Again considering (5.6), we have that $H^1(N,\Lambda) \cong \mathbb{Z}/\#N\mathbb{Z}$ with trivial G/N–action. In particular, for all primes $p \mid \#N$ we have that

$$(\Lambda/p\Lambda)^G \cong \mathbb{Z}/p\mathbb{Z}.$$

Thus, if $\#N$ is divisible by $2, 3$ or 5 then by Corollary 5.5.8 we have that the average of $e_\Lambda(K/\mathbb{Q}; E)$ is bounded as $E/\mathbb{Q}$ runs through elliptic curves ordered by height. Moreover, assuming Hypothesis 1 the same is true for any nontrivial N.

Chapter 6

2-Selmer Groups & Multiquadratic Extensions

In this chapter we will study the average of the genus theory in 2-Selmer groups of elliptic curves in the family of all elliptic curves over multiquadratic extensions $K/\mathbb{Q}$. Combining this with methods of Bhargava and Shankar [BS15a], which allow us to control the average size of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_{A,B}[2])$ in Chapter 7, we are able to prove the results stated in §1.4.

In order to make the chapter more concise, we introduce some notation for its duration.

Notation 6.0.1. For each $v \in \Omega_{\mathbb{Q}}$, each multiquadratic extension $K/\mathbb{Q}$ and each elliptic curve $E/\mathbb{Q}_v$, the local norm index modulo 2 at v of E is denoted

$$\iota_v(K/\mathbb{Q}; E) := \dim_{\mathbb{F}_2} \frac{E(\mathbb{Q}_v)}{N_{K_w/\mathbb{Q}_v} E(K_w) + 2E(\mathbb{Q}_v)}.$$

In particular recall that, by Definition 2.2.8, the genus theory part of the 2-Selmer group of an elliptic curve $E/\mathbb{Q}$ over such K is then given by $g_2(K/\mathbb{Q}; E) := \sum_{v \in \Omega_{\mathbb{Q}}} \iota_v(K/\mathbb{Q}; E)$.

In §6.1 we provide a general counting machine to compute averages for a class of functions on $\mathcal{E}$ which are sums of local invariants, including $g_2(K/\mathbb{Q}; \cdot)$. In §6.2 we then apply this machine to obtain the contribution to the average of the genus theory from primes of additive reduction. We then have to make slight adaptations in the case of multiplicative reduction, and we compute their contribution in §6.3. We compute the average of the final part of the genus theory, the contribution from the archimedean place, in §6.4. Finally in §6.5 we pull forward a result from Chapter 7 to control the corestriction Selmer group, and then use this and our earlier results to prove those stated in §1.4.

§ 6.1 | Averaging Local Constants: General Counting Machine

In this section we prove some counting results for a large class of functions, which will be shown to contain the genus theory invariant, with the expectation that this generality will have utility in future. In particular, it can be expected that these results may describe the statistical behaviour of general Tamagawa ratios for elliptic curves parametrised by $\mathcal{E}$. To maximise on the utility of these results, we will count with respect to "height–like" orderings on $\mathcal{E}$.

Definition 6.1.1. For each pair $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$, and every positive real number X we define a finite set

$$\mathcal{E}^{\mathbf{C}}(X) := \left\{(A,B) \in \mathcal{E} \ : \ |A| \leq C_1 X^{1/3} \text{ and } |B| \leq C_2 X^{1/2}\right\}.$$

Example 6.1.2. *For* $\mathbf{C} = (1/\sqrt[3]{4}, 1/\sqrt{27})$, $\mathcal{E}^{\mathbf{C}}(X) = \mathcal{E}'(X)$ *the set of elliptic curves of naive height at most* X*.*

§ 6.1.1 | Technical Lemmata

Here we provide some elementary proofs of useful results for certain arithmetic functions relating to the set $\mathcal{E}$.

Definition 6.1.3. For every p which is either a prime number or 1, we define functions $f_p, g_p : \mathbb{Z}\setminus\{0\} \to \mathbb{R}$ by, for each $B \in \mathbb{Z}\setminus\{0\}$, setting

$$f_p(B) := \prod_{\substack{\ell \text{ prime} \\ \ell^6 | B \\ \ell \neq p}} (1 - \ell^{-4}), \qquad g_p(B) := \prod_{\substack{\ell \text{ prime} \\ \ell^6 | B \\ \ell \neq p}} \ell^4.$$

Remark 6.1.4. Both of these functions are clearly multiplicative, that is, for coprime m, n we must have that $f_p(mn) = f_p(m)f_p(n)$ and similarly for g_p.

Sums of these functions can be estimated using Dirichlet convolution, even with congruence conditions. We deal with f_p first.

Lemma 6.1.5. *Let* p *be either a prime number or* 1*. For each residue class* $b \in \mathbb{Z}/p^n\mathbb{Z}$ *for some* $n > 0$ *and real number* $Y \geq 1$ *we have*

$$\sum_{\substack{1 \leq |B| \leq Y \\ B \equiv b \mod p^n}} f_p(x) = \begin{cases} 2Y\zeta(10)^{-1} + O(1) & \text{if } p = 1 \\ \frac{2Y}{p^n}\frac{\zeta(10)^{-1}}{1-p^{-10}} + O(1) & \text{otherwise} \end{cases}$$

where the implied constant is 17/6*.*

Proof. Let $\tilde{f}_p := \mu * f_p$ be the Dirichlet convolution of f_p with the Möbius function. Then we note some properties of this new function. Firstly, since f_p and μ are multi-

plicative so is $\tilde{f}_p$. Secondly, for every prime number ℓ and integer $r > 0$ we have

$$\tilde{f}_p(\ell^r) = f_p(\ell^r) - f_p(\ell^{r-1}) = \begin{cases} -\ell^{-4} & \text{if } \ell \neq p \text{ and } r = 6 \\ 0 & \text{else.} \end{cases}$$

From these properties we note that the Euler product for the L-function of $\tilde{f}_p$ is $L(\tilde{f}_p, s) = \prod_{\ell \neq p}(1 - \ell^{-4-6s})$, so that in particular

$$L(\tilde{f}_p, 1) = \begin{cases} \zeta(10)^{-1} & \text{if } p = 1 \\ \frac{\zeta(10)^{-1}}{1-p^{-10}} & \text{if } p \text{ is prime.} \end{cases} \tag{6.1}$$

Moreover the multiplicativity shows that for each integer m we have

$$\left|\tilde{f}_p(m)\right| = \begin{cases} d^{-4} & \text{if } m = \pm d^6 \text{ for some squarefree integer } d \text{ coprime to } p \\ 0 & \text{else.} \end{cases} \tag{6.2}$$

Now, addressing the problem at hand, we have

$$\begin{aligned} \sum_{\substack{1 \leq |B| \leq Y \\ B \equiv b \mod p^n}} f_p(B) &= \sum_{\substack{1 \leq |B| \leq Y \\ B \equiv b \mod p^n}} \sum_{m | B} \tilde{f}_p(m) \\ &= \sum_{\substack{1 \leq m \leq Y \\ (m,p)=1}} \tilde{f}_p(m) \sum_{\substack{1 \leq |B'| \leq Y/m \\ mB' \equiv b \mod p^n}} 1 \\ &= \frac{2Y}{p^n} \sum_{\substack{1 \leq m \leq Y \\ (m,p)=1}} \frac{\tilde{f}_p(m)}{m} + O\left(\sum_{\substack{1 \leq m \leq Y \\ (m,p)=1}} \left|\tilde{f}_p(m)\right| \right), \end{aligned}$$

where the implied constant here is 2. Using (6.2) and an integral estimate we see that term inside the error bracket is at most $(4 - Y^{-1/2})/3 \leq 4/3$. For the main term, note that we have

$$\sum_{\substack{1 \leq m \leq Y \\ (m,p)=1}} \frac{\tilde{f}_p(m)}{m} = L(\tilde{f}_p, 1) - \sum_{m > Y} \frac{\tilde{f}_p(m)}{m},$$

and again using (6.2) and an integral estimate we see that the rightmost sum has absolute value at most $Y^{-3/2}/9 \leq 1/9$, completing the proof. □

Now, for g_p we will settle for an easier estimate since it will appear as an error term for us.

Lemma 6.1.6. *Let p be either a prime number or 1. For every real number $Y \geq 1$,*

$$\sum_{|B| \leq Y} g_p(B) \leq \frac{62 + 10\zeta(2)}{5} Y < 16Y.$$

Proof. Again, we take the Dirichlet convolution $\tilde{g}_p := \mu * g_p$, and compute that for

every prime number ℓ and integer $r > 0$ we have

$$\tilde{g}_p(\ell^r) = \begin{cases} \ell^4 - 1 & \text{if } \ell \neq p \text{ and } r = 6 \\ 0 & \text{else.} \end{cases}$$

In particular, using the multiplicativity of $\tilde{g}_p$ we have for each integer m,

$$\tilde{g}_p(m) = \begin{cases} \prod_{\ell \mid d}(\ell^4 - 1) & \text{if } m = d^6 \text{ for some squarefree integer } d \text{ coprime to } p \\ 0 & \text{else.} \end{cases} \tag{6.3}$$

Then we have, as in the proof of Lemma 6.1.5,

$$\sum_{|B| \leq Y} g_p(B) = 2Y \sum_{1 \leq m \leq Y} \frac{\tilde{g}_p(m)}{m} + O\left(\sum_{1 \leq m \leq Y} \tilde{g}_p(m) \right)$$

where the implied constant is 2. Now, by (6.3)

$$\sum_{1 \leq m \leq Y} \frac{\tilde{g}_p(m)}{m} \leq \sum_{1 \leq d \leq Y^{1/6}} \frac{1}{d^2} \leq \zeta(2),$$

and similarly

$$\sum_{1 \leq m \leq Y} \tilde{g}_p(m) \leq \sum_{1 \leq d \leq Y^{1/6}} d^4 \leq \frac{(Y+1)^{5/6} - 1}{5} \leq \frac{31 Y^{5/6}}{5}.$$

□

§ 6.1.2 | Local Functions

We wish to study behaviour of elliptic curves defined by congruence conditions modulo prime powers. We begin by giving the probability that an elliptic curve satisfies a given congruence condition. These probabilities are known (they can be obtained from the Ekedahl sieve as it is presented in [CS20] or by methods similar to [CJ20]), but we will require explicit estimates of the error.

Notation 6.1.7. For each prime number ℓ, we take our Haar measure μ_ℓ on $\mathbb{Z}_\ell^2$ to be the one which is normalised to have total measure 1. For each integrable function

$$\psi : \mathbb{Z}_\ell^2 \to \mathbb{R},$$

we write $\mathbb{E}_\ell[\psi] := \int_{\mathbb{Z}_\ell} \psi \, \mathrm{d}\mu_\ell$ for the expectation. We say that such a function has *finite level* if there exists a pair of integers $\mathbf{M} = (M_1, M_2) \in \mathbb{Z}_{\geq 0}$ (referred to as a level) such that ψ is constant on each set of the form

$$\left\{ (a,b) \in \mathbb{Z}_\ell^2 \ : \ \begin{smallmatrix} a \equiv N_1 & \bmod \ell^{M_1}, \\ b \equiv N_2 & \bmod \ell^{M_2}, \end{smallmatrix} \right\}$$

and we refer to the pair of smallest such M_1, M_2 as the *minimal level* of ψ, and denote it by $\mathbf{M}_\psi$.

We write $\mathcal{E}_\ell \subseteq \mathbb{Z}_\ell$ for the open set

$$\mathcal{E}_\ell = \mathbb{Z}_\ell^2 \Big\backslash \Big\{ (a,b) \in \mathbb{Z}_\ell^2 \ : \ \substack{a \equiv 0 \mod \ell^4 \\ b \equiv 0 \mod \ell^6} \Big\}.$$

We define the function $\Delta(A,B) := 4A^3 + 27B^2$.

Lemma 6.1.8. *Let ℓ be a prime number, and $\psi : \mathcal{E}_\ell \to \mathbb{R}$ be an integrable function of finite level with $\mathbf{M} = \mathbf{M}_\psi = (M_1, M_2)$. Then for every pair $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$ and every real number $X \geq \max\left\{C_2^{-2}, 1\right\}$ we have*

$$\begin{aligned}\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \psi(A,B) =& \frac{4C_1C_2X^{5/6}}{\zeta(10)} \frac{\ell^{10}}{(\ell^{10}-1)} \mathbb{E}_\ell[\psi] \\ &+ O\left(\ell^{M_1+M_2}\mathbb{E}_\ell[|\psi|]\left(C_2X^{1/2} + C_1X^{1/3}\right)\right),\end{aligned}$$

with implied constant equal to 22.

Proof. For each $(a,b) \in \mathbb{Z}/\ell^{\mathbf{M}}\mathbb{Z}$ we define a function

$$\begin{aligned}\psi_{(a,b)} : \mathbb{Z}_\ell^2 &\to \mathbb{R} \\ (A,B) &\mapsto \begin{cases} \psi(A,B) & \text{if } (A,B) \equiv (a,b) \mod \ell^{\mathbf{M}} \\ 0 & \text{else,} \end{cases}\end{aligned}$$

so that

$$\psi = \sum_{(a,b)\in\mathbb{Z}/\ell^{\mathbf{M}}\mathbb{Z}} \psi_{(a,b)}.$$

Proving the claimed statement is therefore reduced to the case that $\psi = \psi_{(a,b)}$ for some pair $(a,b) \in \mathbb{Z}/\ell^{\mathbf{M}}\mathbb{Z}$. Making this reduction we further assume that $\psi \neq 0$ (as else the statement is trivial), and write A_ψ for the nonzero real number in the image of ψ.

Ignoring the discriminant nonzero condition on $(A,B) \in \mathcal{E}^{\mathbf{C}}(X)$ adds at most $2(2C_1X^{1/3}+1)$ extra curves, so

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \psi(A,B) = \left(\sum_{\substack{|B|\leq C_2X^{1/2} \\ B\equiv b \mod p^{M_2}}} \sum_{\substack{|A|\leq C_1X^{1/3} \\ A\equiv a \mod p^{M_1} \\ \forall \ell^6 | B \ \ell^4 \nmid A}} A_\psi \right) + O\left(|A_\psi|\left(2C_1X^{1/3}+1\right)\right)$$

with implied constant 2. We then move the case $B = 0$ into the error term, so that

$$\begin{aligned}\sum_{\substack{|B|\leq C_2X^{1/2} \\ B\equiv b \mod p^{M_2}}} \sum_{\substack{|A|\leq C_1X^{1/3} \\ A\equiv a \mod p^{M_1} \\ \forall \ell^6 | B \ \ell^4 \nmid A}} A_\psi =& \left(\sum_{\substack{1\leq|B|\leq C_2X^{1/2} \\ B\equiv b \mod p^{M_2}}} \sum_{\substack{|A|\leq C_1X^{1/3} \\ A\equiv a \mod p^{M_1} \\ \forall \ell^6 | B \ \ell^4 \nmid A}} A_\psi \right) \\ &+ O\left(|A_\psi|\left(2C_1X^{1/3}+1\right)\right)\end{aligned}$$

with the implied constant being 1. Now, dealing with the main term here,

$$\begin{aligned}
&\sum_{\substack{1\le|B|\le C_2X^{1/2}\\ B\equiv b \mod p^{M_2}}} \sum_{\substack{|A|\le C_1X^{1/3}\\ A\equiv a \mod p^{M_1}\\ \forall \ell^6\mid B\ \ell^4\nmid A}} A_\psi \\
&= A_\psi \sum_{\substack{1\le|B|\le C_2X^{1/2}\\ B\equiv b \mod p^{M_2}}} \left(\frac{2C_1X^{1/3}}{p^{M_1}} \prod_{\substack{\ell^6\mid B\\ \ell\neq p\\ \ell \text{ prime}}} (1-\ell^{-4}) + O\left(\prod_{\substack{\ell^6\mid B\\ \ell\neq p\\ \ell \text{ prime}}} \ell^4 \right) \right) \\
&= A_\psi \frac{4C_1C_2X^{5/6}}{\zeta(10)} \frac{p^{10}}{p^{n_1+n_2}(p^{10}-1)} + O\left(|A_\psi|\, C_2X^{1/2}\right) + O\left(|A_\psi|\, C_1X^{1/3}\right).
\end{aligned}$$

Here, the first equality is by elementary estimates and the implied constant can be taken to be 2. The second equality is by Lemmas 6.1.5 and 6.1.6, and so the implied constants are at worst $\frac{17}{6}$ and 16 respectively. Now combining this with the error terms from ignoring the discriminant zero curves and the case $B = 0$ above we obtain

$$\begin{aligned}
\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \psi(A,B) &= \frac{4C_1C_2X^{5/6}}{\zeta(10)} \frac{\ell^{10}}{(\ell^{10}-1)} \mathbb{E}_\ell[\psi] \\
&\qquad + O\left(|A_\psi|\, C_2X^{1/2}\right) + O\left(|A_\psi|\, C_1X^{1/3}\right) + O\left(|A_\psi|\right) \\
&= \frac{4C_1C_2X^{5/6}}{\zeta(10)} \frac{\ell^{10}}{(\ell^{10}-1)} \mathbb{E}_\ell[\psi] \\
&\qquad + O\left(\ell^{M_1+M_2}\mathbb{E}_\ell[|\psi|]\left(C_2X^{1/2}+C_1X^{1/3}\right)\right),
\end{aligned}$$

where the implied constants in the first line are $\frac{17}{6}$, 22 and 3. Then, since $C_2X^{1/2} \ge 1$, the second line holds with implied constant 22. □

§ 6.1.3 | Systems of Local Constants

We will now seek to have local functions at every prime number, and recover their data simultaneously.

Definition 6.1.9. A *local constant* (on $\mathcal{E}$) is a collection $\alpha = (\alpha_\ell)_{\ell \text{ prime}}$ of functions

$$\alpha_\ell : \mathbb{Z}_\ell^2 \to \mathbb{R},$$

supported on $\mathcal{E}_\ell$. We say that a local constant α is *orderly* if it satisfies all of the following:

1) for every prime number ℓ, α_ℓ is an integrable function of finite level;

2) there is a pair $\mathbf{M}_\alpha = (M_1, M_2) \in \mathbb{Z}_{\ge 0}$ such that for every prime number ℓ, the function α_ℓ has level $\mathbf{M}_\alpha$;

3) there is a constant $C_\alpha \in \mathbb{R}$ such that for every prime number ℓ, $\max(|\mathrm{im}(\alpha_\ell)|) \le C_\alpha$;

4) there is a finite set Σ_α of prime numbers such that for primes $\ell \notin \Sigma_\alpha$ if $\ell^2 \nmid \Delta(A,B)$ then $\alpha_\ell(A,B) = 0$.

We will consider $\mathbf{M}_\alpha$, C_α and Σ_α to be part of the data of α.

Lemma 6.1.10. *Let $\alpha = (\alpha_\ell)_\ell$ be an orderly local constant. Then for every pair $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$ and every real number $X > \max\{55^2, \exp(\max(\Sigma_\alpha))\}$ we have*

$$\left| \sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \sum_{\substack{\log(X)\le\ell \\ \text{prime}}} \alpha_\ell(A,B) \right| \le 4C_\alpha(C_2+4)\frac{C_1X^{5/6}+X^{1/2}}{\log(X)-8}.$$

Proof. Since α is orderly, and all of the primes in Σ_α are less than $\log(X)$, we must have that $\alpha_\ell(A,B) = 0$ whenever $\ell^2 \nmid (4A^3+27B^2)$ (i.e. $E_{A,B}/\mathbb{Q}_\ell$ has type I_0 or I_1 reduction). Moreover,

$$\left| \sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \sum_{\substack{\log(X)\le\ell \\ \text{prime}}} \alpha_\ell(A,B) \right| \le C_\alpha \sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \#\left\{ \log(X) \le \ell \ : \ \substack{E_{A,B}/\mathbb{Q}_\ell \text{ not} \\ \text{of type } I_0 \text{ or } I_1} \right\}.$$

We now estimate the sum on the right hand side. By Appendix A, since $\log(X) > 4$ we have that

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \#\left\{ \ell \text{ prime} \ : \ \substack{\ell\ge\log(X) \\ E_{A,B}/\mathbb{Q}_\ell \text{ not} \\ \text{of type } I_0 \text{ or } I_1} \right\} \\
&\le \sum_{\substack{\log(X)\le\ell\le X^{1/2} \\ \text{prime}}} \sum_{|A|\le C_1X^{1/3}} \#\left\{ B\in\mathbb{Z} \ : \ \substack{|B|\le C_2X^{1/2} \\ 4A^3+27B^2\equiv 0 \mod \ell^2} \right\} \\
&\le \sum_{\substack{\log(X)\le\ell\le X^{1/2} \\ \text{prime}}} \left(2C_1X^{1/3}+2\right)\left(\frac{2C_2X^{1/2}}{\ell^2}+4\right)
\end{aligned}$$

We then break this term into two parts by expanding the rightmost term. Firstly, note that a simple integral estimate gives

$$\sum_{\substack{\log(X)\le\ell\le X^{1/2} \\ \text{prime}}} \frac{1}{\ell^2} \le \int_{\log(X)-1}^{X^{1/2}} y^{-2}dy \le \frac{1}{\log(X)-1} \le \frac{1}{\log(X)-8}.$$

Moreover by [Ros41, Theorem 29A], since $X^{1/2} \ge 55$

$$\#\left\{ \ell \text{ prime} \ : \ \log(X) \le \ell \le X^{1/2} \right\} \le \pi(X^{1/2}) \le \frac{2X^{1/2}}{\log(X)-8}.$$

Therefore,

$$\sum_{\substack{\log(X)\le\ell\le X^{1/2}\\ \text{prime}}}\left(2C_1X^{1/3}+2\right)\left(\frac{2C_2X^{1/2}}{\ell^2}+2\right)\le\left(2C_1X^{1/3}+2\right)\frac{(8+2C_2)X^{1/2}}{\log(X)-8}$$
$$=4(C_2+4)\frac{C_1X^{5/6}+X^{1/2}}{\log(X)-8}$$

as required. □

We now state and prove the main counting machine for this chapter.

Theorem 6.1.11. *Let $\alpha=(\alpha_\ell)_\ell$ be an orderly local constant, and write the minimal level as $\mathbf{M}_\alpha=(M_1,M_2)$. Then for every $C=(C_1,C_2)\in\mathbb{R}^2_{>0}$ and every real number $X>\max\left\{55^2,\exp(\max(\Sigma_\alpha)),C_2^{-2}\right\}$*

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)}\sum_{\ell\text{ prime}}\alpha_\ell(A,B)=\frac{4C_1C_2X^{5/6}}{\zeta(10)}\sum_{\substack{\ell\le\log(X)\\ \text{prime}}}\frac{\ell^{10}}{\ell^{10}-1}\mathbb{E}_\ell(\alpha_\ell)$$
$$+O\left(4C_\alpha(C_2+4)\frac{(C_1X^{5/6}+X^{1/2})}{\log(X)-8}+22\left(C_2X^{1/2}+C_1X^{1/3}\right)\sum_{\substack{\ell\le\log(X)\\ \text{prime}}}\ell^{M_1+M_2}\mathbb{E}_\ell[|\alpha_\ell|]\right)$$

where the implied constant is 1, $\mathcal{E}^{\mathbf{C}}(X)$ is as in Definition 6.1.1, and $\mathbb{E}_\ell$ is as in Notation 6.1.7.

Proof. By Lemma 6.1.10,

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)}\sum_{\ell\text{ prime}}\alpha_\ell(A,B)=\left(\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)}\sum_{\substack{\ell\le\log(X)\\ \text{prime}}}\alpha_\ell(A,B)\right)$$
$$+O\left(C_\alpha(C_2+4)\frac{C_1X^{5/6}+X^{1/2}}{\log(X)-8}\right),$$

where the implied constant is 4. The error here gives the first error term in the theorem statement. By Lemma 6.1.8 the main term here can then be unpacked as

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)}\sum_{\substack{\ell\le\log(X)\\ \text{prime}}}\alpha_\ell(A,B)$$
$$=\sum_{\substack{\ell\le\log(X)\\ \text{prime}}}\left(\frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^{10}}{(\ell^{10}-1)}\mathbb{E}_\ell[\alpha_\ell]+O\left(\ell^{M_1+M_2}\mathbb{E}_\ell[|\alpha_\ell|]\left(C_2X^{1/2}+C_1X^{1/3}\right)\right)\right)$$

where the implied constant is 22. □

§ 6.2 | Additive Primes

As an application of our explicit results above on averaging orderly local constants, we now find the average of the additive contribution to the genus theory.

Notation 6.2.1. For each multiquadratic extension $K/\mathbb{Q}$, define the function

$$\mathcal{G}_K^{\mathrm{add}} : \{\ell \in \mathbb{Z}_{\geq 5} \ : \ \ell \text{ prime}\} \to \mathbb{R}$$

to map each element ℓ to

$$\mathcal{G}_K^{\mathrm{add}}(\ell) = \begin{cases} \frac{\ell(\ell-1)(\ell^5+1)(5\ell^3-4\ell^2+3)}{6(\ell^{10}-1)} & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is ramified and quadratic;} \\ \frac{\ell(\ell-1)(3\ell^5+\ell^3-2\ell^2+3)}{3(\ell^{10}-1)} & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is unramified and quadratic;} \\ \frac{\ell(\ell^5+1)(5\ell^4-9\ell^3+4\ell^2+6\ell-6)}{6(\ell^{10}-1)} & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is biquadratic;} \\ 0 & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is trivial.} \end{cases}$$

where $\mathfrak{p} \in \Omega_K$ is a choice of place extending ℓ.

§ 6.2.1 | Local Densities for Additive Primes

It will be important to establish local terms at each prime number ℓ, for which we need the following definition.

Definition 6.2.2. For every pair $\mathbf{N} = (N_1, N_2) \in \mathbb{Z}_{>0}^2$ and prime number ℓ, we write as shorthand

$$\mathbb{Z}/\ell^{\mathbf{N}}\mathbb{Z} := \mathbb{Z}/\ell^{N_1}\mathbb{Z} \times \mathbb{Z}/\ell^{N_2}\mathbb{Z}.$$

For each Kodaira type T, we then write

$$\mathcal{E}_{\ell,T} := \{(A,B) \in \mathcal{E} \ : \ E_{A,B}/\mathbb{Q}_\ell \text{ has Kodaira type } T\},$$

and

$$\mathcal{E}_{\ell,T}^{\mathbf{N}} := (\mathcal{E}_{\ell,T} \mod \ell^{\mathbf{N}}) \subseteq \mathbb{Z}/\ell^{\mathbf{N}}\mathbb{Z}.$$

We simply write $\mathcal{E}_\ell^{\mathbf{N}}$ for the image of the full set $\mathcal{E}$ in $\mathbb{Z}/\ell^{\mathbf{N}}\mathbb{Z}$.

It is, of course, very easy to work out $\#\mathcal{E}_{\ell,T}^{\mathbf{N}}$ just by examining the table in Appendix A. Motivated by the extra conditions required to obtain the values of the norm index, we count special subsets of these.

Lemma 6.2.3. *For each prime number $\ell \geq 5$, and $\alpha \in \mathbb{F}_\ell^\times$ we have*

$$\#\left\{(a,b) \in \mathcal{E}_{\ell,III}^{(4,6)} \ : \ a\ell^{-1} \equiv \alpha \mod \ell\right\} = \ell^6.$$

Remark 6.2.4. There are many elements $a' \in \mathbb{Z}/\ell^4\mathbb{Z}$ such that $a'\ell = a$, however these are all equivalent modulo ℓ and so our set is well defined. Similar considerations will not be discussed in future.

Proof. From Appendix A, the elements $(\overline{A}, \overline{B}) \in \mathcal{E}_{\ell,III}^{(4,6)}$ are precisely the elements of $\mathcal{E}_\ell^{(4,6)}$ of the form

$$(\overline{A}, \overline{B}) = (a\ell, b\ell^2),$$

for some $a \in (\mathbb{Z}/\ell^3\mathbb{Z})^\times$ and $b \in \mathbb{Z}/\ell^4\mathbb{Z}$. Noting that we also require $a \equiv \alpha \mod \ell$, we have ℓ^2 choices for a and ℓ^4 choices for b. □

Lemma 6.2.5. *For each prime number $\ell \geq 5$ and $n \in \{0,1,3\}$,*

$$\#\left\{(a,b) \in \mathcal{E}_{\ell,I_0}^{(1,1)} \ : \ T^3+aT+b \text{ has } n \text{ roots}\right\} = \begin{cases} \frac{(\ell^2-1)}{3} & \text{if } n=0 \\ \frac{\ell(\ell-1)}{2} & \text{if } n=1 \\ \frac{(\ell-1)(\ell-2)}{6} & \text{if } n=3 \end{cases}$$

Proof. For ease, we will write $P_{a,b}(T) := T^3+aT+b \in \mathbb{F}_\ell[T]$. From Appendix A, we see immediately that for $n \in \{0,1,3\}$,

$$\begin{aligned} &\left\{(a,b) \in \mathcal{E}_{(4,6)}^{\ell,I_0} \ : \ P_{a,b}(T) \text{ has } n \text{ roots}\right\} \\ &= \left\{(a,b) \in \mathbb{F}_\ell^2 \ : \ P_{(a,b)}(T) \text{ has } n \text{ roots in } \mathbb{F}_\ell \text{ and no repeated roots}\right\}, \end{aligned}$$

since $-(4a^3+27b^2) = \operatorname{disc}(P_{a,b}(T))$. Note that the 3 roots $\{\alpha_1,\alpha_2,\alpha_3\} \subseteq \overline{\mathbb{F}}_\ell$ of $P_{a,b}$ satisfy $\alpha_1+\alpha_2+\alpha_3 = 0$, because the T^2 coefficient in $P_{a,b}$ is 0.

Consider, first, the case $n=0$. Here $P_{a,b}(T)$ is irreducible, and the set of irreducible monic cubic polynomials is in $1:3$ correspondence with elements $\alpha \in \mathbb{F}_{\ell^3}\backslash\mathbb{F}_\ell$. Under this correspondence the polynomials with T^2 coefficient being 0 (our set of $P_{a,b}(T)$) correspond to α with trace 0. Thus

$$\begin{aligned} &\#\left\{(a,b) \in \mathbb{F}_\ell^2 \ : \ P_{(a,b)}(T) \text{ is irreducible over } \mathbb{F}_\ell\right\} \\ &= \frac{1}{3}\left(\#\ker(\mathrm{Tr}_{\mathbb{F}_{\ell^3}/\mathbb{F}_\ell}) - 1\right) \\ &= \frac{\ell^2-1}{3}, \end{aligned}$$

where we use that the trace is surjective (since $\ell \neq 3$, the only element of $\mathbb{F}_\ell$ with trace 0 is 0).

Now consider $n=1$. In this case, $P_{a,b}(T)$ must factor as a product of one monic linear polynomial and one monic irreducible quadratic polynomial. Moreover, since the T^2 coefficient is 0, the root of the linear polynomial must be equal to $-\mathrm{Tr}_{\mathbb{F}_{\ell^2}/\mathbb{F}_\ell}(\alpha)$ where α is a root of the quadratic factor. Thus

$$\begin{aligned} &\#\left\{(a,b) \in \mathbb{F}_\ell^2 \ : \ P_{(a,b)}(T) \text{ has 1 root in } \mathbb{F}_\ell \text{ and no repeated roots}\right\} \\ &= \#\left\{(a',b') \in \mathbb{F}_\ell^2 \ : \ T^2+a'T+b' \text{ is irreducible}\right\} \\ &= \frac{1}{2}\#\mathbb{F}_{\ell^2}\backslash\mathbb{F}_\ell = \frac{\ell(\ell-1)}{2}. \end{aligned}$$

Finally, for the case $n=3$, it is elementary to see that $\#\mathcal{E}_{(1,1)}^{\ell} = \ell^2-\ell$, and so the result follows by subtracting the counts of the previous cases. □

§ 6.2.2 | Averaging the (Additive) Genus Theory

We are now able to compute the average of the additive genus theory.

Notation 6.2.6. For each prime number ℓ, multiquadratic extension $K/\mathbb{Q}$ and pair

$(A,B) \in \mathcal{E}_\ell$ we define

$$\iota_\ell^{\mathrm{add}}(K/\mathbb{Q};A,B) = \begin{cases} 0 & \text{if } \ell \in \{2,3\} \\ 0 & \text{if } E_{A,B}/\mathbb{Q}_\ell \text{ has reduction type } I_n \text{ or } I_n^* \ \exists n>0, \\ \iota_\ell(K/\mathbb{Q};E_{A,B}) & \text{else} \end{cases}$$

We extend each $\iota_\ell^{\mathrm{add}}$ to $\mathbb{Z}_\ell^2$ by setting $\alpha_\ell(A,B)=0$ for $(A,B)\in\mathbb{Z}_\ell^2\backslash\mathcal{E}_\ell$

Lemma 6.2.7. *The endomorphism $\psi \in \mathrm{End}(\mathbb{Z}/\ell^{(4,6)}\mathbb{Z})$ given by $(a,b)\mapsto(\ell^2 a,\ell^3 b)$ induces surjections (for every $\alpha\in\mathbb{F}_\ell^\times$, $m\in\{0,1,3\}$) from*

$$\left\{(a,b)\in\mathcal{E}_{(4,6)}^{\ell,III} \ : \ a\ell^{-1}\equiv\alpha \mod \ell\right\} \text{ to } \left\{(a,b)\in\mathcal{E}_{(4,6)}^{\ell,III^*} \ : \ a\ell^{-3}\equiv\alpha \mod \ell\right\},$$

and from

$$\left\{(a,b)\in\mathcal{E}_{(4,6)}^{\ell,I_0} \ : \ T^3+aT+b \text{ has } n \text{ roots mod } \ell\right\}$$

to

$$\left\{(a,b)\in\mathcal{E}_{(4,6)}^{\ell,I_0^*} \ : \ T^3+a\ell^{-2}T+b\ell^{-3} \text{ has } n \text{ roots mod } \ell\right\}.$$

Additionally, $\#\ker(\psi)=\ell^5$.

Proof. This is clear. □

Lemma 6.2.8. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For every prime number ℓ and pair $(A,B)\in\mathbb{Z}_\ell^2$ write $\alpha_\ell(A,B)=\iota_\ell^{\mathrm{add}}(K/\mathbb{Q};A,B)$. Then the collection $\alpha=(\alpha_\ell)_\ell$ is an orderly local constant with associated constants $\mathbf{M}_\alpha=(4,6)$, $C_\alpha=2$, and $\Sigma_\alpha=\emptyset$.*

Moreover for each prime number ℓ we have

$$\mathbb{E}_\ell[\alpha_\ell] = \begin{cases} \frac{\ell(\ell-1)(\ell^5+1)(5\ell^3-4\ell^2+3)}{6\ell^{10}} & \text{if } K_\mathfrak{p}/\mathbb{Q}_\ell \text{ is ramified and quadratic;} \\ \frac{\ell(\ell-1)(3\ell^5+\ell^3-2\ell^2+3)}{3\ell^{10}} & \text{if } K_\mathfrak{p}/\mathbb{Q}_\ell \text{ is unramified and quadratic;} \\ \frac{\ell(\ell^5+1)(5\ell^4-9\ell^3+4\ell^2+6\ell-6)}{6\ell^{10}} & \text{if } K_\mathfrak{p}/\mathbb{Q}_\ell \text{ is biquadratic;} \\ 0 & \text{if } K_\mathfrak{p}/\mathbb{Q}_\ell \text{ is trivial or if } \ell\in\{2,3\} \end{cases}$$

where $\mathfrak{p}\in\Omega_K$ is any choice of place extending ℓ.

Proof. The claim that α is orderly is immediate from Proposition 3.2.9 and appendix A, as are the claimed values of $\mathbf{M}_\alpha, C_\alpha, \Sigma_\alpha$. We now prove the last claim, regarding the expectation. For $\ell\in\{2,3\}$ this is immediate from the definition of α_ℓ. Thus we assume that $\ell\geq 5$. If $K_\mathfrak{p}/\mathbb{Q}_\ell$ is trivial then this follows immediately from the definition of ι_ℓ.

If $K_\mathfrak{p}/\mathbb{Q}_\ell$ is unramified and quadratic then, since ℓ is inert in $K/\mathbb{Q}$, it follows from

Proposition 3.2.9, Appendix A and Lemma 6.2.7 that

$$\begin{aligned}\mathbb{E}_\ell[\alpha_\ell] &= \ell^{-10} \sum_{(A,B)\in\mathcal{E}_\ell^{(4,6)}} \alpha_\ell(A,B) \\ &= \ell^{-10}(1+\ell^{-5})\#\mathcal{E}_{\ell,III}^{(4,6)} \\ &\quad + 2\ell^{-15}\#\left\{(A,B)\in\mathcal{E}_{\ell,I_0}^{(4,6)} \ : \ T^3+AT+B\in\mathbb{F}_\ell[T] \text{ has 3 roots}\right\}.\end{aligned}$$

Considering this expression, it then follows from Lemmas 6.2.3 and 6.2.5 and Appendix A that

$$\begin{aligned}\mathbb{E}_\ell[\alpha_\ell] &= \ell^{-10}\left((\ell^6+\ell)(\ell-1)+2\ell^3\frac{(\ell-1)(\ell-2)}{6}\right) \\ &= \frac{3\ell^7-3\ell^6+\ell^5-3\ell^4+2\ell^3+3\ell^2-3\ell}{3\ell^{10}}.\end{aligned}$$

Factoring this expression then provides the required form.

If $K_\mathfrak{p}/\mathbb{Q}_\ell$ is ramified and quadratic then it is immediate from Proposition 3.2.9, Lemma 6.2.7 and Appendix A that

$$\begin{aligned}\ell^{10}\mathbb{E}_\ell[\alpha_\ell] &= \left(1+\ell^{-5}\right)\#\left\{(A,B)\in\mathcal{E}_{\ell,III}^{(4,6)} \ : \ A\ell^{-1}\notin\tfrac{\Delta_K}{\ell}\mathbb{F}_\ell^{\times 2}\right\} \\ &\quad + (1+\ell^{-5})\#\left\{(A,B)\in\mathcal{E}_{\ell,I_0}^{(4,6)} \ : \ T^3+AT+B\in\mathbb{F}_\ell[T] \text{ has 1 root}\right\} \\ &\quad + 2(1+\ell^{-5})\#\left\{(A,B)\in\mathcal{E}_{\ell,I_0}^{(4,6)} \ : \ T^3+AT+B\in\mathbb{F}_\ell[T] \text{ has 3 roots}\right\}.\end{aligned}$$

Considering this expression, as in the inert case above, it then follows from Lemmas 6.2.3 and 6.2.5 that

$$\begin{aligned}\mathbb{E}_\ell[\alpha_\ell] &= \ell^{-10}(1+\ell^{-5})\left(\ell^6\frac{\ell-1}{2}+\ell^8\frac{\ell(\ell-1)}{2}+\ell^8\frac{(\ell-1)(\ell-2)}{3}\right) \\ &= \frac{\ell(\ell-1)(\ell^5+1)(5\ell^3-4\ell^2+3)}{6\ell^{10}},\end{aligned}$$

as required.

Finally, if $K_\mathfrak{p}/\mathbb{Q}_\ell$ is biquadratic it follows from Proposition 3.2.11 and Lemma 6.2.7 that

$$\begin{aligned}\ell^{10}\mathbb{E}_\ell[\alpha_\ell] &= (1+\ell^{-5})\#\left\{(A,B)\in\mathcal{E}_{\ell,I_0} \ : \ T^3+AT+B\in\mathbb{F}_\ell \text{ has 1 root}\right\} \\ &\quad + 2(1+\ell^{-5})\#\left\{(A,B)\in\mathcal{E}_{\ell,I_0} \ : \ T^3+AT+B\in\mathbb{F}_\ell \text{ has 3 roots}\right\} \\ &\quad + 2(1+\ell^{-5})\#\mathcal{E}_{\ell,III}.\end{aligned}$$

Using Lemma 6.2.3, Lemma 6.2.5 and Appendix A we then deduce

$$\begin{aligned}\mathbb{E}_\ell[\alpha_\ell] &= \ell^{-10}(1+\ell^{-5})\left(\ell^8\frac{\ell(\ell-1)}{2}+\ell^6(\ell-1)+\ell^8\frac{(\ell-1)(\ell-2)}{3}\right) \\ &= \frac{\ell(\ell^5+1)(5\ell^4-9\ell^3+4\ell^2+6\ell-6)}{6\ell^{10}},\end{aligned}$$

concluding the proof. □

Having established that the contribution to the genus theory coming from additive primes gives an orderly local constant, and studied its properties, we now have our main application of Theorem 6.1.11.

Corollary 6.2.9. *For every multiquadratic extension $K/\mathbb{Q}$, pair $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$ and real number $X > \max\left\{55^2, \exp(\max(\{p \mid \Delta_K\})), C_2^{-2}\right\}$, there is an equality*

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \sum_{\substack{\ell \\ \text{prime}}} \iota_\ell^{\text{add}}(K/\mathbb{Q}; A, B) = \frac{4C_1C_2X^{5/6}}{\zeta(10)} \sum_{5\le\ell\le\log(X)} \mathcal{G}_K^{\text{add}}(\ell) + O\left(8(C_2+4)\frac{(C_1X^{5/6}+X^{1/2})}{\log(X)-8} + 22\left(C_2X^{1/2}+C_1X^{1/3}\right)(\log(X)+1)^{11}\right),$$

where $\mathcal{G}_K^{\text{add}}$ is the function of Notation 6.2.1 and the implied constant is 1.

Proof. This follows from Lemma 6.2.8 and Theorem 6.1.11, after noting that one can, rather wastefully, estimate

$$\sum_{\substack{\ell\le\log(X) \\ \text{prime}}} \ell^{10}\mathbb{E}[\alpha_\ell] \le \sum_{n\le\log(X)} 2n^{10} < (\log(X)+1)^{11}.$$

□

§ 6.3 | Multiplicative Primes

We now deal with the contribution to the genus theory coming from when elliptic curves (or one of their quadratic twists) have multiplicative reduction.

Notation 6.3.1. For each multiquadratic extension $K/\mathbb{Q}$, define the function

$$\mathcal{G}_K^{\text{mult}} : \{\ell \in \mathbb{Z}_{\ge 5} \ : \ \ell \text{ prime}\} \to \mathbb{R}$$

by

$$\mathcal{G}_K^{\text{mult}}(\ell) = \begin{cases} \frac{(\ell^8+\ell^3)(\ell-1)}{(\ell^{10}-1)} & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is ramified and quadratic;} \\ \frac{\ell^3(\ell-1)(\ell^5+\ell+1)}{(\ell+1)(\ell^{10}-1)} & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is unramified and quadratic;} \\ \frac{(\ell^8+\ell^3)(\ell-1)(4\ell+5)}{4(\ell^{10}-1)(\ell+1)} & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is biquadratic;} \\ 0 & \text{if } K_{\mathfrak{p}}/\mathbb{Q}_\ell \text{ is trivial.} \end{cases}$$

where $\mathfrak{p} \in \Omega_K$ is a choice of place extending ℓ.

§ 6.3.1 | Multiplicative Primes

Lemma 6.3.2. *Let $\ell \ge 5$ be a prime number, $n \ge 1$ be an integer. For every $B \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, and $u \in \mathbb{F}_\ell^\times$ we have that*

$$\#\left\{A \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \ : \ (4A^3+27B^2) = u\ell^n\right\} = \begin{cases} \#\mu_3(\mathbb{F}_\ell) & \text{if } (B^2 \mod \ell) \in 4\mathbb{F}_\ell^{\times 3}, \\ 0 & \text{else.} \end{cases}$$

Proof. This is immediate from Hensel lifting: since $\ell \geq 5$ and $\frac{1}{4}(u\ell^n - 27B^2) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, the roots of the polynomial $T^3 - \frac{1}{4}(u\ell^n - 27B^2)$ are in bijection with those of its reduction mod ℓ. □

Proposition 6.3.3. *Let $\ell \geq 5$ be a prime number and $n > 0$ an integer, and let $R_1, R_2 \in \left\{\mathbb{F}_\ell^{\times 2}, \mathbb{F}_\ell^\times \backslash \mathbb{F}_\ell^{\times 2}\right\}$. Then for every pair $\mathbf{C} = (C_1, C_2) \in \mathbb{R}_{>0}$ and every real number $X \geq \max\left\{C_2^{-1}, 1\right\}$ we have*

$$\begin{aligned}&\#\left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(X) \ : \ \begin{smallmatrix} E_{A,B} \text{ is type } I_n \text{ at } \ell \\ (B \mod \ell) \in R_1 \\ ((4A^3+27B^2)/\ell^n \mod \ell) \in R_2 \end{smallmatrix}\right\} \\ &= \frac{4C_1C_2X^{5/6}}{\zeta(10)} \frac{\ell^{8-n}(\ell-1)^2}{4(\ell^{10}-1)} + O\left(C_1X^{1/3} + C_2\ell X^{1/2} + 1\right)\end{aligned}$$

where the implied constant may be taken to be 2^6.

Proof. We begin similarly to Lemma 6.1.8: the discriminant nonzero condition contributes at most $2(2C_1X^{1/3}+2)$. Then,

$$\begin{aligned}&\#\left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(X) \ : \ \begin{smallmatrix} E_{A,B} \text{ is type } I_n \text{ at } \ell \\ (B \mod \ell) \in R_1 \\ ((4A^3+27B^2)/\ell^n \mod \ell) \in R_2 \end{smallmatrix}\right\} \\ &= \sum_{\substack{|B| \leq C_2X^{1/2} \\ (B \mod \ell) \in R_1}} \#\left\{|A| \leq C_1X^{1/3} \ : \ \begin{smallmatrix} 4A^3+27B^2 \mod \ell^{n+1} \in \ell^n R_2; \\ \text{for every prime number } \ell \text{ such that } \ell^6 | B \text{ we have } \ell^4 \nmid A. \end{smallmatrix}\right\} \\ &= \sum_{\substack{|B| \leq C_2X^{1/2} \\ (B \mod \ell) \in R_1 \\ (B^2 \mod \ell) \in 4\mathbb{F}_\ell^{\times 3}}} \left(\frac{2C_1X^{1/3}\#\mu_3(\mathbb{F}_\ell)(\ell-1)}{2\ell^{n+1}} \prod_{\substack{p^6|B \\ p \text{ prime}}} (1-p^{-4}) + O\left(\ell \prod_{\substack{p^6|B \\ \ell \text{ prime}}} p^4\right)\right)\end{aligned}$$

where the second equality follows from Lemma 6.3.2, and the implied constant is 2. Dealing with the error term, by Lemma 6.1.6 we bound

$$2\ell \sum_{|B| \leq C_2X^{1/2}} \prod_{\substack{p^6|B \\ \ell \text{ prime}}} p^4 \leq \frac{124 + 20\zeta(2)}{5} C_2\ell X^{1/2} < 32C_2\ell X^{1/2}.$$

For the main term, Lemma 6.1.5 shows that

$$\begin{aligned}&\sum_{\substack{|B| \leq C_2X^{1/2} \\ (B \mod \ell) \in R_1 \\ (B^2 \mod \ell) \in 4\mathbb{F}_\ell^{\times 3}}} \frac{2C_1X^{1/3}\#\mu_3(\mathbb{F}_\ell)(\ell-1)}{2\ell^{n+1}} \prod_{\substack{p^6|B \\ p \text{ prime}}} (1-p^{-4}) \\ &= \frac{2C_1X^{1/3}\#\mu_3(\mathbb{F}_\ell)(\ell-1)}{2\ell^{n+1}} \#\mathbb{F}_\ell^{\times 6}\left(\frac{2C_2X^{1/2}}{\zeta(10)\ell(1-\ell^{-10})} + O(1)\right) \\ &= \frac{4C_1C_2X^{5/6}}{\zeta(10)} \frac{\ell^{8-n}(\ell-1)^2}{4(\ell^{10}-1)} + O\left(\frac{C_1X^{1/3}}{\ell^{n-1}}\right)\end{aligned}$$

where in the first equality we use that the restrictions on the summand $B \mod \ell$ are equivalent to fixing the image of B in $\mathbb{F}_\ell^\times/\mathbb{F}_\ell^{\times 6}$, and in the second we use the Chinese

remainder theorem to deduce that $\#\mu_3(\mathbb{F}_\ell)\mathbb{F}_\ell^{\times 6} = \#\mathbb{F}_\ell^{\times 2} = (\ell-1)/2$. The error term in the final line then has implied constant at most $17/12$. □

Remark 6.3.4. The proof here is similar to that of Lemma 6.1.8, however if we were simply to apply that Lemma here then in order to have well defined congruence conditions we would have to count the pairs (A,B) over congruence classes in $(\mathbb{Z}/\ell^{n+1}\mathbb{Z})^2$, which would lead to a coefficient of ℓ^n in our error. This will be too large our application, since we will have $\ell, n \approx \log(X)$. We avoid this in the proof above by using that the condition we need to apply in the second summation need not be detected mod ℓ^n but can in fact be seen mod ℓ (removing the n in the error).

§ 6.3.2 | Averaging the (Multiplicative) Genus theory

Notation 6.3.5. For each prime number ℓ, multiquadratic extension $K/\mathbb{Q}$ and pair $(A,B) \in \mathcal{E}_\ell$ we define

$$\iota_\ell^{\mathrm{mult}}(K/\mathbb{Q}; A, B) = \begin{cases} 0 & \text{if } \ell \in \{2,3\} \\ \iota_\ell(K/\mathbb{Q}; E_{A,B}) & \text{if } E_{A,B}/\mathbb{Q}_\ell \text{ has reduction type } I_n \text{ or } I_n^*,\ \exists n>0, \\ 0 & \text{else} \end{cases}$$

We extend each $\iota_\ell^{\mathrm{mult}}$ to $\mathbb{Z}_\ell^2$ by setting $\iota_\ell^{\mathrm{mult}}(A,B) = 0$ for $(A,B) \in \mathbb{Z}_\ell^2 \backslash \mathcal{E}_\ell$.

We record a useful lemma.

Lemma 6.3.6. *Let $X > 0$ be a real number, $\ell \geq 5$ be a prime number and $\mathbf{C} \in \mathbb{R}_{>0}^2$. Moreover, let $n > 0$ be an integer and $R_1, R_2 \in \left\{\mathbb{F}_\ell^{\times 2}, \mathbb{F}_\ell^\times \backslash \mathbb{F}_\ell^{\times 2}\right\}$. Entrywise multiplication by (ℓ^2, ℓ^3) induces bijections for each $n > 0$,*

$$\left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(\ell^{-6}X) \ : \ \substack{E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n \\ 6B \in R_1 \\ \Delta(A,B)\ell^{-n} \in R_2}\right\} \to \left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(X) \ : \ \substack{E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n^* \\ 6B\ell^{-3} \in R_1 \\ \Delta(A,B)\ell^{-(n+6)} \in R_2}\right\}.$$

Proof. Immediate from Tate's algorithm (Appendix A). □

Unramified Quadratic Places

Lemma 6.3.7. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Let $\ell \geq 5$ be a prime number and $\mathfrak{p} \in \Omega_K$ be a place extending ℓ such that $K_\mathfrak{p}/\mathbb{Q}_\ell$ is the unramified quadratic extension. Then for every pair $(C_1, C_2) \in \mathbb{R}_{>0}$ and every $X \geq \max\left\{C_2^{-2},\ 1,\ \Delta(C_1,C_2)^{-1}\ell\right\}$ we have*

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) = \frac{4C_1C_2X^{5/6}}{\zeta(10)}\mathcal{G}_K^{\mathrm{mult}}(\ell) + O\left(\log(\Delta(C_1,C_2)X)\left(C_1X^{1/3} + C_2\ell X^{1/2} + 1\right) + \frac{C_1C_2}{\Delta(C_1,C_2)X^{7/6}}\right)$$

where the implied constant can be taken to be 2^8.

Proof. By Proposition 3.2.9 we have an identity

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B)\\
&= \sum_{n=1}^{\log(\Delta(C_1,C_2)X)/2\log(\ell)} \#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)\ :\ E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_{2n>0} \text{ or } I^*_{2n-1}\right\}\\
&+2\sum_{n=1}^{\log(\Delta(C_1,C_2)X)/2\log(\ell)} \#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)\ :\ \substack{E_{A,B}/\mathbb{Q}_\ell \text{ has type } I^*_{2n>0}\\ -\Delta(A,B)\ell^{-(6+2n)}\in\mathbb{F}_p^{\times 2}}\right\},
\end{aligned}$$

where we can restrict the range of summation for n because $E_{A,B}/\mathbb{Q}_\ell$ having type I_n or I_n^* presupposes that at least $\ell^n \mid \Delta(A,B) \le \Delta(C_1,C_2)X$. Now by Lemma 6.3.6 and Proposition 6.3.3 we have

$$\begin{aligned}
\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) =& \frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^8(\ell-1)^2}{(\ell^{10}-1)}(1+\ell^{-4}+\ell^{-5})\sum_{n=1}^{\log(\Delta(C_1,C_2)X)/2\log(\ell)}\ell^{-2n}\\
&+O\left(\log(\Delta(C_1,C_2)X)\left(C_1X^{1/3}+C_2\ell X^{1/2}+1\right)\right).
\end{aligned}$$

where the implied constant is at worst $2^6\times 12/2\log(\ell) < 2^8$. Note that

$$\begin{aligned}
\sum_{n=1}^{\log(\Delta(C_1,C_2)X)/2\log(\ell)}\ell^{-2n} &= \frac{1-\ell^{-2\lfloor\log(\Delta(C_1,C_2)X)/2\log(\ell)\rfloor}}{\ell^2-1}\\
&= \frac{1}{(\ell^2-1)}+O\left(\frac{1}{\Delta(C_1,C_2)X}\right),
\end{aligned}$$

where the implied constant is $25/24$. Applying this identity the main term above, we simplify to

$$\begin{aligned}
\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) =& \frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^3(\ell-1)(\ell^5+\ell+1)}{(\ell+1)(\ell^{10}-1)}+O\left(\frac{C_1C_2}{\Delta(C_1,C_2)X^{1/6}}\right)\\
&+O\left(\log(\Delta(C_1,C_2)X)\left(C_1X^{1/3}+C_2\ell X^{1/2}+1\right)\right).
\end{aligned}$$

where the implied constants are $\frac{25}{4}$ and 2^8 respectively. □

Ramified Quadratic Places

Lemma 6.3.8. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Let $\ell\ge 5$ be a prime number and $\mathfrak{p}\in\Omega_K$ be a place extending ℓ such that $K_\mathfrak{p}/\mathbb{Q}_\ell$ is a ramified quadratic extension. Then for every pair $(C_1,C_2)\in\mathbb{R}_{>0}$ and real number $X\ge\max\left\{1,C_2^{-1},\Delta(C_1,C_2)^{-1}\ell\right\}$ we have*

$$\begin{aligned}
\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) =& \frac{4C_1C_2X^{5/6}}{\zeta(10)}\mathcal{G}_K^{\mathrm{mult}}(\ell)\\
&+O\left(\frac{C_1C_2}{\Delta(C_1,C_2)X^{1/6}}+\log(\Delta(C_1,C_2)X)\left(C_1X^{1/3}+C_2\ell X^{1/2}+1\right)\right)
\end{aligned}$$

where the implied constant can be taken to be 2^9.

Proof. Let $\theta \in \mathbb{Q}_\ell$ be a uniformiser such that $K_\mathfrak{p} = \mathbb{Q}_\ell(\sqrt{\theta})$. Using Proposition 3.2.9 to compute $\iota_\ell^{\mathrm{mult}}(A,B)$ for $(A,B) \in \mathcal{E}$ we obtain

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) \\
&= \sum_{n=1}^{\log(\Delta(C_1,C_2)X)/\log(\ell)} \Bigg(\#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \;:\; \begin{smallmatrix} E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n, \\ (-1)^{n+1}6B\Delta(A,B)\theta^{-n}\in\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\} \\
&\qquad + 2\#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \;:\; \begin{smallmatrix} E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_{2n}, \\ 6B\notin\mathbb{F}_\ell^{\times 2} \\ -\Delta(A,B)\theta^{-n}\in\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\} \\
&\qquad + \#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \;:\; \begin{smallmatrix} E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n^*, \\ (-1)^{n+1}6B\Delta(A,B)\theta^{-(n+9)}\in\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\} \\
&\qquad + 2\#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \;:\; \begin{smallmatrix} E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_{2n}^*, \\ 6B\theta^{-3}\notin\mathbb{F}_\ell^{\times 2} \\ -\Delta(A,B)\theta^{-(n+6)}\in\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\} \Bigg)
\end{aligned}$$

where we can restrict the range of summation for n because $E_{A,B}/\mathbb{Q}_\ell$ having type I_n presupposes that $\ell^n \mid \Delta(A,B) \le \Delta(C_1,C_2)X$. Now by Lemma 6.3.6 and Proposition 6.3.3 we can simplify this to

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) \\
&= \sum_{n=1}^{\log(\Delta(C_1,C_2)X)/\log(\ell)} \Bigg((1+\ell^{-5})\frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^8(\ell-1)^2}{2(\ell^{10}-1)}(\ell^{-n}+\ell^{-2n}) \\
&\qquad + O\left(C_1X^{1/3}+C_2\ell X^{1/2}+1\right)\Bigg),
\end{aligned}$$

with implied constant 2^9. Note that

$$\begin{aligned}
&\sum_{n=1}^{\log(\Delta(C_1,C_2)X)/\log(\ell)} \ell^{-n}+\ell^{-2n} \\
&= \frac{1-\ell^{-2\lfloor\log(\Delta(C_1,C_2)X)/\log(\ell)\rfloor}}{\ell^2-1} + \frac{1-\ell^{-\lfloor\log(\Delta(C_1,C_2)X)/\log(\ell)\rfloor}}{\ell-1} \\
&= \frac{\ell+2}{\ell^2-1} - \frac{(\ell+1)\ell^{-\lfloor\log(\Delta(C_1,C_2)X)/\log(\ell)\rfloor}+\ell^{-2\lfloor\log(\Delta(C_1,C_2)X)/\log(\ell)\rfloor}}{\ell^2-1} \\
&= \frac{\ell+2}{\ell^2-1} + O\left(\frac{1}{\Delta(C_1,C_2)X}\right)
\end{aligned}$$

Where the implied constant is at most $\frac{25}{24}+\frac{5}{4}<4$. Evaluating the summation we arrive at

$$\begin{aligned}
\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) =& \frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{(\ell^8+\ell^3)(\ell-1)^2(\ell+2)}{(\ell^{10}-1)(\ell^2-1)} \\
&+ O\left(\frac{(\ell^8+\ell^3)(\ell-1)^2C_1C_2}{(\ell^{10}-1)\Delta(C_1,C_2)X^{1/6}}\right) \\
&+ O\left(\log(\Delta(C_1,C_2)X)\left(C_1X^{1/3}+C_2\ell X^{1/2}+1\right)\right),
\end{aligned}$$

with implied constants $2/\zeta(10)$ and 2^9 respectively. Noting that

$$\frac{(\ell^8+\ell^3)(\ell-1)^2}{(\ell^{10}-1)} < 1$$

then the result then follows since $1/\zeta(10) < 1$. □

Biquadratic Places

Lemma 6.3.9. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Assume that $\ell \geq 5$ is a prime number and $\mathfrak{p} \in \Omega_K$ is a prime dividing ℓ such that $K_\mathfrak{p}/\mathbb{Q}_\ell$ is the biquadratic extension. Then for every pair $(C_1, C_2) \in \mathbb{R}_{>0}$ and real number $X \geq \max\left\{C_2^{-2},\ 1,\ \Delta(C_1,C_2)^{-1}\ell\right\}$ we have*

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) = \frac{4C_1C_2X^{5/6}}{\zeta(10)}\mathcal{G}_K^{\mathrm{mult}}(\ell) + O\left(\frac{C_1C_2}{\Delta(C_1,C_2)X^{1/6}} + \log(\Delta(C_1,C_2)X)(C_1X^{1/3}+C_2\ell X^{1/2}+1)\right),$$

where the implied constant can be taken to be 2^9.

Proof. By Proposition 3.2.11 we have an identity

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B)\\
&= \sum_{n=1}^{\log(\Delta(C_1,C_2)X)/\log(\ell)} \#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \ :\ \begin{smallmatrix}E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n \text{ and either:}\\ n \text{ is odd or } -\Delta(A,B)\theta^{-n}\notin\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\}\\
&\qquad + 2\,\#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \ :\ \begin{smallmatrix}E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n \text{ and both:}\\ n \text{ is even and } -\Delta(A,B)\theta^{-n}\in\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\}\\
&\qquad + \ \#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \ :\ \begin{smallmatrix}E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n^* \text{ and either:}\\ n \text{ is odd or } -\Delta(A,B)\theta^{-(n+6)}\notin\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\}\\
&\qquad + 2\,\#\left\{(A,B)\in\mathcal{E}^{\mathbf{C}}(X) \ :\ \begin{smallmatrix}E_{A,B}/\mathbb{Q}_\ell \text{ has type } I_n^* \text{ and both:}\\ n \text{ is even and } -\Delta(A,B)\theta^{-(n+6)}\in\mathbb{F}_\ell^{\times 2}\end{smallmatrix}\right\},
\end{aligned}$$

where we can restrict the range of summation for n because $E_{A,B}/\mathbb{Q}_\ell$ having type I_n presupposes that $\ell^n \mid \Delta(A,B) \leq \Delta(C_1,C_2)X$. Now by Lemma 6.3.6 and Proposition 6.3.3 we have

$$\begin{aligned}
&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B)\\
&= \frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^8(\ell-1)^2}{(\ell^{10}-1)}(1+\ell^{-5})\left(\sum_{n=1}^{\log(\Delta(C_1,C_2)X)/\log(\ell)} \ell^{-n} + \sum_{n=1}^{\log(\Delta(C_1,C_2)X)/2\log(\ell)} \frac{1}{4}\ell^{-2n}\right)\\
&\quad + O\left(\log(\Delta(C_1,C_2)X)(C_1X^{1/3}+C_2\ell X^{1/2}+1)\right)
\end{aligned}$$

where since $10 \times \log(\ell)^{-1} < 8$ the implied constant is at worst 2^9. Note that

$$\begin{aligned}\sum_{n=1}^{\log(\Delta(C_1,C_2)X)/\log(\ell)} \ell^{-n} &= \frac{1-\ell^{-\lfloor \log(\Delta(C_1,C_2)X)/\log(\ell)\rfloor}}{\ell-1} \\ &= \frac{1}{\ell-1} + O\left(\frac{1}{\Delta(C_1,C_2)X}\right), \\ \sum_{n=1}^{\log(\Delta(C_1,C_2)X)/2\log(\ell)} \ell^{-2n} &= \frac{1-\ell^{-2\lfloor \log(\Delta(C_1,C_2)X)/2\log(\ell)\rfloor}}{\ell^2-1} \\ &= \frac{1}{(\ell^2-1)} + O\left(\frac{1}{\Delta(C_1,C_2)X}\right),\end{aligned}$$

where the implied constants are $\frac{5}{4}$ and $\frac{25}{24}$ respectively. Thus we have

$$\begin{aligned}&\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \iota_\ell^{\mathrm{mult}}(A,B) \\ =&\frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^8(\ell-1)^2}{(\ell^{10}-1)}(1+\ell^{-5})\left(\frac{1}{\ell-1}+\frac{1}{4(\ell^2-1)}\right) \\ &+O\left(\log(\Delta(C_1,C_2)X)(C_1X^{1/3}+C_2\ell X^{1/2}+1)\right), \\ &+O\left(\frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{\ell^8(\ell-1)^2}{(\ell^{10}-1)}(1+\ell^{-5})\frac{1}{\Delta(C_1,C_2)X}\right) \\ =&\frac{4C_1C_2X^{5/6}}{\zeta(10)}\frac{(\ell^8+\ell^3)(\ell-1)^2(4\ell+5)}{4(\ell^{10}-1)(\ell^2-1)} \\ &+O\left(\log(\Delta(C_1,C_2)X)(C_1X^{1/3}+C_2\ell X^{1/2}+1)+\frac{C_1C_2}{\Delta(C_1,C_2)X^{1/6}}\right),\end{aligned}$$

with the implied constants in the first equality being 2^9 and $145/96$, and that in the final line being 2^9 (using that $(\ell^8+\ell^3)(\ell-1)^2 < \ell^{10}-1$ and $4/\zeta(10) < 4$). This then matches the proposed result, and so the proof concludes. □

The Multiplicative Genus Theory

Having dealt with the contributions of the various types of primes to the average multiplicative genus theory, we are now ready to finish the computation. We begin, as in the case of averaging orderly local constants in §6.2, by discarding the contribution of large primes.

Lemma 6.3.10. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For every $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$, and every real number $X > \max\{55^2, \exp(\max\{\ell \text{ prime} \ : \ \ell \mid \Delta_K\})\}$*

$$\left|\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \sum_{\substack{\ell\geq\log(X)\\ \text{prime}}} \iota_\ell^{\mathrm{mult}}(A,B)\right| \leq 8(C_2+4)\frac{C_1X^{5/6}+X^{1/2}}{\log(X)-8}$$

Proof. With notation as in the lemma statement, let $N = \lfloor \log(\Delta(C_1,C_2)X)\rfloor$. Let

$\gamma = (\gamma_\ell)_{\ell \text{ prime}}$ be the collection of functions

$$\gamma_\ell : \mathbb{Z}_\ell^2 \to \mathbb{R}$$
$$(A,B) \mapsto \begin{cases} \iota_\ell^{\text{mult}}(A,B) & \text{if } v_\ell(\Delta(A,B)) \leq N \\ 0 & \text{else} \end{cases}$$

Note that $\iota_\ell^{\text{mult}}(A,B) \neq 0$ presupposes that $\ell \mid \Delta(A,B)$, so in particular ι_ℓ^{mult} and γ_ℓ agree on $\mathcal{E}^{\mathbf{C}}(X)$. Note that, since $\gamma_\ell(A,B)$ is determined by the image of (A,B) in $\mathbb{Z}/\ell^{N+1}\mathbb{Z} \times \mathbb{Z}/\ell^{N+1}\mathbb{Z}$, by Proposition 3.2.9 and Proposition 3.2.11, γ is an orderly local constant with constants $\mathbf{M}_\alpha = (N+1, N+1)$, $C_\alpha = 2$, and $\Sigma_\alpha = \{\ell \text{ prime } : \ \ell \mid \Delta_K\}$. Thus the result follows from Lemma 6.1.10. □

We can now compute the average genus theory at multiplicative primes.

Theorem 6.3.11. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For every $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$, and every real number $X > \max\left\{C_2^{-1}, 55^2, \exp(\max\{\ell \text{ prime } : \ \ell \mid \Delta_K\})\right\}$*

$$\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \sum_{\substack{\ell \\ \text{prime}}} \iota_\ell^{\text{mult}}(A,B) = \frac{4C_1C_2X^{5/6}}{\zeta(10)} \left(\sum_{\substack{5\leq\ell\leq\log(X) \\ \text{prime}}} \mathcal{G}_K^{\text{mult}}(\ell) \right)$$
$$O\left(\frac{C_1C_2\log(X)}{\Delta(C_1,C_2)X^{1/6}} + \log(X)\log(\Delta(C_1,C_2)X)\left(C_1X^{1/3} + C_2\log(X)X^{1/2} + 1\right) \right)$$
$$+ O\left((C_2+4)\frac{C_1X^{5/6} + X^{1/2}}{\log(X) - 8} \right),$$

where the implied constants are 2^{11} and 8 respectively, $\mathcal{E}^{\mathbf{C}}(X)$ is as in Definition 6.1.1, and $\mathbb{E}_\ell$ is as in Notation 6.1.7.

Proof. By Lemma 6.3.10 we can restrict the range of our primes, and then applying Lemma 6.3.7, Lemma 6.3.8 and Lemma 6.3.9 we obtain the required result. □

§ 6.4 | The Archimedean Contribution

In order to determine the average behaviour of $g_2(K/\mathbb{Q}; E)$ we have so far broken the contribution from non-archimedean places into additive and multiplicative contributions and then computed the averages of each of those. It remains to determine the contribution coming from the archimedean place. We firstly record a lemma which computes the norm index.

Lemma 6.4.1 ([Kra81, Proposition 6])**.** *Let $E/\mathbb{R}$ be an elliptic curve, write Δ_E for the discriminant of a choice of Weierstrass model for $E/\mathbb{R}$. Then*

$$\#E(\mathbb{R})/N_{\mathbb{C}/\mathbb{R}}E(\mathbb{C}) = \begin{cases} 2 & \text{if } \Delta_E > 0 \\ 1 & \text{else} \end{cases}$$

Thus we need only count the number of elements $(A,B) \in \mathcal{E}^{\mathbf{C}}(X)$ such that $\Delta(A,B) < 0$ (note that $\Delta(A,B) = -\Delta_{E_{A,B}}$ in the lemma above).

Lemma 6.4.2. *Let $\mathbf{C} = (C_1, C_2) \in \mathbb{R}^2_{>0}$, and write $M(\mathbf{C}) := \min\left\{C_2, \frac{2C_1^{3/2}}{\sqrt{27}}\right\}$. For every real number $X \geq 1$,*

$$\#\left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(X) \ : \ \Delta(A,B) < 0\right\} = \frac{4C_1C_2X^{5/6}}{\zeta(10)}\left(\frac{M(\mathbf{C})}{2C_2} - \frac{9M(\mathbf{C})^{5/3}}{20C_1C_2\sqrt[3]{4}}\right) + O\left((C_1 + M(\mathbf{C})^{2/3})X^{1/3} + M(\mathbf{C})X^{1/2} + 1\right)$$

where the implied constant is at worst 32.

Proof. We have

$$\begin{aligned}
&\#\left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(X) \ : \ \Delta(A,B) < 0\right\} \\
&= \sum_{|B| \leq C_2X^{1/2}} \#\left\{A \in \mathbb{Z} \ : \ \begin{smallmatrix} |A| \leq C_1X^{1/3} \\ \gcd(A^3,B^2) \text{ is } 12^{\text{th}}\text{-power free} \\ 4A^3+27B^2<0 \end{smallmatrix}\right\} \\
&= \sum_{|B| \leq C_2X^{1/2}} \#\left\{A \in \mathbb{Z} \ : \ \begin{smallmatrix} -C_1X^{1/3} \leq A < \frac{3B^{2/3}}{\sqrt[3]{4}} \\ \gcd(A^3,B^2) \text{ is } 12^{\text{th}}\text{-power free} \end{smallmatrix}\right\} \\
&= \sum_{1 \leq |B| \leq M(\mathbf{C})X^{1/2}} \left(\left(C_1X^{1/3} - \frac{3}{\sqrt[3]{4}}B^{2/3}\right)\prod_{\ell^6 | B}(1-\ell^{-4}) + O\left(\prod_{\ell^6|B}\ell^4\right)\right) + O\left(C_1X^{1/3}\right),
\end{aligned}$$

where the first implied constant is 2 and the second is 1 (the second error term is the $B = 0$ term). Summing first error term (with implied constant) here gives at worst $32M(\mathbf{C})X^{1/2}$ by Lemma 6.1.6, so we deal with the two terms in the main term to complete the proof. Firstly, by Lemma 6.1.5

$$\sum_{1 \leq |B| \leq M(\mathbf{C})X^{1/2}} C_1X^{1/3}\left(\prod_{\ell^6|B}(1-\ell^{-4})\right) = \frac{2C_1M(\mathbf{C})X^{5/6}}{\zeta(10)} + O\left(C_1X^{1/3}\right)$$

with implied constant 17/6. For the remaining summand, we use Abel's summation formula and Lemma 6.1.5 to obtain, writing $f(B) := f_1(B) = \prod_{\ell^6|B}(1-\ell^{-4})$ for each integer $B \neq 0$,

$$\begin{aligned}
&\sum_{1 \leq |B| \leq M(\mathbf{C})X^{1/2}} B^{2/3}f(B) \\
&= 2\left(\left(\sum_{1 \leq B \leq M(\mathbf{C})X^{1/2}} f(B)\right)M(\mathbf{C})^{2/3}X^{1/3} - \frac{2}{3}\int_1^{M(\mathbf{C})X^{1/2}}\left(\sum_{1 \leq B \leq y} f(B)\right)y^{-1/3}dy\right) \\
&= \frac{2M(\mathbf{C})^{5/3}X^{5/6}}{\zeta(10)} - \frac{4}{3\zeta(10)}\int_1^{M(\mathbf{C})X^{1/2}} y^{2/3}dy + O\left(M(\mathbf{C})^{2/3}X^{1/3}\right) \\
&\qquad + O\left(\int_1^{M(\mathbf{C})X^{1/2}} y^{-1/3}dy\right) \\
&= \frac{6M(\mathbf{C})^{5/3}X^{5/6}}{5\zeta(10)} + O\left(M(\mathbf{C})^{2/3}X^{1/3} + 1\right)
\end{aligned}$$

where the error terms in the second equality are 17/6 and 68/9. The implied constant in the third and fourth lines is then at worst 85/6, where we are using that $X \geq 1$ and $\frac{4}{5\zeta(10)} < \frac{8}{9}$. Thus in total,

$$\#\left\{(A,B) \in \mathcal{E}^{\mathbf{C}}(X) \ : \ \Delta(A,B) < 0\right\} = \frac{4C_1C_2X^{5/6}}{\zeta(10)}\left(\frac{M(\mathbf{C})}{2C_2} - \frac{9M(\mathbf{C})^{5/3}}{20C_1C_2\sqrt[3]{4}}\right) + O\left((C_1 + M(\mathbf{C})^{2/3})X^{1/3} + M(\mathbf{C})X^{1/2} + 1\right)$$

where the implied constant is at most 32 as required. □

§ 6.5 | Applications

We have now completed all of the work required to obtain the average of the genus theory part of the 2-Selmer groups of elliptic curves (defined over $\mathbb{Q}$) over a multiquadratic extension. We will begin by drawing together the results of this chapter to determine the average of the genus theory part in 2-Selmer groups over multiquadratic extensions. Then we pull forward a result from the next chapter, which will allow us to control the average size of the corestriction Selmer groups, and then go on to apply these together to obtain results for the fixed space in the 2-Selmer group and even for the full 2-Selmer group in some cases.

From now on we will restrict our interest to the natural ordering on elliptic curves, given by the sets

$$\mathcal{E}(X) := \mathcal{E}^{(1,1)}(X).$$

This will reduce some headache in what follows.

§ 6.5.1 | The Average of the Genus Theory

Throughout this chapter we have been focussed on computing the average of the genus theory. We split things up so that we could control the contributions to the average of the local norms from primes $\ell \geq 5$ of: multiplicative (including twists of multiplicative) reduction in §6.3; and additive (excluding twists of multiplicative) reduction in §6.2. Together with bounds to control the contribution of local norm indices at 2 and 3, this will enable us to compute the average of the genus theory.

Definition 6.5.1. For each multiquadratic extension $K/\mathbb{Q}$, define the function

$$\mathcal{G}_K : \Omega_{\mathbb{Q}} \to \mathbb{R}$$

as follows. We map each prime number $\ell \geq 5$ to

$$\mathcal{G}_K(\ell) = \begin{cases} \frac{\ell(\ell^5+1)(\ell-1)(5\ell^3+2\ell^2+3)}{6(\ell^{10}-1)} & \text{if } K/\mathbb{Q} \text{ is ramified and quadratic at } \ell, \\ \frac{\ell(\ell-1)(3\ell^7+3\ell^6+3\ell^5+\ell^4+2\ell^3+\ell^2+3\ell+3)}{3(\ell+1)(\ell^{10}-1)} & \text{if } K/\mathbb{Q} \text{ is unramified and quadratic at } \ell, \\ \frac{\ell(\ell^5+1)(10\ell^5+4\ell^4-7\ell^3+5\ell^2-12)}{12(\ell^{10}-1)(\ell+1)} & \text{if } K/\mathbb{Q} \text{ is biquadratic at } \ell, \\ 0 & \text{if } K/\mathbb{Q} \text{ is totally split at } \ell. \end{cases}$$

For the remaining finite primes we define

$$\mathcal{G}_K(2) = \begin{cases} 0 & \text{if } K/\mathbb{Q} \text{ is totally split at 2} \\ 2^{2+[K_2:\mathbb{Q}_2]} & \text{else;} \end{cases} \qquad \mathcal{G}_K(3) = \begin{cases} 0 & \text{if } K/\mathbb{Q} \text{ is totally split at 3,} \\ 4 & \text{else.} \end{cases}$$

We then send the infinite place to

$$\mathcal{G}_K(\infty) = \begin{cases} \frac{7}{10\sqrt{27}} & \text{if } K \text{ is imaginary} \\ 0 & \text{else.} \end{cases}$$

This notation then allows us to succinctly describe the average of the genus theory $g_2(K/\mathbb{Q}; E)$ (see Definition 2.2.8)

Theorem 6.5.2. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Then*

$$\sum_{\substack{v \in \Omega_{\mathbb{Q}} \\ v \nmid 6}} \mathcal{G}_K(v) \leq \lim_{X \to \infty} \frac{\sum_{(A,B) \in \mathcal{E}(X)} g_2(K/\mathbb{Q}; E_{A,B})}{\#\mathcal{E}(X)} \leq \sum_{v \in \Omega_{\mathbb{Q}}} \mathcal{G}_K(v),$$

where $\mathcal{G}_K$ is as in Definition 6.5.1. In particular, if 2 and 3 are totally split in $K/\mathbb{Q}$ then we have an equality

$$\lim_{X \to \infty} \frac{\sum_{(A,B) \in \mathcal{E}(X)} g_2(K/\mathbb{Q}; E_{A,B})}{\#\mathcal{E}(X)} = \sum_{v \in \Omega_{\mathbb{Q}}} \mathcal{G}_K(\ell).$$

Proof. By definition, for each elliptic curve $E/\mathbb{Q}$,

$$\begin{aligned} g_2(K/\mathbb{Q}; E) &= \sum_{v \in \Omega_{\mathbb{Q}}} \iota_v(K/\mathbb{Q}; E) \\ &= \iota_\infty(K/\mathbb{Q}; E) + \iota_2(K/\mathbb{Q}; E) + \iota_3(K/\mathbb{Q}; E) + \sum_{\substack{\ell \geq 5 \\ \text{prime}}} \iota_\ell^{\text{add}}(K/\mathbb{Q}; E) \\ &\quad + \sum_{\substack{\ell \geq 5 \\ \text{prime}}} \iota_\ell^{\text{mult}}(K/\mathbb{Q}; E). \end{aligned}$$

Firstly by Lemma 5.3.3 we have for $\ell \in \{2, 3\}$

$$0 \leq \iota_\ell(K/\mathbb{Q}; E) \leq \mathcal{G}_K(\ell),$$

so that the average for these is bounded similarly. Next, it is simple to compute that

$$\#\mathcal{E}(X) \sim \frac{4X^{5/6}}{\zeta(10)},$$

(for example, apply Theorem 6.1.11 with the orderly local constant α given by taking α_2 to be the constant function 1 and α_ℓ to be the constant function 0 for every $\ell > 2$) so in particular by Lemma 6.4.1 and Lemma 6.4.2 we know that the average of $\iota_\infty(K/\mathbb{Q}; E)$ is $\mathcal{G}_K(\infty)$. Moreover, applying Theorem 6.3.11 and Corollary 6.2.9 we obtain the average

for the remaining sum and so the claimed result. □

§ 6.5.2 | The Corestriction Selmer Group: A Preview

In Chapter 7 we obtain the average size of the corestriction Selmer group. In this subsection we state the key result of that chapter, we ask that the reader wait patiently for the proof – the tools used are quite distinct from the ones in this chapter. Also, the application is more related to the material in this chapter.

Definition 6.5.3. For every multiquadratic extension $K/\mathbb{Q}$ and each prime number $p \geq 5$ define local factors

$$L_p(\mathscr{C}(K)) := \begin{cases} \frac{(p-1)(p^4-p^3+p^2-p+1)(46p^5+62p^4+79p^3+84p^2+84p+48)}{48(p^{10}-1)} & \text{if } K/\mathbb{Q} \text{ is ramified and quadratic at } p, \\ \frac{16p^{11}+16p^{10}+-8p^9+8p^8-8p^7-10p^6-4p^5+7p^4-p^3-8p^2-24p-1}{16(p^{10}-1)(p+1)} & \text{if } K/\mathbb{Q} \text{ is unramified and quadratic at } p, \\ \frac{(p+1)(p-1)(p^4-p^3+p^2-p+1)(5p^5+15p^4+13p^3+9p^2+13p+8)}{8(p^{10}-1)(p+1)} & \text{if } K/\mathbb{Q} \text{ is biquadratic at } p, \\ 1 & \text{if } K/\mathbb{Q} \text{ is totally split at } p. \end{cases}$$

For $p \in \{2,3\}$ we define some 'coarse' local factors

$$L_p(\mathscr{C}(K)) := \begin{cases} 1 & \text{if } K/\mathbb{Q} \text{ is totally split at } p, \\ \frac{1}{2^{2+[K_w:\mathbb{Q}_2]}} & \text{if } p=2 \text{ and } K/\mathbb{Q} \text{ is not totally split at } p, \\ \frac{1}{4} & \text{if } p=3 \text{ and } K/\mathbb{Q} \text{ is not totally split at } p. \end{cases}$$

Moreover, define an archimedean factor

$$L_\infty(\mathscr{C}(K)) := \begin{cases} \frac{1}{2} & \text{if } K \text{ is real}, \\ \frac{9}{20} & \text{if } K \text{ is imaginary}. \end{cases}$$

These local factors allow us to concisely describe the average size of corestriction Selmer groups in Chapter 7. For now, we will be content to pull forward a corollary of the results there, which gives an upper bound on the average dimension of corestriction Selmer groups.

Theorem 6.5.4 (Corollary 7.7.15)**.** *Let $K/\mathbb{Q}$ be a multiquadratic extension, then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_{A,B}[2])}{\#\mathcal{E}(X)} \leq \left(\frac{27}{4}\right)^{5/6} \left(4 \prod_{\substack{v\in\Omega_\mathbb{Q} \\ v\nmid 6}} L_v(\mathscr{C}(K)) \right),$$

where the factors $L_v(\mathscr{C}(K))$ are as in Definition 6.5.3.

§ 6.5.3 | 2-Selmer Groups over Multiquadratic Extensions

We can use the results above to obtain strong upper and lower bounds for the average dimension of the Galois fixed space inside 2-Selmer groups over multiquadratic extensions. We will take some notation to make the statements easier to parse.

Definition 6.5.5. Define the functions FS^+ and S^+ from the set of multiquadratic extensions to $\mathbb{R}_{>0}$ by

$$\mathrm{FS}^+(K) := \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}} \dim \mathrm{Sel}_2(E_{A,B}/K)^{\mathrm{Gal}(K/\mathbb{Q})}}{\#\mathcal{E}(X)},$$
$$S^+(K) := \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}} \dim \mathrm{Sel}_2(E_{A,B}/K)}{\#\mathcal{E}(X)},$$

and similarly let $\mathrm{FS}^-(K)$ and $S^-(K)$ be the liminfs for the above ratios. If $\mathrm{FS}^+(K) = \mathrm{FS}^-(K)$ then we denote the resulting value by $\mathrm{FS}(K)$, and similarly for $S(K)$.

Theorem 6.5.6. *Let $K/\mathbb{Q}$ be a multiquadratic extension and write $G := \mathrm{Gal}(K/\mathbb{Q})$. Then*

$$\sum_{\substack{v\in\Omega_\mathbb{Q}\\ v\nmid 6}} \mathcal{G}_K(v) \le \mathrm{FS}^-(K) \le \mathrm{FS}^+(K) \le \sum_{v\in\Omega_\mathbb{Q}} \mathcal{G}_K(v) + \left(\frac{27}{4}\right)^{5/6} \left(4 \prod_{\substack{v\in\Omega_\mathbb{Q}\\ v\nmid 6}} L_v(\mathscr{C}(K))\right),$$

where $\mathcal{G}_K$ is as in Definition 6.5.1, and $L_v(\mathscr{C}_K)$ is as in Definition 6.5.3.

Proof. By Lemma 5.3.7, for large X we have

$$\frac{\sum_{(A,B)\in\mathcal{E}} \left|\dim \mathrm{Sel}_{\mathscr{F}(K)}(\mathbb{Q}, E_{A,B}[2]) - \dim \mathrm{Sel}_2(E_{A,B}/K)^G\right|}{\#\mathcal{E}(X)} \ll \frac{\log(X)}{X^{1/6}}.$$

Moreover, by Lemma 2.2.11 we have an equality for every elliptic curve $E/\mathbb{Q}$

$$\dim \mathrm{Sel}_{\mathscr{F}(K)}(\mathbb{Q}, E[2]) = \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) + g_2(K/\mathbb{Q}; E).$$

We have the average of the genus theory part by Theorem 6.5.2, providing the lower bound and part of the upper bound, and an upper bound for that of the corestriction Selmer group by Theorem 6.5.4, providing the rest of the upper bound, and so result follows. □

In fact this also allows us to get upper and lower bounds on the average 2-Selmer rank via Lemma 2.2.13.

Corollary 6.5.7. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Then*

$$\sum_{\substack{v\in\Omega_\mathbb{Q}\\ v\nmid 6}} \mathcal{G}_K(v) \le S^-(K) \le S^+(K) \le 2\sum_{v\in\Omega_\mathbb{Q}} \mathcal{G}_K(v) + \left(\frac{27}{4}\right)^{5/6} \left(8 \prod_{\substack{v\in\Omega_\mathbb{Q}\\ v\nmid 6}} L_v(\mathscr{C}(K))\right).$$

Proof. Clearly $\mathrm{FS}^-(K) \le S^-(K)$ and by Lemma 2.2.13 we know that

$$S^+(K) \le [K:\mathbb{Q}]\mathrm{FS}^+(K).$$

The result then follows from Theorem 6.5.6. □

An interesting interpretation of Theorem 6.5.6 is the following.

Corollary 6.5.8 (Theorem 1.4.2)**.** *Assume that* $\mathrm{FS}(K)$ *exists for all* K *in a set* $\mathcal{K}$ *of multiquadratic fields in which* 2 *and* 3 *are totally split. Then for each* $K \in \mathcal{K}$*,*

$$\mathrm{FS}(K) = \sum_{v \in \Omega_{\mathbb{Q}}} \mathcal{G}_K(v) + O\left(\left(\frac{46}{48}\right)^{\omega(\Delta_K)}\right),$$

where the implied constant is independent of K*.*

Proof. It is clear from the definitions that for large enough p (independent of K), if p is ramified in $K/\mathbb{Q}$ then $L_p(\mathscr{C}(K)) \leq 46/48$. Since the unramified primes satisfy $L_p(\mathscr{C}(K)) \leq 1$ we have the result. □

§ 6.5.4 | 2-Selmer Groups over Quadratic Fields

We now apply these results for quadratic fields, where the representation theory of $\mathbb{F}_2[\mathbb{Z}/2\mathbb{Z}]$-modules allows us to obtain a stronger control on the full 2-Selmer group.

We begin by noting that, in fact, the probability that a 2-Selmer group over a quadratic extension has nontrivial Galois action is typically quite small. However, unlike in the family of quadratic twists in Chapter 4, we do not get that this is 0%.

Corollary 6.5.9. *For each squarefree integer* d*, write* $K = \mathbb{Q}(\sqrt{d})$ *and let* $G = \mathrm{Gal}(K/\mathbb{Q})$*. Then*

$$\limsup_{X\to\infty} \frac{\#\left\{(A,B) \in \mathcal{E}(X) \ : \ \substack{G \text{ acts nontrivially} \\ \text{on } \mathrm{Sel}_2(E_{A,B}/K)}\right\}}{\#\mathcal{E}(X)} \ll \left(\frac{46}{48}\right)^{\omega(d)},$$

with constant independent of d*.*

Proof. By Corollary 4.1.4(iii), for each $X \geq 0$

$$\begin{aligned}\frac{\#\left\{(A,B) \in \mathcal{E}(X) \ : \ \substack{G \text{ acts nontrivially} \\ \text{on } \mathrm{Sel}_2(E_{A,B}/K)}\right\}}{\#\mathcal{E}(X)} &\leq \frac{\#\left\{(A,B) \in \mathcal{E}(X) \ : \ \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_{A,B}[2]) \neq 0\right\}}{\#\mathcal{E}(X)}, \\ &\leq \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_{A,B}[2])}{\#\mathcal{E}(X)}.\end{aligned}$$

Then by Theorem 6.5.4

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_{A,B}[2])}{\#\mathcal{E}(X)} \leq \left(\frac{27}{4}\right)^{5/6} \left(4 \prod_{\substack{v\in\Omega_{\mathbb{Q}} \\ v\nmid 6}} L_v(\mathscr{C}(K))\right).$$

The result then follows from looking at the definitions of the factors on the right hand side of this the fact that for sufficiently p, if $p \mid d$ then p is ramified and $L_p(\mathscr{C}(K)) \leq \frac{46}{48}$ and otherwise p is unramified and $L_p(\mathscr{C}(K)) \leq 1$. □

Studying the full 2-Selmer rank we obtain upper and lowed bounds.

Definition 6.5.10. Define the function

$$\mathrm{S}^+ : \{d \in \mathbb{Z} \ : \ d \text{ is squarefree}\} \to \mathbb{R}_{\geq 0},$$

by

$$\mathrm{S}^+(d) := \limsup_{X \to \infty} \frac{\sum\limits_{(A,B)\in\mathcal{E}} \dim \mathrm{Sel}_2(E_{A,B}/\mathbb{Q}(\sqrt{d}))}{\#\mathcal{E}(X)},$$

and similarly let $\mathrm{S}^-(d)$ be the liminf for the above ratio. If $\mathrm{S}^+(d) = \mathrm{S}^-(d)$ then we denote the resulting value by $\mathrm{S}(d)$.

Theorem 6.5.11. *Let d be a squarefree integer. Then*

$$\sum_{v\in\Omega_{\mathbb{Q}}} \mathcal{G}_K(v) \leq S^-(d) \leq S^+(d) \leq \sum_{v\in\Omega_{\mathbb{Q}}} \mathcal{G}_K(v) + \left(\frac{27}{4}\right)^{5/6} \left(8 \prod_{\substack{v\in\Omega_{\mathbb{Q}} \\ v\nmid 6}} L_v(\mathscr{C}(K)) \right),$$

where $\mathcal{G}_K$ is as in Definition 6.5.1, and $L_v(\mathscr{C}_K)$ is as in Definition 6.5.3. In particular, assuming that $S(d)$ exists then we would have

$$S(d) = \sum_{v\in\Omega_{\mathbb{Q}}} \mathcal{G}_K(v) + O\left(\left(\frac{46}{48}\right)^{\omega(d)} \right).$$

Proof. The first statement is an application of Lemma 2.3.11, Lemma 5.3.7 and Corollary 6.5.8. The second then follows from the first in the same way that Corollary 6.5.8 followed from Theorem 6.5.6. □

Chapter 7

Bhargavology & Multiquadratic Extensions

In this chapter, we prove the previously stated result Theorem 6.5.4, on the average size of the corestriction Selmer group in large families of elliptic curves $E/\mathbb{Q}$. The counting techniques used in this chapter are largely due to Bhargava and his collaborators, typically referred to as 'Bhargavology'.

In §7.1 and §7.2 we provide the necessary background on (principal) homogenous spaces for elliptic curves for relating Selmer elements to equivalence classes of binary quartic forms. This material is well known: the first section can be found in [Sil09, Chapter X], and the second begins historically with work of [BSD63] which has been substantially developed by Cremona and his collaborators (see e.g. [Cre97]).

In §2.3 we described the corestriction Selmer group as an intersection of Selmer groups of quadratic twists. Using this, in §7.3 we provide a description of the corestriction Selmer groups in terms of equivalence classes of binary quartic forms.

The counting begins in §7.4, which is a review section recalling necessary details from the influential work of Bhargava and Shankar [BS15a]. In §7.5 we define the notion of a 2-Selmer bundle, which, loosely speaking, assigns a Selmer structure to each elliptic curve $E/\mathbb{Q}$ in a large family in a continuous manner. We show that Bhargava and Shankar's counting techniques can be adapted to compute average sizes of Selmer groups arising from 2-Selmer bundles. In §7.6 we show that the corestriction Selmer structures form a 2-Selmer bundle, and so determine the average size of corestriction Selmer groups in 'large families' of elliptic curves in terms of a product of local densities. In §7.7 we explicitly determine these densities for the family of all elliptic curves, and in particular recover Theorem 6.5.4 as Corollary 7.7.15.

§ 7.1 | Principal Homogeneous Spaces and Selmer Elements

Throughout this section, unless we state further restrictions, K is assumed to be a field of characteristic 0.

§ 7.1.1 | Weil-Châtelet Groups

We recall some useful results which will enable us to interpret the description of corestriction Selmer groups in Proposition 2.3.9 in terms of equivalence classes of binary quartic forms. Later in the chapter we will axiomatise the work of Bhargava–Shankar to count these equivalence classes.

Definition 7.1.1. Let E/K be an elliptic curve. Then a (principal) homogeneous space for E/K is a pair (C, μ) where C/K is a smooth curve and

$$\mu : C \times E \to C$$

is a morphism over K satisfying

(1) for every point $q \in C$

$$\mu(q, O_E) = q,$$

where O_E here refers to the identity element on E;

(2) for every pair of points $P, Q \in E$, and each point $q \in C$, we have

$$\mu(\mu(q, P), Q) = \mu(q, P + Q);$$

(3) for every pair of points $q_0, q_1 \in C$ there is a unique $P \in E$ such that

$$\mu(q_0, P) = q_1.$$

Remark 7.1.2. In other words, a principal homogeneous space for E/K is an algebraic curve over K with a simply transitive (algebraic group) action of E.

Notation 7.1.3. If (C, μ) is a homogeneous space for E/K, then an interpretation of Definition 7.1.1 (3) is to think of the point $P \in E$ as the 'difference' between the points q and p. As such, we will take the notation $q -_\mu p$ for this unique P, or sometimes simply $q - p$ if μ is clear from context.

There is a natural notion of equivalence of such spaces.

Definition 7.1.4. Let E/K be an elliptic curve, and $(C, \mu), (C', \mu')$ be two homogeneous spaces. These two homogeneous spaces are said to be equivalent if there is an

isomorphism $\theta : C \to C'$ defined over K such that the diagram below commutes

$$\begin{array}{ccc} C \times E & \xrightarrow{\mu} & C \\ \downarrow{\scriptstyle \theta \times \mathrm{Id}} & & \downarrow{\scriptstyle \theta} \\ C' \times E & \xrightarrow{\mu'} & C', \end{array}$$

where Id is the identity map.

Remark 7.1.5. In other words, two homogeneous spaces are equivalent if there is an isomorphism over K between them which respects the action of E.

Definition 7.1.6. The collection of equivalence classes of homogeneous spaces for an elliptic curve E/K is called the Weil-Châtelet group for E/K and is denoted by $\mathrm{WC}(E/K)$. The equivalence class of the homogeneous space given by $(E, +)$ (that is, E acting on itself by translation) is called the trivial class.

Proposition 7.1.7 ([Sil09, Proposition 3.3])**.** *Let (C, μ) be a homogeneous space for an elliptic curve E/K. Then (C, μ) is in the trivial class in $\mathrm{WC}(E/K)$ if and only if $C(K) \neq \emptyset$.*

We now have a fundamental result about this group, which relates it to an interesting Galois cohomology group.

Theorem 7.1.8 ([Sil09, Theorem X.3.6 and Proposition X.3.3])**.** *Let E/K be an elliptic curve. There is a natural bijection of pointed sets*

$$\mathrm{WC}(E/K) \to H^1(K, E)$$

defined as follows.

Let (C, μ) be a homogeneous space for E/K, and let $q_0 \in C$ be a point. Then

$$\{(C, \mu)\} \mapsto \{\sigma \mapsto \sigma(q_0) -_\mu q_0\},$$

where the braces are to indicate that we map the equivalence class of (C, μ) to the cohomology class of the cocycle on the right.

Remark 7.1.9. It is clear from the definition of the bijection above that the trivial class in $\mathrm{WC}(E/K)$ maps to the identity element of the group $H^1(K, E)$ (simply choose the marked rational point $q_0 = O_E \in E(K)$).

§ 7.1.2 | n-coverings

We now recall the description of $H^1(K, E[n])$ for each integer $n \geq 2$ in terms of so-called n-coverings. This can be found, for example, in [Sto06, §1.2, First interpretation].

Definition 7.1.10. Let $n \geq 2$ be an integer and E/K be an elliptic curve. Then an n-covering of E/K is a pair (C, π) where C/K is a smooth curve and $\pi : C \to E$ is

a morphism defined over K such that there exists an isomorphism $\theta : C \to E$ defined over the algebraic closure $\overline{K}$ making the diagram below commute.

$$\begin{array}{ccc} C & \xrightarrow{\pi} & E \\ \vdots{\scriptstyle\theta} & & \downarrow{\scriptstyle \mathrm{Id}} \\ E & \xrightarrow{\times n} & E. \end{array} \tag{7.1}$$

Two n-coverings $(C, \pi), (C', \pi')$ are said to be equivalent if there is an isomorphism defined over K, $\phi : C \to C'$, such that the diagram below commutes.

$$\begin{array}{ccc} C & \xrightarrow{\pi} & E \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle \mathrm{Id}} \\ C' & \xrightarrow{\pi'} & E. \end{array}$$

An n-covering is said to be trivial if it is equivalent to the n-covering given by E itself equipped with multiplication by n, $(E, \times n)$.

Theorem 7.1.11 (see, e.g., [Sto06, Proposition 1.3 and proof])**.** *Let $n \geq 2$ be an integer and E/K be an elliptic curve. Then there is a natural bijection of pointed sets*

$$\left\{\begin{smallmatrix}\text{equivalence classes of} \\ n\text{-coverings of } E/K\end{smallmatrix}\right\} \to H^1(K, E[n])$$

defined as follows.

Let (C, π) be an n-covering of E/K, let $\theta : C \to E$ be an isomorphism over $\overline{K}$ such that the diagram (7.1) commutes, and let $P_0 \in E$ be a point over $\overline{K}$. Then

$$\{(C, \pi)\} \mapsto \left\{\sigma \mapsto \sigma \circ \theta \circ \sigma^{-1} \circ \theta^{-1}(P_0) - P_0\right\},$$

where the braces are to indicate that we map the equivalence class of (C, π) to the cohomology class of the cocycle on the right.

Remark 7.1.12. It is easy to see that the trivial class on the left maps to the identity element on the right: choose $C = E$, $\pi = \times n$ and $\theta = \mathrm{Id}$.

These geometric interpretations for the Galois cohomology groups $H^1(K, E[n])$ and $H^1(K, E)$ as equivalence classes of n-coverings and of principal homogeneous spaces are compatible in a natural way.

Theorem 7.1.13 ([Sto06, §1.2 First interpretation])**.** *The diagram (of pointed sets) below commutes:*

$$\begin{array}{ccc} H^1(K, E[n]) & \longrightarrow & H^1(K, E) \\ {\scriptstyle\text{Theorem 7.1.11}}\uparrow & & \uparrow{\scriptstyle\text{Theorem 7.1.8}} \\ \left\{\begin{smallmatrix}\text{equivalence classes of} \\ n\text{-coverings of } E/K\end{smallmatrix}\right\} & \longrightarrow & \mathrm{WC}(E/K), \end{array} \tag{7.2}$$

where the vertical maps are the bijections described in the referenced theorem, the top horizontal is induced by the natural inclusion $E[n] \subseteq E$ and the lower horizontal is

constructed as follows. Let (C, π) be an n-covering of E/K, let $\theta : C \to E$ be an isomorphism over $\overline{K}$ such that the diagram (7.1) commutes, then

$$\{(C, \pi)\} \mapsto \{(C, \mu)\}$$

where for $P \in E$ and $q \in C$, we define $\mu(q, P) := \theta^{-1}(\theta(q) + P)$. The braces are to indicate that the map sends the equivalence class of the n-covering (C, π) to the equivalence class of the homogeneous space (C, μ) defined above.

From this there is then an obvious corollary.

Corollary 7.1.14. *Consider the inclusion $\delta : E(K)/nE(K) \to H^1(K, E[n])$, induced by the multiplication by n exact sequence for E. Then the correspondence of Theorem 7.1.11 identifies the image of δ with the set of equivalence classes of n-coverings (C, π) of E/K such that $C(K) \neq \emptyset$.*

In particular, we have a commutative diagram (of pointed sets) with all of the vertical maps being bijective:

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)/nE(K) & \longrightarrow & H^1(K, E[n]) & \longrightarrow & H^1(K, E) \\ & & \downarrow & & \downarrow{\scriptstyle \text{Thm. 7.1.11}} & & \downarrow{\scriptstyle \text{Thm. 7.1.8}} \\ & & \left\{ \begin{array}{c} \text{equivalence clases of} \\ n\text{-coverings } (C,\pi) \text{ of} \\ E/K \text{ such that } C(K) \neq \emptyset \end{array} \right\} & \hookrightarrow & \left\{ \begin{array}{c} \text{equivalence classes of} \\ n\text{-coverings of } E/K \end{array} \right\} & \xrightarrow[\text{Thm. 7.1.13}]{} & Ш C(E/K) \end{array}$$

Remark 7.1.15. This tells us a lot about n-Selmer elements. Recall that if K is a number field and E/K is an elliptic curve then $\mathrm{Sel}_n(E/K) := \ker(\alpha)$ where α is the diagonal map below.

$$\begin{array}{ccc} H^1(K, E[n]) & \longrightarrow & H^1(K, E) \\ \downarrow & \overset{\alpha}{\searrow} & \downarrow \\ \prod\limits_{v \in \Omega_K} H^1(K_v, E[n]) & \longrightarrow & \prod\limits_{v \in \Omega_K} H^1(K_v, E). \end{array}$$

That is to say, in the language of n-coverings above and using Proposition 7.1.7, the elements of $\mathrm{Sel}_n(E/K)$ are identified with the equivalence classes of n-coverings (C, π) of E/K such that for every place $v \in \Omega_K$, $C(K_v) \neq \emptyset$. Moreover, the inclusion $E(K)/nE(K) \to \mathrm{Sel}_n(E/K)$ identifies this quotient of the Mordell–Weil group with the subset of equivalence classes of n-coverings (C, π) which not only possess points everywhere locally but actually possess a global point, i.e. $C(K) \neq \emptyset$.

§ 7.2 | Binary Quartic Forms

We now discuss the explicit correspondence between 2-Selmer elements and certain equivalence classes of binary quartic forms. This is an explicit version of the correspondence to 2-coverings in §7.1. The original correspondence with binary quartic forms was given some time ago by Birch and Swinnerton-Dyer [BSD63] and has been developed

substantially by Cremona and his collaborators [Cre97] (see also [Cre99, CF09, SC02]).

§ 7.2.1 | Basic Objects

Recall that a binary quartic form over a ring R is a degree 4 homogeneous polynomial in two variables with coefficients in R.

Notation 7.2.1. For each ring R we define V_R to be the set of binary quartic forms with coefficients in R. Moreover, for $i = 0, 1, 2$ denote by $V_{\mathbb{R}}^{(i)}$ to be the subset of binary quartic forms in $V_{\mathbb{R}}$ with nonzero discriminant having i pairs of complex roots in $\mathbb{P}^1_{\mathbb{C}}$ and $4 - 2i$ real roots in $\mathbb{P}^1_{\mathbb{C}}$. The set of definite quartic forms, those which take only positive or only negative values when evaluated at nonzero elements $(x_0, y_0) \in \mathbb{R}^2$, is $V_{\mathbb{R}}^{(2)}$. We denote the subset of positive (resp. negative) definite forms by $V_{\mathbb{R}}^{(2+)}$ (resp. $V_{\mathbb{R}}^{(2-)}$). We write $V_{\mathbb{Z}}^{(i)} := V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$.

Definition 7.2.2. Let K be a field and $g(x, y) \in V_K$ be a binary quartic form. Then we say that f is K-soluble if there are $x, y, z \in K$ with $(x, y) \neq (0, 0)$ such that

$$z^2 = g(x, y).$$

We say that $g \in V_{\mathbb{Q}}$ is locally soluble if g is $\mathbb{Q}_v$-soluble for every place v of $\mathbb{Q}$.

For every ring R there is a well defined (twisted) action of $\mathrm{GL}_2(R)$ on V_R, given for each $g \in V_R$ and $\gamma \in \mathrm{GL}_2(R)$ by

$$\gamma \cdot g(x, y) = \det(\gamma)^{-2} g((x, y) \cdot \gamma^t),$$

where the action of γ on (x, y) on the right hand side is just the standard matrix operation on a row vector, and γ^t is the transpose matrix. Moreover, the centre of $\mathrm{GL}_2(R)$ acts trivially, and so this descends to an action of $\mathrm{PGL}_2(R)$.

Associated to $g(x, y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4 \in V_R$ there are then two invariants of this action, $I(g)$ and $J(g)$, given by

$$\begin{aligned} I(g) &= 12ae - 3bd + c^2, \\ J(g) &= 72ace + 9bcd - 27ad^2 - 27eb^2 - 2c^3. \end{aligned}$$

There are also the covariants $g_4(g; X, Y), g_6(g; X, Y) \in R[X, Y]$, given by

$$\begin{aligned} g_4(g; X, Y) &= (3b^2 - 8ac)X^4 + 4(bc - 6ad)X^3Y + 2(2c^2 - 24ae - 3bd)X^2Y^2 \\ &\quad +4(cd - 6be)XY^3 + (3d^2 - 8ce)Y^4, \\ g_6(g; X, Y) &= b^3 + 8a^2d - 4abc)X^6 + 2(16a^2e + 2abd - 4ac^2 + b^2c)X^5Y \\ &\quad +5(8abe + b^2d - 4acd)X^4Y^2 + 20(b^2e - ad^2)X^3Y^3 \\ &\quad -5(8ade + bd^2 - 4bce)X^2Y^4 - 2(16ae^2 + 2bde - 4c^2e + cd^2)XY^5 \\ &\quad -(d^3 + 8be^2 - 4cde)Y^6. \end{aligned}$$

§ 7.2.2 | Correspondence

We now relate binary quartic forms to homogeneous spaces and 2-coverings. We note the parts of use to us as one large theorem, to gather everything in one place for use later in the thesis. The theorem summarises [CF09, §6], though the reader should note that we consider the elliptic curve $E : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$, whereas the authors in loc. cit. consider the model (for the same curve) $y^2 = x^3 - 27Ix - 27J$, and so there is a change of variables applied between their results and what is stated below.

Theorem 7.2.3 ([CF09, §6])**.** *Given the data of a pair, (E, F) where F is a characteristic 0 field, and E/F is an elliptic curve with specified Weierstrass equation*

$$E : y^2 = x^3 - \tfrac{I}{3}x - \tfrac{J}{27},$$

the following is true.

Let $\overline{L} := \overline{F} \times \overline{F} \times \overline{F}$, let $f(X) := X^3 - 3IX + J$, and consider the étale algebra $L = L(E) := F[\varepsilon]/\langle f(\varepsilon)\rangle$. Fix $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \overline{F}$ to be the three roots of $f(X)$ and so fix the embedding $L \subseteq \overline{L}$ induced by mapping $\varepsilon \mapsto (\varepsilon_1, \varepsilon_2, \varepsilon_3)$. Under this embedding, we define the norm of an element $w = (w_1, w_2, w_3) \in L \subseteq \overline{L}$ to be $N_{L/F}w := w_1w_2w_3 \in F$.

Then there is a commutative diagram (of groups)

$$\begin{array}{ccc} E(F)/2E(F) & \xrightarrow{\quad\delta\quad} & H^1(F, E[2]) \\ \downarrow{\scriptstyle q} & \overset{\delta'}{\nearrow} & \downarrow{\scriptstyle \alpha} \\ \left\{\begin{array}{c}\mathrm{PGL}_2(F)\text{-equivalence classes of} \\ \text{binary quartic forms } g \in V_F \\ \text{with } (I(g),J(g))=(I,J)\end{array}\right\} & \xrightarrow{\quad z\quad} & \ker\left(N_{L/F} : L^\times/L^{\times 2} \to F^\times/F^{\times 2}\right) \end{array} \tag{7.3}$$

where the definitions and properties of the maps are as follows:

- *The map δ is an injection. It is the usual connecting map arising from taking Galois cohomology on the multiplication by 2 short exact sequence for E.*
- *The map q is injective, and its image is the collection of cosets represented by F-soluble binary quartic forms. For $P = (\xi, \eta) \in E(F)$ we define*

$$q(P) := \left\{X^4 - \frac{3}{2}\xi X^2Y^2 - \eta XY^3 + (\tfrac{I}{12} - \tfrac{3\xi^2}{4})Y^4\right\}$$

  where the braces denote that we map to the $\mathrm{PGL}_2(F)$-equivalence class of the stated binary quartic form.

- *The map α is an isomorphism. This map is constructed as follows (see* [Sch95, Theorem 1.1]*): consider the map*

$$\begin{aligned} w : E[2] &\to \mu_2(\overline{L}) \\ P &\mapsto (e_2(P, (\varepsilon_1, 0)),\ e_2(P, (\varepsilon_2, 0)),\ e_2(P, (\varepsilon_3, 0))) \end{aligned}$$

where e_2 denotes the Weil Pairing. This induces a map

$$w^* : H^1(F, E[2]) \to H^1(F, \mu_2(\overline{L})).$$

Additionally we have the Kummer isomorphism (see [Ser79, p.152, Ex.2]*)*

$$\kappa : H^1(F, \mu_2(\overline{L})) \cong L^\times / L^{\times 2}.$$

Then $\alpha := \kappa \circ w^*$.

- *The map z called the cubic invariant, and is injective. It is constructed as follows. For a binary quartic form g representing an element of the domain, define the 'irrational covariant' to be*

$$G(X, Y) := \frac{1}{3}\left(4\varepsilon g(X, Y) + g_4(g; X, Y)\right) \in L[X, Y].$$

Choose $(x, y) \in F \times F$ such that $G(x, y) \in L^\times$ (such a pair exists by [CF09, §2 Paragraph 2]*), and define*

$$z(g) := G(x, y) \in L^\times / L^{\times 2}.$$

This map is independent of the choice of (x, y) by [CF09, Proposition 2]*, and $z(g)$ has square norm by* [CF09, Lemma 1]*.*

- *The map δ' is injective, and is constructed as follows. Let $g(X, Y)$ be a representative of an equivalence class in the domain. Then let C be the smooth projective curve with affine equation $Z^2 = g(X, 1)$, and define the map*

$$\begin{aligned} \pi : C &\to E \\ (x, z) &\mapsto \left(\frac{g_4(g; x, 1)}{12z^2}, \frac{g_6(g; x, 1)}{8z^3}\right). \end{aligned}$$

The pair (C, π) is in fact a 2-covering of E (see [CF09, §6 p11 Remarks (3)] *and references therein). The map δ' sends the equivalence class of g to the equivalence class of the 2-covering (C, π) and then maps this to a cocycle class via the correspondence of Theorem 7.1.11.*

From this we state a shorter helpful corollary, which is at the core of the work of Bhargava and Shankar on 2-Selmer groups [BS15a, see e.g. §3.1].

Corollary 7.2.4 (See also [BS15a, Theorem 3.2] and references therein)**.** *Let F be a characteristic 0 field, and E/F be an elliptic curve with specified Weierstrass equation*

$$E : y^2 = x^3 - \tfrac{I}{3}x - \tfrac{J}{27}.$$

Using the notation of Theorem 7.2.3 for the data (E, F) above, the map q is a bijection between $\mathrm{PGL}_2(F)$-orbits of F-soluble binary quartic forms with invariants I, J

and elements of $E(F)/2E(F)$. Under this bijection, the identity element corresponds to the (unique!) $\mathrm{PGL}_2(F)$*-orbit of binary quartic forms possessing a linear factor over F.*

Furthermore, the stabiliser in $\mathrm{PGL}_2(F)$ *of any (not necessarily F-soluble) binary quartic form $g \in V_F$ with invariants $(I, J) = (I(g), J(g))$ such that $4I^3 - J^2 \neq 0$ is isomorphic to $E(F)[2]$ where E is the elliptic curve defined by $y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$.*

§ 7.2.3 | Elliptic Curves Over $\mathbb{Q}$

At this point we restrict to our case of interest, which here is $F = \mathbb{Q}$. We begin with a useful bookkeeping definition.

Definition 7.2.5 ([BS15a, §3])**.** Let $E/\mathbb{Q}$ be an elliptic curve, and let $(A, B) \in \mathcal{E}$ be the unique pair such that

$$E \cong E_{A,B} : y^2 = x^3 + Ax + B. \tag{7.4}$$

Then we define the quantities

$$I(E) := -3A$$
$$J(E) := -27B$$

Moreover, for $(I, J) = (I(E), J(E))$ we will use the notation $E^{I,J} : y^2 = x^3 - \frac{I}{3}x - \frac{J}{27}$ in order to pass back from the invariants $I(E), J(E)$ to a model for the curve E.

We then have the following proposition, which is well known and follows from [BSD63, Lemma 2] (see also [Cre97]).

Proposition 7.2.6 (see also [BS15a, Proposition 3.3])**.** *Let $E/\mathbb{Q}$ be an elliptic curve, with specified Weierstrass equation*

$$E : y^2 = x^3 - \tfrac{I}{3}x - \tfrac{J}{27}.$$

Then using the notation of Theorem 7.2.3 for the data $(E, \mathbb{Q})$: the map δ' is a bijection between the set of $\mathrm{PGL}_2(\mathbb{Q})$*-orbits of locally soluble binary quartic forms $g \in V_{\mathbb{Q}}$ with $(I(g), J(g)) = (I, J)$ and the 2-Selmer group* $\mathrm{Sel}_2(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[2])$.

Furthermore, the set of binary quartic forms $g \in V_{\mathbb{Q}}$ having a linear factor (over $\mathbb{Q}$) and invariants (I, J) lie in a single $\mathrm{PGL}_2(\mathbb{Q})$*-orbit, and this orbit maps to the identity element of* $\mathrm{Sel}_2(E/\mathbb{Q})$.

Proof. By [BSD63, Lemma 2] we know that the 2-coverings corresponding to Selmer elements are in the image of δ'. It is then clear from construction that the local restriction map for each $v \in \Omega_{\mathbb{Q}}$, $H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}_v, E[2])$, sends a 2-covering (C, π) to (C, π) considered now over $\mathbb{Q}_v$. By definition 2-Selmer elements thus correspond to the elements (C, π) in the image of δ' such that $C(\mathbb{Q}_v) \neq \emptyset$ for every $v \in \Omega_{\mathbb{Q}}$, which is equivalent to the local solubility of the binary quartic form mapping to C. □

In order to reduce to counting lattice points, we have the following lemma which follows from [BSD63, Lemmas 3,4,5] and shows that we can always find an integral representative (i.e. $g \in V_{\mathbb{Z}} \subset V_{\mathbb{Q}}$) in the $\mathrm{PGL}_2(\mathbb{Q})$-orbit of a locally soluble binary quartic form.

Lemma 7.2.7 ([BSD63, Lemmas 3,4,5], see also [BS15a, Lemma 3.4])**.** *Let $g \in V_{\mathbb{Q}}$ be a locally soluble binary quartic form having integer invariants $(I, J) := (I(g), J(g))$ such that $(2^4 \cdot 3) \mid I$ and $(2^6 \cdot 3^3) \mid J$. Then g is $\mathrm{PGL}_2(\mathbb{Q})$-equivalent to an element of $V_{\mathbb{Z}}$.*

Since each elliptic curve $E/\mathbb{Q}$ is isomorphic to the elliptic curve defined by the equation $y^2 = x^3 - \frac{2^4 I(E)}{3}x - \frac{2^6 J(E)}{27}$, Lemma 7.2.7 and Proposition 7.2.6 imply the following key theorem.

Theorem 7.2.8 (see also [BS15a, Theorem 3.5])**.** *Let $(A, B) \in \mathcal{E}$, and specify the Weierstrass equation for $E = E_{A,B}$ to be*

$$E : y^2 = x^3 + 2^4 Ax + 2^6 B.$$

Then using the notation of Theorem 7.2.3 for the data $(E, \mathbb{Q})$: the map δ' induces a bijection between $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of locally soluble binary quartic forms $g \in V_{\mathbb{Z}}$ with invariants $(I(g), J(g)) = (2^4 I(E), 2^6 J(E))$ and the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q})$.

Furthermore, the set of $g \in V_{\mathbb{Z}}$ having a linear factor (over $\mathbb{Q}$) and invariants $(2^4 I(E), 2^6 J(E))$ lie in a single $\mathrm{PGL}_2(\mathbb{Q})$-orbit, and this orbit maps to the identity element of $\mathrm{Sel}_2(E/\mathbb{Q})$.

§ 7.3 | Binary Quartic Forms & the Corestriction Selmer Group

We now improve Corollary 7.2.4 (in the case that F is a local field) to determine which locally soluble binary quartic forms correspond to elements of the local groups in the corestriction Selmer structure. We will then improve Theorem 7.2.8, to also describe the corestriction Selmer group in terms of binary quartic forms. We will make fundamental use of Proposition 2.3.9, and the results in the previous section.

Definition 7.3.1. Let F be a characteristic 0 field, and $S \leq F^\times/F^{\times 2}$ be a finite subgroup. Then we say that a binary quartic form $g(X, Y) \in V_F$ is (F, S)-soluble if for each $\theta \in S$ there exist $x, y, z \in F$ with $(x, y) \neq (0, 0)$ such that

$$z^2 = \theta g(x, y).$$

Moreover, we say that $g \in V_{\mathbb{Q}}$ is locally S-soluble if for every place $v \in \Omega_{\mathbb{Q}}$, g is $(\mathbb{Q}_v, S)$-soluble (S here being interpreted as its image in $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$).

Remark 7.3.2. This is clearly well defined, since altering θ by a square scales the chosen z-coordinate. Further note that being $(F, \langle 1 \rangle)$-soluble is the same as being F-soluble, and in fact being (F, S)-soluble always requires at least being F-soluble.

Before we can describe image of (F, S)-soluble binary quartic forms under the correspondence of Corollary 7.2.4, we will require a helpful lemma.

Theorem 7.3.3. *Let F be a characteristic 0 field, and let E/F be an elliptic curve with fixed Weierstrass equation $E : y^2 = x^3 + \frac{I}{3}x - \frac{J}{27}$. Let $\theta \in F^\times$ be nonsquare, and fix the following model for the quadratic twist E_θ*

$$E_\theta : y^2 = x^3 - \frac{\theta^2 I}{3}x - \frac{\theta^3 J}{27}.$$

Write $\varphi_\theta : E_\theta \to E$ for the isomorphism (over $F(\sqrt{\theta})$) given by $(x, y) \mapsto (\frac{y}{\theta\sqrt{\theta}}, \frac{x}{\theta})$. This map restricts to an isomorphism (over F) $E_\theta[2] \to E[2]$, and the diagram below commutes:

$$\begin{array}{ccc} H^1(F, E_\theta[2]) & \xrightarrow{\quad\varphi_\theta^*\quad} & H^1(F, E[2]) \\ \uparrow{\scriptstyle \delta'} & & \uparrow{\scriptstyle \delta'} \\ \left\{\begin{array}{c}\text{PGL}_2(F)\text{-equivalence classes of} \\ \text{binary quartic forms } g \in V_F \\ \text{with } (I(g), J(g)) = (\theta^2 I, \theta^3 J)\end{array}\right\} & \xrightarrow{\phi_\theta} & \left\{\begin{array}{c}\text{PGL}_2(F)\text{-equivalence classes of} \\ \text{binary quartic forms } g \in V_F \\ \text{with } (I(g), J(g)) = (I, J)\end{array}\right\}, \end{array}$$

where the vertical maps are those described in Theorem 7.2.3 for the data (E_θ, F) and (E, F) respectively. The map ϕ_θ is given by sending the equivalence class of a binary quartic form g to that of $\theta^{-1}g$.

Proof. Note firstly that the new map ϕ_θ is well defined: scalar multiplication commutes with the action of $\text{PGL}_2(F)$ on the forms, and the claimed invariants in the image are correct as $I(g)$ and $J(g)$ are homogeneous of degree 2 and 3 in the coefficients of the associated form g.

Write $L := L(E) = F[\varepsilon]/\varepsilon^3 - 3I\varepsilon + J$ and $L_\theta := L(E_\theta) = F[\varepsilon]/\varepsilon^3 - 3\theta^2 I\varepsilon + \theta^3 J$ for the étale algebras associated to the data of (E, F) and (E_θ, F) by Theorem 7.1.11. Moreover, let us write

$$\begin{aligned} \beta : L_\theta &\to L \\ \varepsilon &\mapsto \theta\varepsilon. \end{aligned}$$

We begin by noting that the following diagram commutes:

$$\begin{array}{ccc} L_\theta & \xrightarrow{\beta} & L \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ \overline{L} & = & \overline{L} \end{array} \tag{7.5}$$

where κ are the Kummer maps induced by the inclusions $L, L_\theta \subset \overline{L}$ fixed in Theorem 7.2.3. Then, since the Weil pairing is preserved by the isomorphism φ_θ, it is

then clear from the definition of the maps α of Theorem 7.2.3 that the diagram below commutes:

$$\begin{array}{ccc} H^1(F, E_\theta[2]) & \xrightarrow{\qquad\varphi_\theta^*\qquad} & H^1(F, E[2]) \\ \downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha} \\ \ker(N_{L_\theta/F} : L_\theta^\times/L_\theta^{\times 2} \to K^\times/K^{\times 2}) & \xrightarrow{\beta} & \ker(N_{L/F} : L^\times/L^{\times 2} \to K^\times/K^{\times 2}), \end{array}$$

where the vertical maps are those described in Theorem 7.2.3 for the data (E_θ, F) and (E, F) respectively.

Using the commutativity of the diagram in Theorem 7.2.3 for the data (E, F) and (E_θ, F), and that the α-maps are injective, we then see that the claim that $\delta' \circ \phi_\theta = \varphi_\theta^* \circ \delta'$ holds if and only if the diagram below commutes:

$$\begin{array}{ccc} \ker(N_{L_\theta/F} : L_\theta^\times/L_\theta^{\times 2} \to K^\times/K^{\times 2}) & \xrightarrow{\beta} & \ker(N_{L/F} : L^\times/L^{\times 2} \to K^\times/K^{\times 2}) \\ \uparrow{\scriptstyle z} & & \uparrow{\scriptstyle z} \\ \left\{\begin{smallmatrix}\mathrm{PGL}_2(F)\text{-equivalence classes of} \\ \text{binary quartic forms } g \in V_F \\ \text{with } (I(g), J(g)) = (\theta^2 I, \theta^3 J)\end{smallmatrix}\right\} & \xrightarrow{\phi_\theta} & \left\{\begin{smallmatrix}\mathrm{PGL}_2(F)\text{-equivalence classes of} \\ \text{binary quartic forms } g \in V_F \\ \text{with } (I(g), J(g)) = (I, J)\end{smallmatrix}\right\}, \end{array}$$

but this follows from the definition of the maps z: if g is a binary quartic form with invariants $(\theta^2 I, \theta^3 J)$ then (for an appropriate choice of $(x, y) \in F \times F$)

$$\begin{aligned} \beta \circ z(g) &= \beta\left(\frac{1}{3}(4\varepsilon g(x, y) + g_4(g; x, y))\right) \\ &= \frac{1}{3}(4\theta\varepsilon g(x, y) + g_4(g; x, y)) \\ &\equiv \frac{1}{3}(4\theta^{-1}\varepsilon g(x, y) + \theta^{-2} g_4(g; x, y)) \\ &= \frac{1}{3}(4\varepsilon\theta^{-1} g(x, y) + g_4(\theta^{-1} g; x, y)) \\ &= z \circ \phi_\theta(g) \end{aligned}$$

□

Using Theorem 7.3.3 we are then able to describe the local groups of the corestriction Selmer structure in terms of the correspondence to binary quartic forms from Corollary 7.2.4.

Corollary 7.3.4. *Let F be a number field, and K/F be a Galois extension. Let $v \in \Omega_F$, assume that $w \in \Omega_K$ is a place extending v such that K_w/F_v is multiquadratic, and write $S := \ker(F_v^\times/F_v^{\times 2} \to K_w^\times/K_w^{\times 2})$. Let E/F_v be an elliptic curve, with specified Weierstrass equation*

$$E : y^2 = x^3 - \tfrac{I}{3}x - \tfrac{J}{27}.$$

Using the notation of Theorem 7.2.3 for the data (E, F_v) above, the map δ' restricts to a bijection between $\mathrm{PGL}_2(F)$-orbits of (F, S)-soluble binary quartic forms with invariants I, J and elements of $\mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K; E))$. Under this bijection, the identity

element corresponds to the (unique!) $\mathrm{PGL}_2(F)$*-orbit of binary quartic forms possessing a linear factor over* F*.*

Equivalently: q *is a bijection between* $\mathrm{PGL}_2(F)$*-orbits of* (F,S)*-soluble binary quartic forms with invariants* I, J *and elements of* $(N_{K_w/F_v}E(K) + 2E(F))/2E(F)$*, with the same stipulations about the quartic forms corresponding to the identity element.*

Proof. By Proposition 2.3.8, we know that

$$\mathrm{cor}_{K_w/F_v}(\mathscr{S}_w(K;E)) = \bigcap_{\theta\in S} \mathscr{S}_v^{(\theta)}(F;E).$$

By Theorem 7.3.3 and Corollary 7.2.4 $\mathscr{S}_v^{(\theta)}(F;E)$ corresponds through δ' to the equivalence classes of binary quartic forms $g \in V_F$ with invariants I, J such that θg is F-soluble. Thus the intersection corresponds precisely to the equivalence classes of (F,S)-soluble binary quartic forms. That the second statement is equivalent is clear from Theorem 7.2.3. □

We can now strengthen Theorem 7.2.8 to identify the corestriction Selmer group as a subset of the equivalence classes of locally soluble binary quartic forms.

Theorem 7.3.5. *Let* $K/\mathbb{Q}$ *be a multiquadratic extension, and* $S := \ker(\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to K^\times/K^{\times 2})$*. Let* $(A,B) \in \mathcal{E}$*, and specify the Weierstrass equation for* $E = E_{A,B}$ *to be*

$$E : y^2 = x^3 + 2^4Ax + 2^6B.$$

Then using the notation of Theorem 7.2.3 for the data $(E,\mathbb{Q})$*: the map* δ' *induces a bijection between* $\mathrm{PGL}_2(\mathbb{Q})$*-equivalence classes of locally* S*-soluble binary quartic forms* $g \in V_\mathbb{Z}$ *with invariants* $(I(g),J(g)) = (2^4I(E), 2^6J(E))$ *and the corestriction Selmer group* $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q},E[2]) \subseteq H^1(\mathbb{Q},E[2])$*.*

Furthermore, the set of $g \in V_\mathbb{Z}$ *having a linear factor (over* $\mathbb{Q}$*) and invariants* $(2^4I(E), 2^6J(E))$ *lie in a single* $\mathrm{PGL}_2(\mathbb{Q})$*-orbit, and this orbit maps to the identity element of* $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q},E[2])$*.*

Proof. To ease discussion below, for each $v \in \Omega_\mathbb{Q}$ let δ'_v be the map from Theorem 7.2.3 with the data $(E,\mathbb{Q}_v)$. Moreover write S_v for the image of S in $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$.

Let A be the set of $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of locally soluble binary quartic forms $g \in V_\mathbb{Z}$ having invariants $(I(g),J(g)) = (2^4I, 2^6J)$ such that: for every $v \in \Omega_\mathbb{Q}$, the map δ'_v maps the equivalence class of g to an element of $\mathscr{C}_v(K/\mathbb{Q};E)$. By Corollary 7.3.4, $\mathscr{C}_v(K/\mathbb{Q};E)$ corresponds under the δ' to the set of equivalence classes of $(\mathbb{Q}_v,S_v)$-soluble binary quartic forms $g \in V_{\mathbb{Q}_v}$ with invariants $(2^4I, 2^6J)$.

Now by the definition of the corestriction Selmer structure, and Theorem 7.2.8, δ' induces a bijection between $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q},E[2]) \subseteq \mathrm{Sel}_2(E/\mathbb{Q})$ and the set A, as required. □

Theorem 7.3.5 tells us which $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of integral binary quartic forms $g \in V_{\mathbb{Z}}$ to count in order to determine the average of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E_{A,B}[2])$ as $(A, B) \in \mathcal{E}$ varies.

§ 7.4 | Recalling Bhargava–Shankar

For each multiquadratic extension $K/\mathbb{Q}$, we wish to understand $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ as $E \in \mathcal{E}$ varies. By construction this is a subgroup of $\mathrm{Sel}_2(E/\mathbb{Q})$, the object studied by Bhargava and Shankar in [BS15a] when they obtained the first bounds on average ranks of elliptic curves. This section is a brief summary of the necessary parts of their work, which we will use in what follows. Everything will be written in the generality of 'large families', as is done in their work, though our main interest will be the family of elliptic curves parametrised by $\mathcal{E}$.

§ 7.4.1 | Elliptic Curves and Families

Firstly, we have the invariants corresponding to each elliptic curve.

Definition 7.4.1 ([BS15a, §3])**.** For each pair $(I, J) \in \mathbb{R}^2$ we define the height to be

$$H(I, J) := \max\left\{|I|^3, J^2/4\right\}.$$

For an elliptic curve $E/\mathbb{Q}$, with associated invariants $I := I(E)$ and $J := J(E)$ (see Definition 7.2.5), we define the height of E to be

$$H'(E) := H(I, J).$$

The discriminant of the pair (I, J) is defined to be

$$\Delta'(I, J) := \frac{4I^3 - J^2}{27}$$

Example 7.4.2. *In the language of the previous chapter, for* $\mathbf{C} = (\frac{1}{3}, \frac{2}{27})$ *and* $X > 0$

$$\left\{E_{A,B} \ : \ (A, B) \in \mathcal{E}^{\mathbf{C}}(X)\right\} = \left\{E/\mathbb{Q} \ : \ H'(E) \leq X\right\}.$$

Remark 7.4.3. Note that if we present $E = E_{A,B}$ for $(A, B) \in \mathcal{E}$ then it is easy to see that the notion of height introduced above differs from the naive height by a constant factor:

$$H'(E) = \max\left\{|-3A|^3, (-27B)^2\right\} = \frac{27}{4}\max\left\{4\,|A|^3, 27B^2\right\},$$

so the ordering on elliptic curves is equivalent to that of the naive height. Moreover,

$$\Delta'(I, J) = -(4A^3 + 27B^2) = -\Delta(A, B)$$

recovers the discriminant of the given model of E.

We now introduce the 'large families' of elliptic curves to which the results of [BS15a] apply.

Definition 7.4.4 ([BS15a, §3])**.** For each prime p, let

$$\Sigma_p \subset \left\{(I,J) \in \mathbb{Z}_p^2 \ : \ \Delta'(I,J) \neq 0\right\}$$

be a nonempty closed subset with boundary of measure 0. Moreover let Σ_∞ be one of the following:

$$\left\{(I,J) \in \mathbb{R}^2 \ : \ \Delta'(I,J) < 0\right\}, \ \left\{(I,J) \in \mathbb{R}^2 \ : \ \Delta'(I,J) > 0\right\},$$
$$\left\{(I,J) \in \mathbb{R}^2 \ : \ \Delta'(I,J) \neq 0\right\}.$$

Associated to the data $\Sigma = (\Sigma_v)_{v \in \Omega_\mathbb{Q}}$, we have a family of elliptic curves over $\mathbb{Q}$,

$$\mathcal{F}_\Sigma := \left\{E/\mathbb{Q} \ : \ (I(E),J(E)) \in \Sigma_v \quad \forall v \in \Omega_\mathbb{Q}\right\}.$$

A family of elliptic curves $\mathcal{F}$ is said to be defined by congruence conditions if $\mathcal{F} = \mathcal{F}_\Sigma$ for some $\Sigma = (\Sigma_v)_{v \in \Omega_\mathbb{Q}}$ as above.

Associated to a family of curves which is defined by congruence conditions, we have some additional data.

Notation 7.4.5. Let $\mathcal{F} = \mathcal{F}_\Sigma$ be a family of elliptic curves defined by congruence conditions. Then we have

- $\mathrm{Inv}(\mathcal{F}) := \{(I(E),J(E)) \ : \ E \in \mathcal{F}\}$.
- For each prime number p, $\mathrm{Inv}_p(\mathcal{F})$ is the set of (I,J) in the p-adic closure of $\mathrm{Inv}(\mathcal{F})$ in $\mathbb{Z}_p^2$ for which $\Delta'(I,J) \neq 0$.
- $\mathrm{Inv}_\infty(\mathcal{F}) := \Sigma_\infty$.

Remark 7.4.6. It is not, in this generality, true that $\mathrm{Inv}_p(\mathcal{F}_\Sigma) = \Sigma_p$. Take, for instance,

$$\Sigma_p = \left\{(I,J) \in \mathbb{Z}_p^2 \ : \ I \equiv J \equiv 0 \mod p \text{ and } \Delta'(I,J) \neq 0\right\}$$

for every prime number p. Then of course $\mathcal{F}_\Sigma = \emptyset$, so $\mathrm{Inv}_p(\mathcal{F}_\Sigma) = \emptyset$.

The families that can be studied with the analytic tools of [BS15a] are those defined by congruence conditions that satisfy an additional 'largeness' axiom.

Definition 7.4.7. A family $\mathcal{F}$ of elliptic curves which is defined by congruence conditions is further called a large family if for all but finitely many primes p the set $\mathrm{Inv}_p(\mathcal{F})$ contains all pairs $(I,J) \in \mathbb{Z}_p^2$ such that $p^2 \nmid \Delta(I,J)$.

Remark 7.4.8. Rephrased in terms of the associated elliptic curves, this definition states that: for sufficiently large p, Σ_p contains all elliptic curves with reduction types I_0 and I_1.

§ 7.4.2 | Counting Binary Quartic Forms

By Theorem 7.2.8, finding the average of $\mathrm{Sel}_2(E/\mathbb{Q})$ as E varies in a large family is equivalent to counting $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of elements $g \in V_{\mathbb{Z}}$ with certain invariants. Bhargava and Shankar count $\mathrm{PGL}_2(\mathbb{Z})$-orbits in $V_{\mathbb{Z}}$, rather than $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes. We postpone the relationship between the two counting problems to the next subsection, and simply present the results.

Definition 7.4.9. The height of a binary quartic form $f \in V_{\mathbb{Q}}$ with invariants I, J is defined to be

$$H(f) := \max\left\{|I|^3, J^2/4\right\}$$

Remark 7.4.10. The height of a binary quartic form is a function of its invariants. In particular, the binary quartic forms $g \in V_{\mathbb{Z}}$ which have $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes corresponding (via Theorem 7.2.8) to 2-Selmer group elements for $E/\mathbb{Q}$ have height

$$H(g) = 2^{12}H'(E).$$

Thus counting $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of binary quartic forms of bounded height corresponds to counting the elements of all $E_{A,B}$ of bounded naive height.

In order to apply local conditions (such as solubility) to the equivalence classes of binary quartic forms, we require a notion of acceptable congruence conditions.

Definition 7.4.11 ([BS15a, §2.7])**.** A function $\psi : V_{\mathbb{Z}} \to [0,1] \subset \mathbb{R}$ is said to be defined by congruence conditions if, for all primes p, there exist functions $\psi_p : V_{\mathbb{Z}_p} \to [0,1]$ satisfying

(i) For all $f \in V_{\mathbb{Z}}$, the product $\prod_p \psi_p(f)$ converges to $\psi(f)$.

(ii) For each prime p, the function ψ_p is locally constant outside some closed set $S_p \subset V_{\mathbb{Z}_p}$ of measure zero.

If additionally for all but finitely many primes p, we have $\psi_p(f) = 1$ whenever $p^2 \nmid \Delta(f)$, then we say ψ is acceptable.

We then have our notation for the relevant counts.

Definition 7.4.12. For each real number $X > 0$, we define $N(V_{\mathbb{Z}}^{(i)}; X)$ to be the number of $\mathrm{PGL}_2(\mathbb{Z})$-equivalence classes of irreducible elements $f \in V_{\mathbb{Z}}^{(i)}$ satisfying $H(f) < X$

Let ψ be an acceptable function with corresponding local functions ψ_p which are $\mathrm{PGL}_2(\mathbb{Z})$-invariant. Then we further define $N_\psi(V_{\mathbb{Z}}^{(i)}; X)$ to be the number of $\mathrm{PGL}_2(\mathbb{Z})$-orbits of irreducible elements $f \in V_{\mathbb{Z}}^{(i)}$ satisfying $H(f) < X$, where each equivalence class is counted with weight $\psi(f)$.

We then have their main counting machine.

Theorem 7.4.13 ([BS15a, Theorem 2.21]). *Let $\psi : V_{\mathbb{Z}} \to [0,1]$ be an acceptable function defined by congruence conditions via local functions $\psi_p : V_{\mathbb{Z}_p} \to [0,1]$ which are $\mathrm{PGL}_2(\mathbb{Z})$-invariant. Then for $i \in \{0, 1, 2+, 2-\}$*

$$N_\psi(V_{\mathbb{Z}}^{(i)}; X) = N(V_{\mathbb{Z}}^{(i)}; X) \prod_p \int_{f \in V_{\mathbb{Z}_p}} \psi_p(f) df + o(X^{5/6})$$

§ 7.4.3 | Weighted integral orbits

We now explain the reduction from $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes in $V_{\mathbb{Z}}$ to $\mathrm{PGL}_2(\mathbb{Z})$-orbits. Doing so makes use of a certain well-behaved weighting. Ideally, in order to count $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes in $V_{\mathbb{Z}}$, one could simply count the number of $\mathrm{PGL}_2(\mathbb{Z})$-orbits of $f \in V_{\mathbb{Z}}$ with weight $1/n(f)$ where $n(f)$ is the number of $\mathrm{PGL}_2(\mathbb{Z})$-orbits inside the $\mathrm{PGL}_2(\mathbb{Q})$-equivalence class of f. However, this weighting is not defined by congruence conditions and so Theorem 7.4.13 would not be possible. In order to resolve this, one replaces $n(f)$ by a slightly different weight $m(f)$.

Definition 7.4.14 ([BS15a, §3.2]). For a binary quartic form $f \in V_{\mathbb{Z}}$ we define a weighting

$$m(f) := \sum_{f' \in B(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}}(f)}{\#\mathrm{Aut}_{\mathbb{Z}}(f')},$$

where $B(f)$ denotes a set of representatives of orbits of the action of $\mathrm{PGL}_2(\mathbb{Z})$ on the $\mathrm{PGL}_2(\mathbb{Q})$-equivalence class of $f \in V_{\mathbb{Z}}$, and $\mathrm{Aut}_R(f)$ is the stabiliser of f in $\mathrm{PGL}_2(R)$. Analogously there are local weights at each prime p for $f \in V_{\mathbb{Z}_p}$

$$m_p(f) := \sum_{f' \in B_p(f)} \frac{\#\mathrm{Aut}_{\mathbb{Q}_p}(f)}{\#\mathrm{Aut}_{\mathbb{Z}_p}(f')},$$

where $B_p(f)$ denotes a set of representatives of orbits for the action of $\mathrm{PGL}_2(\mathbb{Z}_p)$ on the $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivalence class of $f \in V_{\mathbb{Z}}$.

This new weighting is defined by congruence conditions, which keeps us on track for using Theorem 7.4.13.

Proposition 7.4.15 ([BS15a, Prop 3.6]). *Suppose $f \in V_{\mathbb{Z}}$ has invariants I, J such that $\Delta'(I,J) \neq 0$, then $m(f) = \prod_p m_p(f)$.*

Helpfully, weighting by $m(f)$ instead of $n(f)$ does not matter particularly for counting purposes – they differ only in a density zero set.

Lemma 7.4.16 ([BS15a, Lemma 2.4], see also [BS15a, §3.2]). *For $f \in V_{\mathbb{Z}}$, denote its $\mathrm{PGL}_2(\mathbb{Q})$-equivalence class in $V_{\mathbb{Z}}$ by $[f]_{\mathbb{Q}}$. Then for sufficiently large $X > 0$ and any $\varepsilon > 0$*

$$\#\left\{ [f]_{\mathbb{Q}} \ : \ \begin{smallmatrix} f \in V_{\mathbb{Z}}, \\ H(f) < X \\ \Delta'(I(f),J(f)) \neq 0 \\ m(f) \neq n(f) \end{smallmatrix} \right\} \ll_\varepsilon X^{3/4+\varepsilon}$$

Thus, in order to count $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes of elements $f \in V_{\mathbb{Z}}$, it is enough to count $\mathrm{PGL}_2(\mathbb{Z})$-equivalence classes of f with weight $1/m(f)$, as the number

of forms for which the correct weight differs from this is negligible when taking an average.

Finally, if we write $\psi_p := \mathbb{1}_p/m_p(f)$, where $\mathbb{1}_p$ is the indicator function for the set of $\mathbb{Q}_p$-soluble binary quartic forms then we see that $\psi = (\psi_p)_p$ an acceptable function defined by congruence conditions.

Proposition 7.4.17 ([BS15a, Prop. 3.18])**.** *Let $p > 2$ be an odd prime number. If $f \in V_{\mathbb{Z}}$ is either not $\mathbb{Q}_p$-soluble or $m_p(f) \neq 1$ then $p^2 \mid \Delta'(I(f), J(f))$.*

In particular we can use Theorem 7.4.13 to count our orbits of interest. In doing so, it will be helpful to compute the p-adic masses on the right hand side of the equation there. For this we have the following.

Theorem 7.4.18 ([BS15a, Cor. 3.8])**.** *Let p be a prime and ϕ_p a continuous $\mathrm{PGL}_2(\mathbb{Q}_p)$-invariant function on $V_{\mathbb{Z}_p}$, such that every element $f \in V_{\mathbb{Z}_p}$ in the support of ϕ_p has nonzero discriminant, is soluble and satisfies $2^4 \cdot 3 \mid I(f)$ and $2^6 \cdot 3^3 \mid J(f)$. Then*

$$\begin{aligned}&\int_{\mathbb{Z}_p} \frac{\phi_p(f)}{m_p(f)} df \\ &= \left|\frac{1}{27}\right|_p \mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z}_p) \int_{\substack{(I,J)\in\mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \frac{1}{\#E^{I,J}(\mathbb{Q}_p)[2]} \left(\sum_{\sigma \in E^{I,J}(\mathbb{Q}_p)/2E^{I,J}(\mathbb{Q}_p)} \phi_p(f_\sigma) \right) dI dJ\end{aligned}$$

where f_σ is any element in $V_{\mathbb{Z}_p}$ corresponding to σ under the correspondence in Theorem 7.2.8.

§ 7.5 | A Statistical Wiles–Greenberg Formula

Having now recalled the technology we need, we give a useful application. For the duration of this section, we let $\mathcal{F}$ be a large family of elliptic curves.

§ 7.5.1 | 2-Selmer Bundles

We shall firstly need a way to gather together the elements of general Selmer structures on elliptic curves in our large family $\mathcal{F}$.

Definition 7.5.1. A 2-Selmer bundle $\mathscr{L}$ (on $\mathcal{F}$) is the data of, for each place $v \in \Omega_{\mathbb{Q}}$, a subset

$$\mathscr{L}_v(\mathcal{F}) \subseteq \left\{ f \in V_{\mathbb{Q}_v} \ : \ \substack{(2^{-4}I(f), 2^{-6}J(f)) \in \mathrm{Inv}_v(\mathcal{F}) \\ \text{and } f \text{ is } \mathbb{Q}_v\text{-soluble}} \right\},$$

such that

(I) $\mathscr{L}_\infty(\mathcal{F})$ is either the whole set or the subset of binary quartic forms which have a linear factor over $\mathbb{R}$ – we say that $\mathscr{L}_\infty(\mathcal{F})$ is type 2 or type 1 respectively for the two options;

(II) for each prime number p, $\mathscr{L}_p(\mathcal{F}) \cap V_{\mathbb{Z}_p}$ is closed and open in $V_{\mathbb{Z}_p}$ and is a union of $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivalence classes;

(III) for every $(I,J) \in \mathrm{Inv}(\mathcal{F})$, all but finitely many prime numbers p satisfy

$$\left\{ f \in V_{\mathbb{Z}_p} \ : \ \substack{(I(f),J(f))=(2^4I,2^6J) \\ \text{and } f \in \mathscr{L}_p(\mathcal{F})} \right\} = \left\{ f \in V_{\mathbb{Z}_p} \ : \ \substack{(I(f),J(f)) \in (2^4I,2^6J) \\ f \text{ is } \mathbb{Q}_p\text{-soluble}} \right\};$$

(IV) there is a constant $C(\mathscr{L}) \in \mathbb{R}_{>0}$ such that for every prime number $p \geq C(\mathscr{L})$ and every $f \in V_{\mathbb{Z}}$: if $p^2 \nmid \Delta(f)$ then $f \in \mathscr{L}_p(\mathcal{F})$.

For each 2-Selmer bundle $\mathscr{L}$ we denote the subset

$$\mathscr{L}(\mathcal{F}) := \left\{ f \in V_{\mathbb{Z}} \ : \ \substack{(2^{-4}I(f),\ 2^{-6}J(f)) \in \mathrm{Inv}(\mathcal{F}) \\ \forall v \in \Omega_{\mathbb{Q}},\ f \in \mathscr{L}_v(\mathcal{F})} \right\} \subseteq V_{\mathbb{Z}}.$$

Remark 7.5.2. By definition, $\mathscr{L}(\mathcal{F})$ is automatically a union of $\mathrm{PGL}_2(\mathbb{Q})$-equivalence classes. The restrictions on $\mathscr{L}_\infty(\mathcal{F})$ should be understood as follows. If $\Delta'(I,J) < 0$ then $\#E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}) = 1$ so that being $\mathbb{R}$-soluble is equivalent to having a linear factor by Corollary 7.2.4. If instead $\Delta'(I,J) > 0$ then $\#E^{I,J}(\mathbb{R})/2E^{I,J}(\mathbb{R}) = 2$, and so a choice of subgroup can be either the whole group or trivial. Under the correspondence Corollary 7.2.4 such a choice is equivalent to deciding whether to include all $\mathbb{R}$-soluble forms with appropriate invariants or just the ones with a linear factor. Our constraint essentially forces that this decision is uniform across all of the elliptic curves $E \in \mathcal{F}$.

We can understand the set $V_{\mathbb{Z}} \cap \mathscr{L}_\infty(\mathcal{F})$ of binary quartic forms in terms of the $V_{\mathbb{Z}}^{(i)}$ of Notation 7.2.1. We list all of the possibilities in the table below for the readers convenience, for an explanation of this see the discussion at the start of [BS15a, §2.1].

Type of $\mathscr{L}_\infty(\mathcal{F})$	$\mathrm{Inv}_\infty(\mathcal{F})$	$V_{\mathbb{Z}} \cap \mathscr{L}_\infty(\mathcal{F})$
1	$\{(I,J) \ : \ \Delta(I,J) < 0\}$	$V_{\mathbb{Z}}^{(1)}$
1	$\{(I,J) \ : \ \Delta(I,J) > 0\}$	$V_{\mathbb{Z}}^{(0)}$
1	$\{(I,J) \ : \ \Delta(I,J) \neq 0\}$	$V_{\mathbb{Z}}^{(0)} \cup V_{\mathbb{Z}}^{(1)}$
2	$\{(I,J) \ : \ \Delta(I,J) < 0\}$	$V_{\mathbb{Z}}^{(1)}$
2	$\{(I,J) \ : \ \Delta(I,J) > 0\}$	$V_{\mathbb{Z}}^{(0)} \cup V_{\mathbb{Z}}^{(2+)}$
2	$\{(I,J) \ : \ \Delta(I,J) \neq 0\}$	$V_{\mathbb{Z}}^{(0)} \cup V_{\mathbb{Z}}^{(1)} \cup V_{\mathbb{Z}}^{(2+)}$

Table 7.1: The possibilities for $V_{\mathbb{Z}} \cap \mathscr{L}_\infty(\mathcal{F})$, dependent on the type of $\mathscr{L}_\infty(\mathcal{F})$ and $\mathrm{Inv}_\infty(\mathcal{F})$

A 2-Selmer bundle associates a Selmer structure of sorts to every elliptic curve in the family. We will define it below, then prove the important properties afterwards.

Definition 7.5.3. Let $\mathscr{L}$ be a 2-Selmer bundle. Then for each elliptic curve $E \in \mathcal{F}$ and each place $v \in \Omega_{\mathbb{Q}}$, writing $(I,J) := (I(E),J(E))$, we define the subset

$$\mathscr{L}(E)_v := \delta\left(\left\{ x \in E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \ : \ \substack{x \text{ corresponds via Corollary 7.2.4} \\ \text{(with Weierstrass model } E^{2^4I,2^6J}) \\ \text{to a subset of } \mathscr{L}_v(\mathcal{F})} \right\} \right) \subseteq H^1(\mathbb{Q}_v, E[2]),$$

where $\delta : E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, E[2])$ is the usual connecting map from the Galois cohomology of the multiplication-by-2 exact sequence on E.

We then define the associated Selmer set for each $E \in \mathcal{F}$ to be

$$\mathrm{Sel}_{\mathscr{L}}(\mathbb{Q}, E[2]) := \left\{ x \in H^1(\mathbb{Q}, E[2]) \ : \ \mathrm{res}_v(x) \in \mathscr{L}(E)_v \ \forall v \in \Omega_{\mathbb{Q}} \right\},$$

where $\mathrm{res}_v : H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}_v, E[2])$ is the usual restriction map.

Remark 7.5.4. Note that, as in Remark 7.5.2, for each 2-Selmer bundle $\mathscr{L}$ we have that $\mathscr{L}_\infty(\mathcal{F})$ has type 2 if and only if for every $E \in \mathcal{F}$ with $\Delta'(I(E), J(E)) > 0$, we have $\#\mathscr{L}(E^{I,J})_\infty = 2$.

Lemma 7.5.5. *Let $\mathscr{L}$ be a 2-Selmer bundle, and $E \in \mathcal{F}$ be an elliptic curve. If $\mathscr{L}(E)_v \subseteq H^1(\mathbb{Q}_v, E[2])$ is a subgroup for every $v \in \Omega_{\mathbb{Q}}$ then $\mathscr{L}(E) := \{\mathscr{L}(E)_v\}_{v \in \Omega_{\mathbb{Q}}}$ is a Selmer structure with Selmer group $\mathrm{Sel}_{\mathscr{L}}(\mathbb{Q}, E[2])$.*

Proof. All that needs to be checked is that for all but finitely many $v \in \Omega_{\mathbb{Q}}$, $\mathscr{L}(E)_v$ is in fact the group of unramified classes. Let $I = I(E)$ and $J = J(E)$ for convenience.

Note that the constraint in the definition of a 2-Selmer bundle ensures that all but finitely many $v \in \Omega_{\mathbb{Q}}$ satisfy that the set of $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivalence classes in

$$\{ f \in \mathscr{L}_p(\mathcal{F}) \ : \ (I(f), J(f)) = (I, J) \}$$

corresponds via Corollary 7.2.4 to $E^{2^4 I, 2^6 J}(\mathbb{Q}_p)/2E^{2^4 I, 2^6 J}(\mathbb{Q}_p)$. In particular, since for all but finitely many p this right hand set maps under the connecting map δ to the subgroup of unramified classes $H^1_{\mathrm{nr}}(\mathbb{Q}, E[2])$, we have the result. □

Of course there is a classical example of the construction above: the 2-Selmer bundle which gives the usual 2-Selmer groups.

Example 7.5.6. *Consider the 2-Selmer bundle $\mathscr{S}$ given by, for each place $v \in \Omega_{\mathbb{Q}}$, setting*

$$\mathscr{S}_p(\mathcal{F}) = \left\{ f \in V_{\mathbb{Q}_v} \ : \ \substack{(2^{-4}I(f), 2^{-6}J(f)) \in \mathrm{Inv}_v(\mathcal{F}) \\ \text{and } f \text{ is } \mathbb{Q}_v\text{-soluble}} \right\}.$$

Indeed: Axioms (I), (II) and (III) are clear from the definitions (and also implicit in [BS15a]*). Finally Axiom (IV) follows from Proposition 7.4.17.*

The associated Selmer group for $E \in \mathcal{F}$ is the usual 2-Selmer group, i.e.

$$\mathrm{Sel}_{\mathscr{S}}(\mathbb{Q}, E[2]) = \mathrm{Sel}_2(E/\mathbb{Q}).$$

§ 7.5.2 | Statistics

Here we use the statistical results of [BS15a], as recalled in §7.4, to conclude a local mass formula for the average size of Selmer groups obtained by 2-Selmer bundles. More specifically we will apply Theorem 7.4.13, but we shall unpack the right hand side of this a little. Firstly we establish the archimedean contribution.

Proposition 7.5.7. *If $\mathscr{L}$ is a 2-Selmer bundle then*

$$N(V_{\mathbb{Z}} \cap \mathscr{L}_\infty(\mathcal{F}); X) = \frac{1}{27}\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R}) \int_{\substack{(I,J)\in \mathrm{Inv}_\infty(\mathcal{F}) \\ H(I,J)<X}} \frac{\#\mathscr{L}(E^{I,J})_\infty}{\#E^{I,J}(\mathbb{R})[2]} dIdJ + O(X^{3/4+\varepsilon})$$

Proof. If $\#\mathscr{L}(E^{I,J}) = 2$ for $\Delta(I,J) > 0$ then this is [BS15a, Final paragraph before Thm. 3.19]. We expose the proof alongside the case that we set the archimedean condition to be triviality. Note that by [BS15a, eq. (20)] and [BS15a, Prop. 2.8 and preceding discussion], and in their notation, we have for every $i = 0, 1, 2+, 2-$, writing $n_1 = 2$ and $n_i = 4$ for $i \neq 1$, then

$$\begin{aligned} &N(V_{\mathbb{Z}}^{(i)}; X) \\ &= \mathrm{Vol} R_X(L^{(i)})/n_i + O(X^{3/4+\varepsilon}) \\ &= \begin{cases} \frac{1}{27}\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R}) \int_{\substack{(I,J)\in \mathrm{Inv}_\infty(\mathcal{F}) \\ \Delta(I,J)>0 \\ H(I,J)<X}} \frac{1}{4} dIdJ + O(X^{3/4+\varepsilon}) & i = 0, 2+, 2- \\ \frac{1}{27}\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R}) \int_{\substack{(I,J)\in \mathrm{Inv}_\infty(\mathcal{F}) \\ \Delta(I,J)<0 \\ H(I,J)<X}} \frac{1}{2} dIdJ + O(X^{3/4+\varepsilon}) & i = 1 \end{cases} \end{aligned}$$

The result then follows from Remark 7.5.4 and Table 7.1, checking each possibility for $\mathrm{Inv}_\infty(\mathcal{F})$ and type for $\mathscr{L}_\infty(\mathcal{F})$ and using that $N(V_{\mathbb{Z}}^{(i)})$ is uniform for $i = 0, 2+, 2-$. □

We then we compute the local masses coming from the non archimedean places.

Lemma 7.5.8. *Let $\mathscr{L}$ be a 2-Selmer bundle. Then for every prime p we have*

$$\int_{\mathscr{L}_p(\mathcal{F})\cap V_{\mathbb{Z}_p}} \frac{1}{m_p(f)} df = \left|\frac{2^{10}}{27}\right|_p \mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z}_p) \int_{(I,J)\in \mathrm{Inv}_p(\mathcal{F})} \frac{\#\mathscr{L}(E^{I,J})_p}{\#E^{I,J}(\mathbb{Q}_p)[2]} dIdJ$$

Proof. Define the function $\phi_p : V_{\mathbb{Z}_p} \to \{0, 1\}$, by $\phi_p(f) = 1$ if and only if $f \in \mathscr{L}_p(\mathcal{F})$. By definition, ϕ_p is continuous and so by Theorem 7.4.18 we obtain

$$\begin{aligned} \int_{\mathscr{L}_p(\mathcal{F})} \frac{1}{m_p(f)} df &= \int_{\mathbb{Z}_p} \frac{\phi_p(f)}{m_p(f)} df \\ &= \left|\frac{1}{27}\right|_p \mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z}_p) \int_{\substack{(I,J)\in \mathbb{Z}_p^2 \\ \Delta(I,J)\neq 0}} \frac{\#\mathscr{L}(E^{I,J})_p}{\#E^{I,J}(\mathbb{Q}_p)[2]} dIdJ \\ &= \left|\frac{2^{10}}{27}\right|_p \mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z}_p) \int_{(I,J)\in \mathrm{Inv}_p(\mathcal{F})} \frac{\#\mathscr{L}(E^{I,J})_p}{\#E^{I,J}(\mathbb{Q}_p)[2]} dIdJ \end{aligned}$$

where the final step is given by the variable change $(2^4 I, 2^6 J) \mapsto (I, J)$, noting that $E^{I,J}$ is $\mathbb{Q}_p$ isomorphic to $E^{2^4 I, 2^6 J}$. □

We then have the weighted indicator function for counting elements in a 2-Selmer bundle.

Definition 7.5.9. For every 2-Selmer bundle $\mathscr{L}$ and prime number p, let

$$\phi_{\mathscr{L},p} : V_{\mathbb{Z}_p} \to \{0,1\}$$

be the indicator function which is 1 if $f \in \mathscr{L}_p(\mathcal{F})$ and 0 else. Moreover, let $\psi_{\mathscr{L},p} := \phi_{\mathscr{L},p}/m_p$, and denote $\psi_{\mathscr{L}} := \prod_p \psi_{\mathscr{L},p} : V_{\mathbb{Z}} \to \{0,1\}$.

Finally, we need to know that this weighted indicator function (with which we wish to apply Theorem 7.4.13) is indeed acceptable.

Lemma 7.5.10. *Let $\mathscr{L}$ be a 2-Selmer bundle. Then the function $\psi_{\mathscr{L}}$ is acceptable (in the sense of Definition 7.4.11), with local functions $\psi_{\mathscr{L},p} = \phi_{\mathscr{L},p}/m_p$.*

Proof. That these local functions converge to the required global one is immediate from Proposition 7.4.15. The second condition, that $\psi_{\mathscr{L},p}$ is locally constant outside of a closed set of measure 0, is clear from the definitions of the maps $\phi_{\mathscr{L},p}$ and m_p. Finally, to obtain the final condition, we need that for sufficiently large prime p, $\psi_{\mathscr{L},p}(f) = 1$ whenever $p^2 \nmid \Delta(f)$. This follows from Proposition 7.4.17 and Axiom (IV) for the 2-Selmer bundle $\mathscr{L}$. □

We are now ready to state the main statistical corollary.

Theorem 7.5.11. *Let $\mathscr{L}$ be a 2-Selmer bundle. Then, for each large family $\mathcal{F}$ of elliptic curves,*

$$\frac{\sum_{\substack{E\in\mathcal{F}\\ H'(E)<X}} (\#\mathrm{Sel}_{\mathscr{L}}(\mathbb{Q},E[2]) - 1)}{\sum_{\substack{E\in\mathcal{F}\\ H'(E)<X}} 1} = 2\mathscr{M}_\infty^{\mathscr{L}}(\mathcal{F};X)\prod_p \mathscr{M}_p^{\mathscr{L}}(\mathcal{F}) + o(1),$$

where the local masses are

$$\mathscr{M}_\infty^{\mathscr{L}}(\mathcal{F};X) := \frac{\int_{\substack{(I,J)\in \mathrm{Inv}_\infty(\mathcal{F})\\ H(I,J)<X}} \frac{\#\mathscr{L}(E^{I,J})_\infty}{\#E^{I,J}(\mathbb{R})[2]} dIdJ}{\int_{\substack{(I,J)\in \mathrm{Inv}_\infty(\mathcal{F})\\ H(I,J)<X}} dIdJ}$$

$$\mathscr{M}_p^{\mathscr{L}}(\mathcal{F}) := \frac{\int_{(I,J)\in \mathrm{Inv}_p(\mathcal{F})} \frac{\#\mathscr{L}(E^{I,J})_p}{\#E^{I,J}(\mathbb{Q}_p)[2]} dIdJ}{\int_{(I,J)\in \mathrm{Inv}_p(\mathcal{F})} dIdJ}$$

Proof. By Lemma 7.4.16 (and the explanation below it) and Theorem 7.2.8 the numerator of the left hand side is equal to the number of $\mathrm{PGL}_2(\mathbb{Z})$-orbits in $\mathscr{L}(\mathcal{F})$ of height at most $2^{12}X$ with no rational linear factor counted with weights $1/m(f)$ (up to acceptable error). Moreover, by [BS15a, Lemma 2.3] the number of $\mathrm{PGL}_2(\mathbb{Z})$-orbits in $\mathscr{L}(\mathcal{F})$ of height at most $2^{12}X$ which are reducible but factor as a pair of irreducible quadratics is at worst $O\left(X^{2/3+\varepsilon}\right)$ and so by counting orbits of irreducible forms we will be within acceptable error of counting the orbits of forms with no rational linear factor.

Thus by Theorem 7.4.13, Lemma 7.5.10 and Table 7.1 we have

$$\sum_{\substack{E\in\mathcal{F}\\ H'(E)<X}} (\#\mathrm{Sel}_{\mathscr{L}}(\mathbb{Q},E[2])-1) = N_{\psi_{\mathscr{L}}}(V_{\mathbb{Z}}\cap\mathscr{L}_\infty(\mathcal{F});2^{12}X)$$
$$= N(V_{\mathbb{Z}}\cap\mathscr{L}_\infty(\mathcal{F});2^{12}X)\prod_p\int_{f\in V_{\mathbb{Z}_p}}\psi_p(f)df+o(X^{5/6})$$

Then, using the mass formulae in Proposition 7.5.7 and Lemma 7.5.8, this gives

$$N(V_{\mathbb{Z}}\cap\mathscr{L}_\infty(\mathcal{F});2^{12}X)\prod_p\int_{f\in V_{\mathbb{Z}_p}}\psi_p(f)df+o(X^{5/6})$$
$$=\frac{2^{10}}{27}\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})\int\limits_{\substack{(I,J)\in\mathrm{Inv}_\infty(\mathcal{F})\\ H(I,J)<X}}\frac{\#\mathscr{L}(E^{I,J})_\infty}{\#E^{I,J}(\mathbb{R})[2]}dIdJ$$
$$\prod_p\left(\left|\frac{2^{10}}{27}\right|_p\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z}_p)\int\limits_{(I,J)\in\mathrm{Inv}_p(\mathcal{F})}\frac{\#\mathscr{L}(E^{I,J})_p}{\#E^{I,J}(\mathbb{Q}_p)[2]}dIdJ\right)+o(X^{5/6})$$
$$=2\left(\int\limits_{\substack{(I,J)\in\mathrm{Inv}_\infty(\mathcal{F})\\ H(I,J)<X}}\frac{\#\mathscr{L}(E^{I,J})_\infty}{\#E^{I,J}(\mathbb{R})[2]}dIdJ\right)\prod_p\left(\int\limits_{(I,J)\in\mathrm{Inv}_p(\mathcal{F})}\frac{\#\mathscr{L}(E^{I,J})_p}{\#E^{I,J}(\mathbb{Q}_p)[2]}dIdJ\right)+o(X^{5/6}).$$

where the last equality uses that $\prod_p\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z}_p)=\zeta(2)^{-1}$ as well as the equality $\mathrm{Vol}\mathrm{PGL}_2(\mathbb{Z})\backslash\mathrm{PGL}_2(\mathbb{R})=2\zeta(2)$. Moreover by [BS15a, Thm 3.17]

$$\sum_{\substack{E\in\mathcal{F}\\ H'(E)<X}}1=\left(\int_{\substack{(I,J)\in\mathrm{Inv}_\infty(\mathcal{F})\\ H(I,J)<X}}dIdJ\right)\prod_p\left(\int_{(I,J)\in\mathrm{Inv}_p(\mathcal{F})}dIdJ\right)+o(X^{5/6}).$$

Thus we have the result. □

We have now reduced computing the average size of certain Selmer structures on elliptic curves to proving that they can be packaged as Selmer groups arising from 2-Selmer bundles, a purely algebraic task, and then applying Theorem 7.5.11 and computing some local masses.

§ 7.6 | The Corestriction Selmer Bundle

Our goal is to apply Theorem 7.5.11 to count the average size of corestriction Selmer groups. In order to do this, we have the, somewhat algebraic, task of showing that these Selmer groups arise from a 2-Selmer bundle. As in the previous section, we take $\mathcal{F}$ to be a large family.

Definition 7.6.1. Let $K/\mathbb{Q}$ be a multiquadratic extension and let $S:=\ker(\mathbb{Q}^\times/\mathbb{Q}^{\times 2}\to K^\times/K^{\times 2})$. Define the 2-Selmer bundle $\mathscr{C}(K)$ given by, for each place $v\in\Omega_{\mathbb{Q}}$,

$$\mathscr{C}(K)_v(\mathcal{F})=\left\{f\in V_{\mathbb{Q}_v}\ :\ \substack{(2^{-4}I(f),2^{-6}J(f))\in\mathrm{Inv}_v(\mathcal{F})\\ \text{and } f \text{ is } (\mathbb{Q}_v,S)\text{-soluble}}\right\}.$$

Now we verify that this does indeed define a 2-Selmer bundle.

Lemma 7.6.2. *For every multiquadratic extension $K/\mathbb{Q}$, $\mathscr{C}(K)$ is indeed a 2-Selmer bundle. Moreover, our notation is well chosen:*

- *for every place $v \in \Omega_{\mathbb{Q}}$, and every pair $(I,J) \in \mathrm{Inv}_v(\mathcal{F})$, choosing a place $w \in \Omega_K$ extending v we have*

$$\mathscr{C}(K)(E^{I,J})_v = \mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathscr{S}_w(K_w; E^{I,J}));$$

- *for every $E \in \mathcal{F}$ the group $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ (in the sense of Definition 7.5.3) is precisely the corestriction Selmer group (of Definition 2.2.1).*

Proof. The identity $\mathscr{C}(K)(E^{I,J})_v = \mathrm{cor}_{K_w/\mathbb{Q}_v}(\mathscr{S}_w(K_w; E^{I,J}))$ in the lemma statement is clear from the definition and Corollary 7.3.4. Similarly, the Selmer group statement is immediate so long as it is well defined (i.e. so long as $\mathscr{C}(K)$ is a 2-Selmer bundle).

Note that for every $v \in \Omega_{\mathbb{Q}}$ we can write

$$\mathscr{C}(K)_v(\mathcal{F}) = \bigcap_{\theta \in S} \left(\theta^{-1} \cdot \mathscr{S}_v(\mathcal{F})\right).$$

As Axioms (I) and (II) are clearly invariant under taking intersections and scaling, these follow from the fact that $\mathscr{S}$ is a 2-Selmer bundle.

By Corollary 7.3.4 we see that for each pair $(I,J) \in \mathrm{Inv}(\mathcal{F})$, and place $v \in \Omega_{\mathbb{Q}}$ the set of $\mathrm{PGL}_2(\mathbb{Q}_v)$-equivalence classes in

$$\{f \in \mathscr{C}(K)_v(\mathcal{F}) \ : \ (I(f), J(f)) = (I,J)\}$$

corresponds to the local corestriction group $\mathscr{C}_v(K/\mathbb{Q}; E^{I,J}) \subset H^1(\mathbb{Q}, E^{I,J}[2])$. By Lemma 2.2.4, all but finitely many v satisfy

$$\mathscr{C}_v(K/\mathbb{Q}; E^{I,J}) = H^1_{\mathrm{nr}}(\mathbb{Q}, E[2]) = \mathscr{S}_v(\mathbb{Q}; E^{I,J}).$$

Now for all but finitely many v the local corestriction group corresponds to the set of soluble forms with invariants I, J as required for Axiom (III).

It remains to prove that Axiom (IV) holds. Let $p \geq 5$ be a prime number, and assume $f \in V_{\mathbb{Z}}$ is such that $p^2 \nmid \Delta(f)$. By Proposition 7.4.17, f is soluble and so its $\mathrm{PGL}_2(\mathbb{Q}_p)$-equivalence class corresponds to an element of $\mathscr{S}_p(\mathbb{Q}; E^{I,J})$. Writing $(I,J) := (I(f), J(f))$, we note that (by Appendix A) $E^{I,J}$ has reduction type I_0 or I_1. By [Maz72, Corollary 4.4], Proposition 3.1.4 and Proposition 3.1.2, we thus have $\mathscr{C}_p(K/\mathbb{Q}; E^{I,J}) = \mathscr{S}_p(\mathbb{Q}; E^{I,J})$ and so $f \in \mathscr{C}(K)_p(\mathcal{F})$ as required. □

Thus we have the following corollary of Theorem 7.5.11.

Corollary 7.6.3. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Then,*

$$\frac{\sum_{\substack{E\in\mathcal{F}\\ H'(E)<X}}(\#\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q},E[2])-1)}{\sum_{\substack{E\in\mathcal{F}\\ H'(E)<X}}1}=2\mathscr{M}_{\infty}^{\mathscr{C}(K)}(\mathcal{F};X)\prod_{p}\mathscr{M}_{p}^{\mathscr{C}(K)}(\mathcal{F})+o(1),$$

where the local masses are

$$\mathscr{M}_{\infty}^{\mathscr{C}(K)}(\mathcal{F};X):=\frac{\int_{\substack{(I,J)\in\mathrm{Inv}_{\infty}(\mathcal{F})\\ H(I,J)<X}}\frac{\#\mathscr{C}(K)(E^{I,J})_{\infty}}{\#E^{I,J}(\mathbb{R})[2]}dIdJ}{\int_{\substack{(I,J)\in\mathrm{Inv}_{\infty}(\mathcal{F})\\ H(I,J)<X}}dIdJ},$$

$$\mathscr{M}_{p}^{\mathscr{C}(K)}(\mathcal{F}):=\frac{\int_{(I,J)\in\mathrm{Inv}_{p}(\mathcal{F})}\frac{\#\mathscr{C}(K)(E^{I,J})_{p}}{\#E^{I,J}(\mathbb{Q}_{p})[2]}dIdJ}{\int_{(I,J)\in\mathrm{Inv}_{p}(\mathcal{F})}dIdJ}.$$

Proof. Immediate from Lemma 7.6.2 and Theorem 7.5.11. □

Of course: the local masses above depend on the family $\mathcal{F}$, and so we cannot really go much further in this generality.

§ 7.7 | The Family of All Elliptic Curves

We conclude the chapter by applying Corollary 7.6.3 for the most common family of interest: that of all elliptic curves.

Notation 7.7.1. We denote by $\mathcal{F}^{all}$ the large family of elliptic curves $\mathcal{F}_{\Sigma}$ where each Σ_v is taken to be maximal (see Definition 7.4.4).

Note that $\mathcal{F}^{all}$ is, of course, in bijection with the set $\mathcal{E}$.

§ 7.7.1 | Local Densities

Here we provide some lemmas and compute some integrals which will be of use when we go to apply Corollary 7.6.3. To ease our space use somewhat, we introduce some notation for this section.

Notation 7.7.2. Recall the notation in Notation 6.1.7. We additionally define for each prime number p the relative density of a subset $Z\subseteq\mathcal{E}_p$ to be

$$D_p(Z):=\frac{\int_{(A,B)\in Z}dAdB}{\int_{(A,B)\in\mathcal{E}_p}dAdB}=\frac{\int_{(A,B)\in Z}dAdB}{1-p^{-10}}.$$

Lemma 7.7.3. *Let $p\geq 5$ be a prime number and $a\in\mathbb{F}_p^{\times}$, then*

$$D_p\left(\left\{(A,B)\in\mathcal{E}_p\ :\ \begin{smallmatrix}E_{A,B}\text{ has reduction type }III\\ \text{and }Ap^{-1}\equiv a\mod p\end{smallmatrix}\right\}\right)=\frac{p^6}{p^{10}-1},$$

and

$$D_p\left(\left\{(A,B)\in\mathcal{E}_p\ :\ \begin{smallmatrix}E_{A,B}\text{ has reduction type }III^*\\ \text{and }Ap^{-3}\equiv a\mod p\end{smallmatrix}\right\}\right)=\frac{p}{p^{10}-1}.$$

Proof. The first equality follows from Lemma 6.2.3. The second equality is seen by noting that the set we are taking density of is the image of the one in the first equality under the map $(A, B) \mapsto (p^2A, p^3B)$ by Appendix A. □

Lemma 7.7.4. *Let $p \geq 5$ be a prime number and $n \in \{0, 1, 3\}$, then*

$$D_p\left(\left\{(A,B) \in \mathcal{E}_p \ : \ \begin{smallmatrix} E_{A,B} \text{ has reduction type } I_0 \\ \text{and } T^3+AT+B \text{ has } n \text{ roots}\end{smallmatrix}\right\}\right) = \begin{cases} \frac{p^8(p^2-1)}{3(p^{10}-1)} & \text{if } n = 0, \\ \frac{p^9(p-1)}{2(p^{10}-1)} & \text{if } n = 1, \\ \frac{p^8(p-1)(p-2)}{6(p^{10}-1)} & \text{if } n = 3, \end{cases}$$

and

$$D_p\left(\left\{(A,B) \in \mathcal{E}_p \ : \ \begin{smallmatrix} E_{A,B} \text{ has reduction type } I_0^* \\ \text{and } T^3+Ap^{-2}T+Bp^{-3} \text{ has } n \text{ roots}\end{smallmatrix}\right\}\right) = \begin{cases} \frac{p^3(p^2-1)}{3(p^{10}-1)} & \text{if } n = 0, \\ \frac{p^4(p-1)}{2(p^{10}-1)} & \text{if } n = 1, \\ \frac{p^3(p-1)(p-2)}{6(p^{10}-1)} & \text{if } n = 3, \end{cases}$$

Proof. The first equality follows from Lemma 6.2.5. The second equality is seen by noting that the set we are taking the density of is the image of the one in the first equality under the map $(A, B) \mapsto (p^2A, p^3B)$ by Appendix A. □

Lemma 7.7.5. *Let $p \geq 5$ be a prime number and $n > 0$ an integer, and let $R_1, R_2 \in \left\{\mathbb{F}_p^{\times 2}, \mathbb{F}_p^{\times} \backslash \mathbb{F}_p^{\times 2}\right\}$. Then*

$$D_p\left(\left\{(A,B) \in \mathcal{E}_p \ : \ \begin{smallmatrix} E_{A,B} \text{ is type } I_n \text{ at } p \\ (B \mod p) \in R_1 \\ ((4A^3+27B^2)/p^n \mod p) \in R_2\end{smallmatrix}\right\}\right) = \frac{p^{8-n}(p-1)^2}{4(p^{10}-1)}$$

and

$$D_p\left(\left\{(A,B) \in \mathcal{E}_p \ : \ \begin{smallmatrix} E_{A,B} \text{ is type } I_n^* \text{ at } p \\ (Bp^{-3} \mod p) \in R_1 \\ ((4A^3+27B^2)/p^{n+6} \mod p) \in R_2\end{smallmatrix}\right\}\right) = \frac{p^{3-n}(p-1)^2}{4(p^{10}-1)}.$$

Proof. We note that by Tate's algorithm (see Appendix A)

$$\left\{(A,B) \in \mathcal{E}_p \ : \ \begin{smallmatrix} E_{A,B} \text{ is type } I_n \text{ at } p \\ (B \mod p) \in R_1 \\ ((4A^3+27B^2)/p^n \mod p) \in R_2\end{smallmatrix}\right\} = \left\{(A,B) \in \mathbb{Z}_p^2 \ : \ \begin{smallmatrix} (B \mod p) \in R_1 \\ 4A^3+27B^2 \equiv 0 \mod p^n \\ ((4A^3+27B^2)/p^n \mod p) \in R_2\end{smallmatrix}\right\}.$$

It follows from Lemma 6.3.2 that for each $B \in \mathbb{Z}_p^{\times}$,

$$\begin{aligned} \int_{\substack{A \in \mathbb{Z}_p \\ 4A^3+27B^2 \equiv 0 \bmod p^n \\ ((4A^3+27B^2)p^{-n} \bmod p) \in R_2}} dA &= \sum_{u \in R_2} \int_{\substack{A \in \mathbb{Z}_p \\ 4A^3+27B^2 \equiv up^n \bmod p^{n+1}}} dA \\ &= \begin{cases} \frac{(p-1)\#\mu_3(\mathbb{F}_p)}{2p^{n+1}} & \text{if } B^2 \bmod p \in 4\mathbb{F}_p^{\times 3}, \\ 0 & \text{else.} \end{cases} \end{aligned}$$

Thus

$$\begin{aligned}\int_{\substack{B\in\mathbb{Z}_p\\(B \bmod p)\in R_1}}\int_{\substack{A\in\mathbb{Z}_p\\v_p(4A^3+27B^2)=n\\((4A^3+27B^2)p^{-n} \bmod p)\in R_2}} dAdB &= \int_{\substack{B\in\mathbb{Z}_p\\(B \bmod p)\in R_1\\(B^2 \bmod p)\in 4\mathbb{F}_p^{\times 3}}} \frac{\#\mu_3(\mathbb{F}_p)(p-1)}{2p^{n+1}}dB\\ &= \frac{\#\mathbb{F}_p^\times}{\#\mathbb{F}_p}\frac{\#\mathbb{F}_p^{\times 6}}{\#\mathbb{F}_p^\times}\frac{\#\mu_3(\mathbb{F}_p)(p-1)}{2p^{n+1}}\\ &= \frac{\#\mu_3(\mathbb{F}_p)(p-1)^2}{\#\mu_6(\mathbb{F}_p)2p^{n+2}}\\ &= \frac{(p-1)^2}{4p^{n+2}},\end{aligned}$$

and so

$$D_p\left(\left\{(A,B)\in\mathcal{E}_p \ : \ \begin{smallmatrix}E_{A,B} \text{ is type } I_n \text{ at } p\\ (B \bmod p)\in R_1\\ ((4A^3+27B^2)/p^n \bmod p)\in R_2\end{smallmatrix}\right\}\right) = \frac{p^{8-n}(p-1)^2}{4(p^{10}-1)},$$

as required.

The second equality is seen by noting that the set we are taking the density of is the image of the one in the first equality under the map $(A,B)\mapsto(p^2A,p^3B)$ by Appendix A. □

§ 7.7.2 | Computing the p-adic Factors

We can now compute each of the p-adic masses in Corollary 7.6.3 for the family of all elliptic curves. Recall Notation 6.1.7.

Lemma 7.7.6. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For every prime number p,*

$$\mathscr{M}_p^{\mathscr{C}(K)}(\mathcal{F}^{all}) = \left|\frac{1}{2}\right|_p \frac{\int_{(A,B)\in\mathcal{E}_p}\#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1}dAdB}{1-p^{-10}},$$

where $w\in\Omega_K$ is a place extending the place at p.

Proof. Let p be a prime number, $(I,J)\in \mathrm{Inv}_p(\mathcal{F}^{all})$, and for ease write $E=E^{I,J}$. Firstly note that, since $E(\mathbb{Q}_p)$ has a finite index subgroup isomorphic to the additive group $\mathbb{Z}_p$ (see e.g. [Sil09, VII Prop. 6.3]), we have

$$\frac{\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)}{\#E(\mathbb{Q}_p)[2]} = \frac{\#\mathbb{Z}_p/2\mathbb{Z}_p}{\#\mathbb{Z}_p[2]} = \left|\frac{1}{2}\right|_p$$

Therefore, by Lemma 7.6.2 and Lemma 2.2.10, the ratio $\mathscr{M}_p^{\mathscr{C}(K)}(\mathcal{F}^{all})$ is described by the local norm index modulo 2 from Chapter 6

$$\frac{\#\mathscr{C}(K)(E)_p}{\#E(\mathbb{Q}_p)[2]} = \frac{\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)}{\#E(\mathbb{Q}_p)[2]2^{\iota_p(K/\mathbb{Q};E)}} = \left|\frac{1}{2}\right|_p 2^{-\iota_p(K/\mathbb{Q};E)}$$

Also, for every prime number $p\neq 3$ we have

$$\mathrm{Inv}_p(\mathcal{F}^{all}) = \left\{(-3A,-27B)\in\mathbb{Z}_p^2 \ : \ v_p(A)<4 \text{ or } v_p(B)<6\right\} = \mathcal{E}_p,$$

Therefore, by the above and in the language of Notation 6.1.7 we have (for $p \neq 3$)

$$\mathscr{M}_p^{\mathscr{C}(K)}(\mathcal{F}^{all}) = \left|\frac{1}{2}\right|_p \frac{\int_{(A,B)\in\mathcal{E}_p} \#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1} dAdB}{1-p^{-10}},$$

as required. When $p = 3$, the change of variables $(I, J) \mapsto (A, B)$ contributes a factor of $|81|_3$ to both the numerator and denominator, so that the above expression holds for $p = 3$ also. □

It remains to compute the integral above, which we now break into cases and compute using the density calculations in §7.7.1.

Lemma 7.7.7. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For each prime number $p \geq 5$ such that $K/\mathbb{Q}$ is unramified at p,*

$$\frac{\int_{(A,B)\in\mathcal{E}_p} \#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1} dAdB}{1-p^{-10}}$$
$$= \frac{16p^{11}+16p^{10}+-8p^9+8p^8-8p^7-10p^6-4p^5+7p^4-p^3-8p^2-24p-1}{16(p^{10}-1)(p+1)}.$$

Proof. Define the following sets

$$S_1 = \left\{(A,B)\in\mathcal{E}_p \ : \ \begin{array}{c} E_{A,B} \text{ has reduction type given by one of the following:} \\ \bullet I_n \text{ for some } n\in 2\mathbb{Z}_{>0} \\ \bullet III \\ \bullet I_n^* \text{ for some } n\in(2\mathbb{Z}_{\geq 0}+1) \\ \bullet III^* \end{array}\right\},$$
$$S_2 = \left\{(A,B)\in\mathcal{E}_p \ : \ \begin{array}{c} E_{A,B} \text{ has reduction type given by one of the following:} \\ \bullet I_0^* \text{ and } T^3+Ap^{-2}T+Bp^{-3} \text{ has 3 roots in } \mathbb{F}_p \\ \bullet I_n^* \text{ for some } n\in 2\mathbb{Z}_{\geq 0} \text{ and } -(27B^2+4A^4)p^{-(6+n)}\in\mathbb{F}_p^{\times 2} \end{array}\right\},$$
$$S_0 = \mathcal{E}_p\backslash(S_1\cup S_2).$$

Then by Proposition 3.2.9,

$$\frac{\int_{(A,B)\in\mathcal{E}_p} \#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1} dAdB}{1-p^{-10}} = \sum_{i=0}^{2} 2^{-i} D_p(S_i).$$

The relative densities of these sets can then be computed directly from Lemmas 7.7.3, 7.7.4, and 7.7.5 as

$$D_p(S_i) = \begin{cases} \frac{(p^5+1)p}{(p^{10}-1)} + \frac{(1+p^4)p^4(p-1)^2}{(p^{10}-1)(p^2-1)} & \text{if } i=1 \\ \frac{p^3(p-1)(p-2)}{6(p^{10}-1)} + \frac{p^3(p-1)^2}{4(p^{10}-1)(p^2-1)} & \text{if } i=2 \end{cases}$$
$$= \begin{cases} \frac{p(p^8-p^7+p^6+p^5+p^4-p^3+p+1)}{(p^{10}-1)(p+1)} & \text{if } i=1 \\ \frac{p^3(p-1)(2p^2-2p-1)}{12(p^{10}-1)(p+1)} & \text{if } i=2 \end{cases}$$

and so, since $D_p(S_0) = 1-(D_p(S_1)+D_p(S_2))$, the result follows. □

Lemma 7.7.8. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For each prime number $p \geq 5$*

such that $K/\mathbb{Q}$ is ramified and quadratic at p,

$$\frac{\int_{(A,B)\in\mathcal{E}_p} \#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1} dAdB}{1-p^{-10}} = \frac{(p-1)(p^4-p^3+p^2-p+1)(46p^5+62p^4+79p^3+84p^2+84p+48)}{48(p^{10}-1)}.$$

Proof. Fix a place $w \in \Omega_K$ such that $w \mid p$ and choose $\theta \in \mathbb{Z}_p$ such that $K_w = \mathbb{Q}_p(\sqrt{\theta})$. Define the following sets

$$S_1 = \left\{ (A,B) \in \mathcal{E}_p \ : \ \begin{array}{c} E_{A,B} \text{ has reduction type given by one of the following:} \\ \bullet I_0 \text{ and } T^3+AT+B \text{ has 1 root in } \mathbb{F}_p \\ \bullet I_0^* \text{ and } T^3+A\theta^{-2}T+B\theta^{-3} \text{ has 1 root in } \mathbb{F}_p \\ \bullet I_n \text{ for some } n\in\mathbb{Z}_{>0} \text{ and } (-1)^{n+1}6B(4A^3+27B^2)\theta^{-n}\in\mathbb{F}_p^{\times 2} \\ \bullet I_n^* \text{ for some } n\in\mathbb{Z}_{>0} \text{ and } (-1)^{n+1}6B(4A^3+27B^2)\theta^{-(n+6)}\in\mathbb{F}_p^{\times 2} \\ \bullet III \text{ and } -A\theta^{-1}\notin\mathbb{F}_p^{\times 2} \\ \bullet III^* \text{ and } -A\theta^{-3}\notin\mathbb{F}_p^{\times 2} \end{array} \right\},$$

$$S_2 = \left\{ (A,B) \in \mathcal{E}_p \ : \ \begin{array}{c} E_{A,B} \text{ has reduction type given by one of the following:} \\ \bullet I_0 \text{ and } T^3+AT+B \text{ has 3 roots in } \mathbb{F}_p \\ \bullet I_0^* \text{ and } T^3+A\theta^{-2}T+B\theta^{-3} \text{ has 3 roots in } \mathbb{F}_p \\ \bullet I_n \text{ for some } n\in 2\mathbb{Z}_{>0} \text{ and } 6B\notin\mathbb{F}_p^{\times 2} \text{ and } (4A^3+27B^2)\theta^{-n}\in\mathbb{F}_p^{\times 2} \\ \bullet I_n^* \text{ for some } n\in 2\mathbb{Z}_{>0} \text{ and } 6B\theta^{-3}\notin\mathbb{F}_p^{\times 2} \text{ and } (4A^3+27B^2)\theta^{-(n+6)}\in\mathbb{F}_p^{\times 2} \end{array} \right\},$$

$$S_0 = \mathcal{E}_p \setminus (S_1 \cup S_2).$$

Then by Proposition 3.2.9,

$$\frac{\int_{(A,B)\in\mathcal{E}_p} \#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1} dAdB}{1-p^{-10}} = \sum_{i=0}^{2} 2^{-i} D_p(S_i).$$

The relative densities of these sets can then be computed directly from Lemmas 7.7.3, 7.7.4, and 7.7.5 as

$$\begin{aligned} D_p(S_i) &= \begin{cases} \frac{(p^5+1)p^4(p-1)}{2(p^{10}-1)} + \frac{(p^5+1)p^3(p-1)}{2(p^{10}-1)} + \frac{(p^5+1)p(p-1)}{2(p^{10}-1)} & \text{if } i=1 \\ \frac{(p^5+1)p^3(p-1)(p-2)}{6(p^{10}-1)} + \frac{(p^5+1)p^3(p-1)}{4(p^{10}-1)(p+1)} & \text{if } i=2 \end{cases} \\ &= \begin{cases} \frac{p(p-1)(p^3+p^2+1)(p^5+1)}{2(p^{10}-1)} & \text{if } i=1 \\ \frac{p^3(p-1)(2p^2-2p-1)(p^5+1)}{12(p^{10}-1)(p+1)} & \text{if } i=2 \end{cases} \end{aligned}$$

and so, since $D_p(S_0) = 1-(D_p(S_1)+D_p(S_2))$, the result follows. □

Lemma 7.7.9. *Let $K/\mathbb{Q}$ be a multiquadratic extension. For each prime number $p \geq 5$ such that $K/\mathbb{Q}$ is biquadratic at p,*

$$\frac{\int_{(A,B)\in\mathcal{E}_p} \#\left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p}E_{A,B}(K_w)+2E_{A,B}(\mathbb{Q}_p)}\right)^{-1} dAdB}{1-p^{-10}} = \frac{(p+1)(p-1)(p^4-p^3+p^2-p+1)(5p^5+15p^4+13p^3+9p^2+13p+8)}{8(p^{10}-1)(p+1)}.$$

Proof. Define the following sets

$$S_1 = \left\{ (A,B) \in \mathcal{E}_p \ : \ \begin{array}{c} E_{A,B} \text{ has reduction type given by one of the following:} \\ \bullet I_0 \text{ and } T^3+AT+B \text{ has 1 root in } \mathbb{F}_p \\ \bullet I_0^* \text{ and } T^3+A\theta^{-2}T+B\theta^{-3} \text{ has 1 root in } \mathbb{F}_p \\ \bullet I_n \text{ for some } n\in 2\mathbb{Z}_{>0} \text{ and } -(4A^3+27B^2)p^{-n} \notin \mathbb{F}_p^{\times 2} \\ \bullet I_n^* \text{ for some } n\in 2\mathbb{Z}_{>0} \text{ and } -(4A^3+27B^2)p^{-(n+6)} \notin \mathbb{F}_p^{\times 2} \\ \bullet I_n \text{ or } I_n^* \text{ for some } n\in(2\mathbb{Z}_{>0}-1) \end{array} \right\},$$

$$S_2 = \left\{ (A,B) \in \mathcal{E}_p \ : \ \begin{array}{c} E_{A,B} \text{ has reduction type given by one of the following:} \\ \bullet I_0 \text{ and } T^3+AT+B \text{ has 3 roots in } \mathbb{F}_p \\ \bullet I_0^* \text{ and } T^3+A\theta^{-2}T+B\theta^{-3} \text{ has 3 roots in } \mathbb{F}_p \\ \bullet I_n \text{ for some } n\in 2\mathbb{Z}_{>0} \text{ and } -(4A^3+27B^2)p^{-n} \in \mathbb{F}_p^{\times 2} \\ \bullet I_n^* \text{ for some } n\in 2\mathbb{Z}_{>0} \text{ and } -(4A^3+27B^2)p^{-(n+6)} \in \mathbb{F}_p^{\times 2} \\ \bullet III \text{ or } III^* \end{array} \right\},$$

$$S_0 = \mathcal{E}_p \backslash (S_1 \cup S_2).$$

Then by Proposition 3.2.11,

$$\frac{\int_{(A,B)\in\mathcal{E}_p} \# \left(\frac{E_{A,B}(\mathbb{Q}_p)}{N_{K_w/\mathbb{Q}_p} E_{A,B}(K_w) + 2E_{A,B}(\mathbb{Q}_p)} \right)^{-1} dAdB}{1-p^{-10}} = \sum_{i=0}^{2} 2^{-i} D_p(S_i).$$

The relative densities of these sets can then be computed directly from Lemmas 7.7.3, 7.7.4, and 7.7.5 as

$$\begin{aligned} D_p(S_i) &= \begin{cases} \frac{(p^5+1)p^4(p-1)}{2(p^{10}-1)} + \frac{(p^5+1)(p^3+2p^2)(p-1)^2}{2(p^{10}-1)(p^2-1)} & \text{if } i=1 \\ \frac{(p^5+1)p^3(p-1)(p-2)}{6(p^{10}-1)} + \frac{(p^5+1)p^3(p-1)^2}{2(p^{10}-1)(p^2-1)} + \frac{(p^5+1)(p-1)p}{2(p^{10}-1)} & \text{if } i=2 \end{cases} \\ &= \begin{cases} \frac{p^2(p^5+1)(p-1)(p^3+p^2+p+2)}{2(p^{10}-1)(p+1)} & \text{if } i=1 \\ \frac{(p^5+1)(p-1)p(p^4-p^3+p^2+3p+3)}{6(p^{10}-1)(p+1)} & \text{if } i=2 \end{cases} \end{aligned}$$

and so, since $D_p(S_0) = 1 - (D_p(S_1) + D_p(S_2))$, the result follows. □

§ 7.7.3 | The Archimedean Contribution

We now compute the archimedean factor in Corollary 7.6.3 for the family $\mathcal{F}^{all}$.

Lemma 7.7.10. *Let $K/\mathbb{Q}$ be a multiquadratic field, and $(I,J) \in \mathbb{R}^2$ be elements such that $\Delta'(I,J) \neq 0$. Then*

$$\frac{\#\mathscr{C}(K)(E^{I,J})_\infty}{\#E^{I,J}(\mathbb{R})[2]} = \begin{cases} \frac{1}{4} & \text{if } K \text{ is imaginary and } \Delta'(I,J) > 0 \\ \frac{1}{2} & \text{else} \end{cases}$$

Proof. Let $w \in \Omega_K$ be an archimedean place, and denote $E := E^{I,J}$. Then note that by Lemma 7.6.2

$$\mathscr{C}(K)(E)_\infty = N_{K_w/\mathbb{R}} E(K_w)/2E(\mathbb{R}).$$

From this identity the case that K is real (so $K_w = \mathbb{R}$) is obvious (see e.g. [BK77, Prop 3.7]).

If, on the other hand, K is imaginary then noting that $N_{\mathbb{C}/\mathbb{R}}E(\mathbb{C}) = 2E(\mathbb{R})$ we have

$$\frac{\#(N_{\mathbb{C}/\mathbb{R}}E(\mathbb{C})/2E(\mathbb{R}))}{\#E(\mathbb{R})[2]} = \begin{cases} \frac{1}{2} & \text{if } \Delta'(I,J) < 0 \\ \frac{1}{4} & \text{if } \Delta'(I,J) > 0, \end{cases}$$

as required, since $\Delta'(I,J)$ is the discriminant of the elliptic curve $E^{I,J}$. □

Lemma 7.7.11. *Let $K/\mathbb{Q}$ be a multiquadratic extension. Then we have an equality*

$$\mathscr{M}_\infty^{\mathscr{C}(K)}(\mathcal{F}^{all}; X) = \begin{cases} \frac{1}{2} & \text{if } K \text{ is real,} \\ \frac{9}{20} & \text{if } K \text{ is imaginary.} \end{cases}$$

Proof. If K is real then this is immediate from the definition of $\mathscr{M}_\infty^{\mathscr{C}(K)}(\mathcal{F}^{all}; X)$ and Lemma 7.7.10. If K is imaginary then by Lemma 7.7.10 we have

$$\begin{aligned} \mathscr{M}_\infty^{\mathscr{C}(K)}(\mathcal{F}; X) &= \frac{\int_{\substack{(I,J)\in\mathbb{R}^2 \\ \Delta'(I,J)\neq 0 \\ H(I,J)<X}} \frac{\#\mathscr{C}(K)(E^{I,J})_\infty}{\#E^{I,J}(\mathbb{R})[2]} dIdJ}{\int_{\substack{(I,J)\in\mathbb{R}^2 \\ \Delta'(I,J)\neq 0 \\ H(I,J)<X}} dIdJ} \\ &= \frac{1}{2} - \frac{\int_{\substack{(I,J)\in\mathbb{R}^2 \\ H(I,J)<X \\ \Delta'(I,J)>0}} dIdJ}{4\int_{\substack{(I,J)\in\mathbb{R}^2 \\ \Delta'(I,J)\neq 0 \\ H(I,J)<X}} dIdJ} \\ &= \frac{9}{20}. \end{aligned}$$

where the final equality is obtained via simple minded calculus. □

§ 7.7.4 | The Average Size of the Corestriction Selmer Group

We can now compute the average size of the corestriction Selmer group. We begin with a definition.

Definition 7.7.12. For every multiquadratic extension $K/\mathbb{Q}$ and each prime number $p \geq 5$ define local factors

$$L_p(\mathscr{C}(K)) := \begin{cases} \frac{(p-1)(p^4-p^3+p^2-p+1)(46p^5+62p^4+79p^3+84p^2+84p+48)}{48(p^{10}-1)} & \text{if } K/\mathbb{Q} \text{ is ramified and quadratic at } p, \\ \frac{16p^{11}+16p^{10}+-8p^9+8p^8-8p^7-10p^6-4p^5+7p^4-p^3-8p^2-24p-1}{16(p^{10}-1)(p+1)} & \text{if } K/\mathbb{Q} \text{ is unramified and quadratic at } p, \\ \frac{(p+1)(p-1)(p^4-p^3+p^2-p+1)(5p^5+15p^4+13p^3+9p^2+13p+8)}{8(p^{10}-1)(p+1)} & \text{if } K/\mathbb{Q} \text{ is biquadratic at } p, \\ 1 & \text{if } K/\mathbb{Q} \text{ is totally split at } p. \end{cases}$$

For $p \in \{2,3\}$ we define some 'coarse' local factors

$$L_p(\mathscr{C}(K)) := \begin{cases} 1 & \text{if } K/\mathbb{Q} \text{ is totally split at } p, \\ \frac{1}{2^{2+[K_w:\mathbb{Q}_2]}} & \text{if } p = 2 \text{ and } K/\mathbb{Q} \text{ is not totally split at } p, \\ \frac{1}{4} & \text{if } p = 3 \text{ and } K/\mathbb{Q} \text{ is not totally split at } p. \end{cases}$$

Moreover, define an archimedean factor

$$L_\infty(\mathscr{C}(K)) := \begin{cases} \frac{1}{2} & \text{if } K \text{ is real,} \\ \frac{9}{20} & \text{if } K \text{ is imaginary.} \end{cases}$$

These local factors allow us to, finally, concisely describe the average size of corestriction Selmer groups.

Theorem 7.7.13. *Let $K/\mathbb{Q}$ be a multiquadratic extension, recall Notation 7.7.1, and for concision write*

$$A(K) := \lim_{X\to\infty} \frac{\sum_{\substack{E\in\mathcal{F}^{all} \\ H'(E)<X}} \left(\#\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) - 1\right)}{\sum_{\substack{E\in\mathcal{F}^{all} \\ H'(E)<X}} 1}.$$

Then we have inequalities

$$4 \prod_{v\in\Omega_\mathbb{Q}} L_v(\mathscr{C}(K)) \leq A(K) \leq 4 \prod_{\substack{v\in\Omega_\mathbb{Q} \\ v\nmid 6}} L_v(\mathscr{C}(K)).$$

In particular, if 2 and 3 are totally split in $K/\mathbb{Q}$ we have an equality

$$A(K) = 4 \prod_{v\in\Omega_\mathbb{Q}} L_v(\mathscr{C}(K)).$$

Proof. By Corollary 7.6.3, computing all of the masses except those at 2 and 3 using Lemmas 7.7.7, 7.7.8, 7.7.9, and 7.7.11, we have

$$A(K) = \left(\prod_{p\in\{2,3\}} \mathscr{M}_p^{\mathscr{C}(K)}(\mathcal{F}^{all})\right) 2L_\infty(\mathscr{C}(K)) \prod_{\substack{p\geq 5 \\ \text{prime}}} L_p(\mathscr{C}(K)). \tag{7.6}$$

For $p \in \{2,3\}$, using Lemma 5.3.3 and the fact that if $K/\mathbb{Q}$ is totally split at p then the local norm is the identity map, we know that for every elliptic curve $E/\mathbb{Q}_p$

$$L_p(\mathscr{C}(K)) \leq \frac{1}{\#\left(E(\mathbb{Q}_p)/(N_{K_w/\mathbb{Q}_p}E(K_w) + 2E(\mathbb{Q}_p))\right)} \leq 1.$$

Combining these bounds with Lemma 7.7.6 we obtain

$$\left|\frac{1}{2}\right|_p \cdot L_p(\mathscr{C}(K)) \leq \mathscr{M}_p^{\mathscr{C}(K)}(\mathcal{F}^{all}) \leq \left|\frac{1}{2}\right|_p.$$

Combining with the identity (7.6) we obtain the claimed result. □

Remark 7.7.14. It is clear that the 'coarse' local factors L_2 and L_3 are approximations of the correct factors for $\mathscr{M}_2^{\mathscr{C}(K)}$ and $\mathscr{M}_3^{\mathscr{C}(K)}$. Broadly, the only ingredients going into computing the local factors L_p for $p \geq 5$ was the studious account of local norm indices at p in §3.2, which itself only required performing Tate's algorithm carefully. Certainly, for $p \in \{2,3\}$ one could go through Tate's algorithm, compute the corresponding results

to those in §3.2, and then find the correct factors L_2 and L_3. However, we feel that both the reader and the author have suffered enough already, and leave this as an exercise for a reader who has an exceptionally long train journey to pass.

We state, as corollary, the bounds that this result leaves us with for the average dimension of corestriction Selmer groups in the natural ordering on elliptic curves.

Corollary 7.7.15 (see also Theorem 6.5.4)**.** *Let $K/\mathbb{Q}$ be a multiquadratic extension, then*

$$\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])}{\#\mathcal{E}(X)} \leq \left(\frac{27}{4}\right)^{5/6} \left(4 \prod_{\substack{v\in\Omega_{\mathbb{Q}} \\ v\nmid 6}} L_v(\mathscr{C}(K)) \right).$$

Proof. Using the inequality $r \leq 2^r - 1$, by Theorem 7.7.13 and Example 6.1.2 we know that for $\mathbf{C} = (\frac{1}{\sqrt[3]{4}}, \frac{1}{\sqrt{27}})$ we have

$$\begin{aligned} &\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])}{\#\mathcal{E}^{\mathbf{C}}(X)} \\ &\leq \limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(X)} \left(\#\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2]) - 1\right)}{\#\mathcal{E}^{\mathbf{C}}(X)} \\ &\leq 4 \prod_{\substack{v\in\Omega_{\mathbb{Q}} \\ v\nmid 6}} L_v(\mathscr{C}(K)) \end{aligned}$$

Now using the clear inclusions

$$\mathcal{E}^{\mathbf{C}}(4X) \subseteq \mathcal{E}(X) \subseteq \mathcal{E}^{\mathbf{C}}(27X),$$

we obtain

$$\begin{aligned} &\limsup_{X\to\infty} \frac{\sum_{(A,B)\in\mathcal{E}(X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])}{\#\mathcal{E}(X)} \\ &\leq \limsup_{X\to\infty} \frac{\#\mathcal{E}^{\mathbf{C}}(27X)}{\#\mathcal{E}^{\mathbf{C}}(4X)} \frac{\sum_{(A,B)\in\mathcal{E}^{\mathbf{C}}(27X)} \dim \mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])}{\#\mathcal{E}^{\mathbf{C}}(27X)} \\ &\leq \left(\frac{27}{4}\right)^{5/6} \left(4 \prod_{\substack{v\in\Omega_{\mathbb{Q}} \\ v\nmid 6}} L_v(\mathscr{C}(K)) \right) \end{aligned}$$

where the final inequality uses that $\#\mathcal{E}^{\mathbf{C}}(X) \sim \frac{4C_1C_2X^{5/6}}{\zeta(10)}$ and the inequality from Theorem 7.7.13 above. □

Appendix A

Tate's Algorithm

Let F be the completion of a number field at a non-archimedean place with residue characteristic $p \geq 5$. Let $\mathcal{O}_F$, v_F and k_F be the ring of integers, normalised valuation, and residue field. Let $E : y^2 = x^3 + Ax + B$ be a minimal integral model for an elliptic curve defined over F (as in Definition 3.2.2), and write $P_E(T) := T^3 + A\pi_F^{-2}T + B\pi_F^{-3}$.

In Table A.1 we present the well known summary of the outcome of Tate's algorithm (as presented in [Sil94]) in this setting.

Kodaira Type	**Subtype**	**c(E/F)**	**condition**
I_0		1	$v_F(4A^3+27B^2)=0$
I_n	split	n	$v_F(AB)=0$, $v_F(4A^3+27B^2)=n$ and $6B\in k_F^{\times 2}$
	nonsplit, n even	2	$v_F(AB)=0$, $v_F(4A^3+27B^2)=n$ and $6B\notin k_F^{\times 2}$
	nonsplit, n odd	1	$v_F(AB)=0$, $v_F(4A^3+27B^2)=n$ and $6B\notin k_F^{\times 2}$
II		1	$v_F(A)\geq 1$ and $v_F(B)=1$
III		2	$v_F(A)=1$ and $v_F(B)\geq 2$
IV	split	3	$v_F(A)\geq 2$, $v_F(B)=2$ and $B\pi_F^{-2}\in k_F^{\times 2}$
	nonsplit	1	$v_F(A)\geq 2$, $v_F(B)=2$ and $B\pi_F^{-2}\notin k_F^{\times 2}$
I_0^*	nonsplit	1	$v_F(A)\geq 2$, $v_F(B)\geq 3$, $v_F(4A^3+27B^2)=6$, and $\#\{\alpha\in k_F \ : \ P_E(\alpha)=0\}=0$
	partially split	2	$v_F(A)\geq 2$, $v_F(B)\geq 3$, $v_F(4A^3+27B^2)=6$, and $\#\{\alpha\in k_F \ : \ P_E(\alpha)=0\}=1$
	completely split	4	$v_F(A)\geq 2$, $v_F(B)\geq 3$, $v_F(4A^3+27B^2)=6$, and $\#\{\alpha\in k_F \ : \ P_E(\alpha)=0\}=3$
I_n^*	split, n even	4	$v_F(A)=2$, $v_F(B)=3$, $v_F(4A^3+27B^2)=6+n$ and $-(4A^3+27B^2)\pi_F^{-(6+n)}\in k_F^{\times 2}$
	nonsplit, n even	2	$v_F(A)=2$, $v_F(B)=3$, $v_F(4A^3+27B^2)=6+n$ and $-(4A^3+27B^2)\pi_F^{-(6+n)}\notin k_F^{\times 2}$
	split, n odd	4	$v_F(A)=2$, $v_F(B)=3$, $v_F(4A^3+27B^2)=6+n$ and $6B(4A^3+27B^2)\pi_F^{-(9+n)}\in k_F^{\times 2}$
	nonsplit, n odd	2	$v_F(A)=2$, $v_F(B)=3$, $v_F(4A^3+27B^2)=6+n$ and $6B(4A^3+27B^2)\pi_F^{-(9+n)}\notin k_F^{\times 2}$
IV^*	split	3	$v_F(A)\geq 3$, $v_F(B)=4$ and $B\pi_F^{-4}\in k_F^{\times 2}$
	nonsplit	1	$v_F(A)\geq 3$, $v_F(B)=4$ and $B\pi_F^{-4}\notin k_F^{\times 2}$
III^*		2	$v_F(A)=3$ and $v_F(B)\geq 5$
II^*		1	$v_F(A)\geq 4$ and $v_F(B)=5$

Table A.1: Tate's Algorithm for a minimal model in residue characteristic at least 5

Appendix B

Corestriction Selmer Group Computations

The explicit description of the corestriction Selmer group in §2.3 (originally due to Kramer for quadratic extensions [Kra81]), along with the explicit realisation of the twisted Kummer images in Chapter 7, allows us to compute corestriction Selmer groups by adapting current methods for 2-Selmer groups. Work of Kramer [Kra81] shows that the image of the norm from $\mathrm{Sel}_2(E/K)$ inside of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$ is precisely the kernel of the Cassels–Tate pairing restricted to the corestriction Selmer group, so we are also able to compute the image of the norm.

In §B.1 we present the outcome of some such computations. We count the dimension of $\mathrm{Sel}_{\mathscr{C}(K)}(E/\mathbb{Q})$ for each quadratic field $K = \mathbb{Q}(\sqrt{d})$ with d squarefree of absolute value at most 20, and for each elliptic curve $E/\mathbb{Q}$ with height at most 10^7. As we discuss in §1.4.3, the data seems to suggest that the statistical behaviour of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$ is similar to that of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$. In particular it seems likely that its average size will also be positive, and so $\mathrm{Sel}_2(E/K)$ would have nontrivial $\mathrm{Gal}(K/\mathbb{Q})$-action for a positive proportion of elliptic curves (ordered by height).

We present the code which was used to compute our data in §B.2.

§ B.1 | Corestriction Selmer Group Data

Selmer structures over $\mathbb{Q}(\sqrt{d})$ for all elliptic curves of height at most 10^7						
Dimension	0	1	2	3	4	5
Count of $\mathrm{Sel}_2(E/\mathbb{Q})$	702001	1251306	654229	109166	4378	16
$K = \mathbb{Q}(\sqrt{-19})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1475870	961149	254582	28526	967	2
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1550766	976689	180331	12987	322	1
$K = \mathbb{Q}(\sqrt{-17})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1747192	801070	158007	14362	465	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1796425	808795	109101	6637	138	0

Dimension	0	1	2	3	4	5
$K = \mathbb{Q}(\sqrt{-15})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1570766	899551	225201	24705	869	4
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1639053	911830	157352	12426	431	4
$K = \mathbb{Q}(\sqrt{-14})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1907473	689456	114673	9211	283	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1944670	694638	77659	4029	100	0
$K = \mathbb{Q}(\sqrt{-13})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1792345	769029	146364	12999	357	2
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1838316	775987	100630	6043	120	0
$K = \mathbb{Q}(\sqrt{-11})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1428843	989455	271021	30742	1031	4
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1508209	1005984	192353	14215	333	2
$K = \mathbb{Q}(\sqrt{-10})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1935023	667272	109823	8753	225	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1971005	672187	73990	3838	76	0
$K = \mathbb{Q}(\sqrt{-7})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1271553	1066312	338525	43089	1612	5
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1365659	1086773	245335	22629	696	4
$K = \mathbb{Q}(\sqrt{-6})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1877363	708409	124700	10358	265	1
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1919689	714137	82522	4630	117	1
$K = \mathbb{Q}(\sqrt{-5})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1702623	832722	169696	15602	453	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1756508	841140	116106	7184	158	0
$K = \mathbb{Q}(\sqrt{-3})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1364074	1012410	306132	37128	1346	6
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1463054	1033708	207987	15831	511	5
$K = \mathbb{Q}(\sqrt{-2})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1567855	921926	210267	20399	648	1
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1634648	933059	143913	9266	209	1
$K = \mathbb{Q}(\sqrt{-1})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1356169	1038346	291823	33529	1225	4
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1448835	1056667	200023	15211	359	1
$K = \mathbb{Q}(\sqrt{2})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1606088	894675	200316	19387	629	1
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1671520	905625	135324	8437	189	1
$K = \mathbb{Q}(\sqrt{3})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1695879	830127	177373	17207	509	1
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1756483	839827	117070	7507	208	1

Dimension	0	1	2	3	4	5
$K = \mathbb{Q}(\sqrt{5})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1431466	982759	274044	31711	1113	3
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1517338	1000640	188929	13830	356	3
$K = \mathbb{Q}(\sqrt{6})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1886698	700868	122974	10269	286	1
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1928753	706561	81084	4576	121	1
$K = \mathbb{Q}(\sqrt{7})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1730907	810900	163284	15505	500	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1783613	819391	110948	7014	130	0
$K = \mathbb{Q}(\sqrt{10})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1911182	686194	114457	9025	238	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1948266	691140	77523	4079	88	0
$K = \mathbb{Q}(\sqrt{11})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1776615	780860	149746	13502	371	2
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1823772	788101	102840	6263	120	0
$K = \mathbb{Q}(\sqrt{13})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1453037	974343	263061	29687	963	5
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1531146	990412	185586	13620	329	3
$K = \mathbb{Q}(\sqrt{14})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1942107	662161	108003	8556	269	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1977786	667007	72504	3710	89	0
$K = \mathbb{Q}(\sqrt{15})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1990830	621291	100335	8359	281	0
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	2026192	626247	65159	3403	95	0
$K = \mathbb{Q}(\sqrt{17})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1316558	1042928	320321	39833	1451	5
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1403336	1061659	234361	21103	633	4
$K = \mathbb{Q}(\sqrt{19})$						
Count of $\mathrm{Sel}_{\mathscr{C}(K)}(\mathbb{Q}, E[2])$	1757324	795545	154170	13667	389	1
Count of $N_{K/\mathbb{Q}}\mathrm{Sel}_2(E/K)$	1804416	802711	107345	6501	122	1

Table B.1: The count of curves of height at most 10^7 with the size of corestriction Selmer group or norm of Selmer group from a fixed quadratic field

§ B.2 | Corestriction Selmer Group Code

Below is the code, written for the magma computer algebra system [BCP97], which we use to compute the data in the previous section.

```
function IsInCoresSubgroup(C, selmer_primes_for_E : quad_twists := [1])
// Input:
```

```
//                  C: Hyperelliptic curve representing a class in the
//                     two selmer group of an elliptic curve E
// selmer_primes_for_E: finite set of primes for which the 2-selmer
//                     conditions of E above are not necessarily the
//                     unramified condition
//         quad_twists: a set of elements in the mult group of the ground
//                     field of C
// Output:
//             boolean: whether all of the quadratic twists of C by
//                     elements in quad_twists are everywhere locally soluble
////////////////////////////////////////////////////////////////////////
    for D in quad_twists do
        f_D := D*HyperellipticPolynomials(C);
        for p in selmer_primes_for_E cat PrimeFactors(D) do
            if not HasPoint(f_D, 2, p) then return false; end if;
        end for;
    end for;
    return true;
end function;

function CoresSelmer(E, quad_discs)
// Input:
//              E: Elliptic curve.
//     quad_discs: A set for which K is the field obtained from Q by adjoining
//                 the squareroots found within.
// Output:
//          AbGrp: The Corestriction Selmer group associated to E and the
//                 multiquadratic field K as a subgroup of the two Selmer
//                 group of E/Q.
//          AbGrp: The two Selmer group of E/Q.
//            map: map from the two selmer group to the etale algebra used in
//                 computations of two selmer groups
////////////////////////////////////////////////////////////////////////
    TwoSel, mm := TwoSelmerGroup(E);
    m := Inverse(mm);
    selmer_primes_for_E :=
        [p : p in BadPrimes(E) | p ne 2 and IsEven(TamagawaNumber(E, p))]
        cat [2];
    quad_twists := [&*Q:Q in &join[Subsequences(Set(quad_discs), k) : k in
    ↪ [0..#quad_discs]]];
    cores_elts := [];
    for s in TwoSel do
        if IsInCoresSubgroup(TwoCover(m(s)), selmer_primes_for_E: quad_twists :=
        ↪ quad_twists) then
            Append(~cores_elts, s);
        end if;
    end for;
    return sub<TwoSel|cores_elts>, TwoSel, m;
end function;
```

```
50
51
52  function NormOfSelmer(E, D)
53  // Input:
54  //              E: Elliptic curve.
55  //              D: A squarefree integer
56  // Output:
57  //          AbGrp: The norms from the two Selmer group of E/Q(sqrt(d))
58  //          AbGrp: The Corestriction Selmer group associated to E and the
59  //                 quadratic field Q(sqrt(d)) as a subgroup of the two Selmer
60  //                 group of E/Q.
61  //          AbGrp: The two Selmer group of E/Q.
62  //            map: map from the two selmer group to the etale algebra used in
63  //                 computations of two selmer groups
64  ////////////////////////////////////////////////////////////////////////
65      Cores, TwoSel, m := CoresSelmer(E, [D]);
66      NTwoSel := [];
67      for g in Cores do
68          if g eq Cores.0 then continue; end if;
69          Cg := TwoCover(m(g));
70          inker := true;
71          for h in Cores do
72              if h eq Cores.0 then continue; end if;
73              if not CasselsTatePairing(Cg, TwoCover(m(h))) eq 0 then
74                  inker := false;
75                  continue;
76              end if;
77          end for;
78          if inker then Append(~NTwoSel, g); end if;
79      end for;
80      return sub<Cores|NTwoSel>, Cores, TwoSel, m;
81  end function;
```

Bibliography

[Alp86] J. L. Alperin, *Local representation theory*, Cambridge Studies in Advanced Mathematics, vol. 11, Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups. MR860771 ↑1.2.3, 1.4.3, 1.5.2, 1.5.1, 2.2.3, 2.3.2

[AW67] M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 94–115. MR0219512 ↑2.3.4

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). MR1484478 ↑5.5.3, B.2

[Bil95] P. Billingsley, *Probability and measure*, Third, Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, Inc., New York, 1995. A Wiley-Interscience Publication. MR1324786 ↑4.2.2

[BK77] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44** (1977), no. 4, 715–743. MR457453 ↑7.7.3

[Bra14] J. Brau, *Selmer groups of elliptic curves in degree p extensions*, arXiv:1401.3304 [math.NT] (2014). ↑2.3.4

[BS13] M. Bhargava and A. Shankar, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, arXiv:1312.7859v1 [math.NT] (2013). ↑1.1.6, 1.1.7, 1.3.6, 5, 5.2, 5.2.3, 5.2.3, 5.3.10

[BS15a] ———, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242. MR3272925 ↑1.1.6, 1.5.4, 5.2.3, 5.2.3, 6, 7, 7.2.2, 7.2.4, 7.2.5, 7.2.6, 7.2.7, 7.2.8, 7.4, 7.4.1, 7.4.1, 7.4.4, 7.4.1, 7.4.11, 7.4.13, 7.4.14, 7.4.15, 7.4.16, 7.4.17, 7.4.18, 7.5.1, 7.5.6, 7.5.2, 7.5.2, 7.5.2

[BS15b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621. MR3275847 ↑1.1.6, 5, 5.2, 5.2.3, 5.2.3

[BSD63] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. Reine Angew. Math. **212** (1963), 7–25. MR146143 ↑7, 7.2, 7.2.3, 7.2.3, 7.2.7

[BSS21] M. Bhargava, A. Shankar, and A. Swaminathan, *The second moment of the size of the 2-selmer group of elliptic curves*, arXiv:2110.09063v1 [math.NT] (2021). ↑1.1.2

[CF09] J. E. Cremona and T. A. Fisher, *On the equivalence of binary quartics*, J. Symbolic Comput. **44** (2009), no. 6, 673–682. MR2509048 ↑7.2, 7.2.2, 7.2.3, 7.2.3

[CJ20] P. J. Cho and K. Jeong, *On the distribution of analytic ranks of elliptic curves*, arXiv:2003.09102v1 [math.NT] (2020). ↑5.3.2, 6.1.2

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 1984, pp. 33–62. MR756082 ↑1

[CR81] C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I* (1981), xxi+819. With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication. MR632548 ↑4.3.3

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, Second, Cambridge University Press, Cambridge, 1997. MR1628193 ↑7, 7.2, 7.2.3

[Cre99] ———, *Reduction of binary cubic and quartic forms*, LMS J. Comput. Math. **2** (1999), 64–94. MR1693411 ↑7.2

[CS20] J. E. Cremona and M. Sadek, *Local and global densities for weierstrass models of elliptic curves*, arXiv:2003.08454v2 [math.NT] (2020). ↑6.1.2

[Duk97] W. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818. MR1485897 ↑1.3.6, 5.1, 5.1, 5.1.1, 5.3.3

[EK40] P. Erdös and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742. MR2374 ↑1.2.1

[FK07] É. Fouvry and J. Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), no. 3, 455–513. MR2276261 ↑(document), 1.5.2, 4, 4.5.4, 4.5.6, 4.5.6, 4.5.6, 4.5.6, 4.5.6, 4.5.6, 4.5.6, 4.5.6, 4.5.6

[FK10] ———, *On the negative Pell equation*, Ann. of Math. (2) **172** (2010), no. 3, 2035–2104. MR2726105 ↑4.5.6

[Gal73] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972), 1973, pp. 91–101. MR0332694 ↑5.1.1

[Gre01] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), 2001, pp. 407–464. MR1860044 ↑1.3.16

[GS07] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac theorem*, Equidistribution in number theory, an introduction, 2007, pp. 15–27. MR2290492 ↑4.2.2

[Har20] D. Harari, *Galois cohomology and class field theory*, Universitext, Springer, Cham, 2020. Translated from the 2017 French original by Andrei Yafaev. MR4174395 ↑2.1.2

[HB93] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195. MR1193603 ↑(document), 1.1.1, 1.5.2, 4, 4.5.4

[HB94] ———, *The size of Selmer groups for the congruent number problem.II*, Invent. Math. **118** (1994), no. 2, 331–370. With an appendix by P. Monsky. MR1292115 ↑(document), 1.1.1, 1.5.2, 4, 4.5.4

[HB95] ———, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), no. 3, 235–275. MR1347489 ↑4.5.6

[HR00] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n [Quart. J. Math.* **48** *(1917), 76–92]*, Collected papers of Srinivasa Ramanujan, 2000, pp. 262–275. MR2280878 ↑4.5.6

[Hux68] M. N. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika **15** (1968), 178–187. MR237455 ↑5.1.1

[Jon10] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570. MR2563740 ↑5.1.2

[Kan13] D. Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory **7** (2013), no. 5, 1253–1279. MR3101079 ↑1.1.1, 1.1.2, 4.2.2, 4.3.2, 4.3.2

[Kat04] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, 2004, pp. ix, 117–290. Cohomologies p-adiques et applications arithmétiques. III. MR2104361 ↑1.3.16

[KLO16] Z. Klagsbrun and R. J. Lemke Oliver, *The distribution of 2-Selmer ranks of quadratic twists of elliptic curves with partial two-torsion*, Mathematika **62** (2016), no. 1, 67–78. MR3430377 ↑(B)

[KMR14] Z. Klagsbrun, B. Mazur, and K. Rubin, *A Markov model for Selmer ranks in families of twists*, Compos. Math. **150** (2014), no. 7, 1077–1106. MR3230846 ↑(C)

[Kra81] K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. MR597871 ↑1.2.2, 2, 2.2, 2.2.3, 2.3.2, 2.3.10, 2.3.11, 2.3.13, 3.1, 4.1, 4.2.5, 6.4.1, B

[KT82] K. Kramer and J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), no. 3, 307–352. MR664648 ↑1.4.3, 4.2.5

[LO77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), 1977, pp. 409–464. MR0447191 ↑4.2.2, 4.5.2

[Lor11] D. Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier (Grenoble) **61** (2011), no. 5, 1995–2037 (2012). MR2961846 ↑3.2.2

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR444670 ↑2.2.1, 2.2.9, 4.2.1, 5.3.2, 7.6

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287 ↑4.3.3

[Maz84] ———, *Modular curves and arithmetic*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 1984, pp. 185–211. MR804682 ↑1.3.6

[Mil72] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR330174 ↑5.2.1, 5.2.2

[MP22] A. Morgan and R. Paterson, *On 2-Selmer groups of twists after quadratic extension*, J. Lond. Math. Soc. (2) **105** (2022), no. 2, 1110–1166. MR4400944 ↑1.1.1, 1.2, 1.3.3, 2.2, 2.3.4, 4

[MR04] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96. MR2031496 ↑2.1

[MR07] ———, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612. MR2373150 ↑4.1, 5.2, 5.2.2, 5.2.2, 5.2.2, 5.2.8

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. MR2660452 ↑4.1

[MRS07] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), no. 1, 419–438. MR2331769 ↑1.5.2, 3.2.2, 5.2.1, 5.2.3, 5.2.2, 5.2.5, 5.2.6, 5.2.2

[Neu13] J. Neukirch, *Class field theory*, Springer, Heidelberg, 2013. The Bonn lectures, edited and with a foreword by Alexander Schmidt, Translated from the 1967 German original by F. Lemmermeyer and W. Snyder, Language editor: A. Rosenschon. MR3058613 ↑2.2.1, 2.3.2, 5.2.2

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Second, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 ↑2.1

[Pat21] R. Paterson, *The failure of Galois descent for p-Selmer groups of elliptic curves*, arXiv:2106.02486v1 [math.NT] (2021), submitted. ↑1.3, 2.2, 5

[PPVW19] J. Park, B. Poonen, J. Voight, and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903. MR3985613 ↑1.3.6

[PR12] B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269. MR2833483 ↑1, 2.2.1, 2.2.1, 5.2.11

[Roh84] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423. MR735333 ↑1.3.16

[Ros41] B. Rosser, *Explicit bounds for some functions of prime numbers*, Amer. J. Math. **63** (1941), 211–232. MR3018 ↑6.1.3

[SC02] M. Stoll and J. E. Cremona, *Minimal models for 2-coverings of elliptic curves*, LMS J. Comput. Math. **5** (2002), 220–243. MR1951757 ↑7.2

[Sch95] E. F. Schaefer, 2*-descent on the Jacobians of hyperelliptic curves*, J. Number Theory **51** (1995), no. 2, 219–232. MR1326746 ↑7.2.3

[Sch96] ———, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114. MR1370197 ↑3.2.2

[SD08] P. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Cambridge Philos. Soc. **145** (2008), no. 3, 513–526. MR2464773 ↑1.1.1

[Ser79] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 ↑7.2.3

[Shi80] P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. **313** (1980), 161–170. MR552470 ↑4.5.2

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑1.1.5, 2.2.1, 2.3.1, 3.2.2, 3.2.2, 4.4.2, 5.3.2, 7, 7.1.7, 7.1.8, 7.7.2

[Sil94] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368 ↑1.4.3, 1.6, 3.1, 3.1, A

[Smi17] A. Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325v2 [math.NT] (2017). ↑1.1.4

[Smi22] ———, *The distribution of* ℓ^∞*-selmer groups in degree* ℓ *twist families*, arXiv:2207.05674v1 [math.NT] (2022). ↑1.1.4

[Ste18] P. Stevenhagen, *Redei reciprocity, governing fields, and negative pell*, Preprint, arXiv:1806.06250 (2018). ↑4.6.2, 4.6.2, 4.6.2

[Sto06] M. Stoll, *Descent on elliptic curves*, arXiv:math (2006). ↑7.1.2, 7.1.11, 7.1.13

[Tat63] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), 1963, pp. 288–295. MR0175892 ↑2.3.1

[Was97a] L. C. Washington, *Galois cohomology*, Modular forms and Fermat's last theorem (Boston, MA, 1995), 1997, pp. 101–120. MR1638477 ↑2.1, 2.1

[Was97b] ———, *Introduction to cyclotomic fields*, Second, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575 ↑1.3.15

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR1333035 ↑2.1

[XZ08] M. Xiong and A. Zaharescu, *Distribution of Selmer groups of quadratic twists of a family of elliptic curves*, Adv. Math. **219** (2008), no. 2, 523–553. MR2435648 ↑(B)

[Zyw10] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826. MR2721742 ↑5.1, 5.1.2, 5.1.3, 5.3.3