

On 2-Selmer groups of twists after quadratic extension

Adam Morgan¹ | Ross Paterson²

¹ Max-Planck-Institut für Mathematik,
Bonn, Germany

² School of Mathematics and Statistics,
University of Glasgow, University Place,
Glasgow, UK

Correspondence

Ross Paterson, School of Mathematics
and Statistics, University of Glasgow,
University Place, Glasgow G12 8QQ, UK.
Email: r.paterson.2@research.gla.ac.uk

Funding information

Max-Planck-Institut für Mathematik in
Bonn; Carnegie Trust for the Universities
of Scotland

Abstract

Let E/\mathbb{Q} be an elliptic curve with full rational 2-torsion. As d varies over squarefree integers, we study the behaviour of the quadratic twists E_d over a fixed quadratic extension K/\mathbb{Q} . We prove that for 100% of twists the dimension of the 2-Selmer group over K is given by an explicit local formula, and use this to show that this dimension follows an Erdős–Kac type distribution. This is in stark contrast to the distribution of the dimension of the corresponding 2-Selmer groups over \mathbb{Q} , and this discrepancy allows us to determine the distribution of the 2-torsion in the Shafarevich–Tate groups of the E_d over K also. As a consequence of our methods we prove that, for 100% of twists d , the action of $\text{Gal}(K/\mathbb{Q})$ on the 2-Selmer group of E_d over K is trivial, and the Mordell–Weil group $E_d(K)$ splits integrally as a direct sum of its invariants and anti-invariants. On the other hand, we give examples of thin families of quadratic twists in which a positive proportion of the 2-Selmer groups over K have non-trivial $\text{Gal}(K/\mathbb{Q})$ -action, illustrating that these previous results are genuinely statistical phenomena.

MSC (2020)

11G05 (primary), 11G10, 11N45, 14H52 (secondary)

Contents

1. INTRODUCTION	1111
2. NOTATION AND CONVENTIONS	1116
3. SELMER STRUCTURES	1117
4. 2-SELMER GROUPS OVER QUADRATIC EXTENSIONS.	1119
5. QUADRATIC TWISTS AND A DISTRIBUTION RESULT	1128
6. MAIN RESULTS	1133
7. EXPLICIT LOCAL CONDITIONS FOR FULL 2-TORSION	1138
8. PROOF OF THEOREM 6.1.	1141
9. PRIME TWISTS OF THE CONGRUENT NUMBER CURVE	1156
ACKNOWLEDGEMENTS.	1164
REFERENCES.	1165

1 | INTRODUCTION

Let E/\mathbb{Q} be an elliptic curve with $E[2] \subseteq E(\mathbb{Q})$, and consider the family of quadratic twists of E over \mathbb{Q} :

$$\{E_d : d \in \mathbb{Z} \text{ squarefree}\}.$$

Let K/\mathbb{Q} be a quadratic extension. In this paper, as d varies we study the 2-Selmer groups $\text{Sel}^2(E_d/K)$ of E_d over K .

1.1 | Erdős–Kac for 2-Selmer

Our first result, strongly reminiscent of the Erdős–Kac theorem [6], shows that the distribution of the quantity

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

is standard normal. That is, we have the following theorem.

Theorem 1.1 (Corollary 6.6). *For every $z \in \mathbb{R}$ we have*

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

One immediate consequence is that, for any fixed real number z , the proportion of $|d| \leq X$ for which $\dim \text{Sel}^2(E_d/K)$ is smaller than z tends to 0 as X tends to infinity. We present this as Corollary 5.11.

By contrast, if we assume that E has no cyclic 4-isogeny defined over \mathbb{Q} , it is a result of Kane [16], building on work of Heath–Brown [13] and Swinnerton–Dyer [36], that for any fixed integer

$n \geq 2$ a positive proportion of twists d have $\dim \text{Sel}^2(E_d/\mathbb{Q})$ equal to n . Thus, Theorem 1.1 shows that the groups $\text{Sel}^2(E_d/K)$ 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 1.1 remains true when $\dim \text{Sel}^2(E_d/K)$ is replaced by $\dim \text{III}(E_d/K)[2]$ in the statement. We present this alternative perspective as Corollary 6.7.

The distribution in Theorem 1.1 does show up in a slightly different setting over \mathbb{Q} however, and is the same form as that appearing in work of Klagsbrun–Lemke Oliver [18] and Xiong–Zaharescu [39] concerning the distribution of 2-isogeny Selmer groups in quadratic twist families of certain elliptic curves. We discuss a precise analogy explaining this similarity in Section 1.3.

1.2 | Structural results for 100% of twists

The growth of the 2-Selmer group when passing from \mathbb{Q} to K apparent in Theorem 1.1 can be explained by work of Kramer [20]. Write $G = \text{Gal}(K/\mathbb{Q})$ for the Galois group of K over \mathbb{Q} . For any elliptic curve E'/\mathbb{Q} , the 2-Selmer group of E' over K is naturally a G -module. Roughly speaking, the work of Kramer identifies a quotient of the invariant subgroup $\text{Sel}^2(E'/K)^G$ whose dimension is controlled by purely local invariants (this is implicit in [20, Theorem 1], see also Lemmas 4.5 and 4.6). 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.

To prove Theorem 1.1 we study, as d varies, the discrepancy between the ‘systematic’ part of the 2-Selmer group $\text{Sel}^2(E_d/K)$ alluded to above, and the full 2-Selmer group. Ultimately, Theorem 1.1 is a consequence of the following result, giving a precise description of the full 2-Selmer group for 100% of twists.

Notation 1.2. For each place v of \mathbb{Q} , and any place w of K extending v , define the local norm map

$$N_{K_w/\mathbb{Q}_v} : E(K_w) \longrightarrow E(\mathbb{Q}_v)$$

by the formula

$$N_{K_w/\mathbb{Q}_v}(P) = \sum_{\sigma \in \text{Gal}(K_w/\mathbb{Q}_v)} \sigma(P).$$

Theorem 1.3 (Corollary 6.4). *For 100% of squarefree d ordered by absolute value, the $\text{Gal}(K/\mathbb{Q})$ -action on $\text{Sel}^2(E_d/K)$ is trivial, and we have*

$$\dim \text{Sel}^2(E_d/K) = -2 + \sum_{v \text{ place of } \mathbb{Q}} \dim E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E_d(K_w). \quad (1.4)$$

Here N_{K_w/\mathbb{Q}_v} is defined as in Notation 1.2. Since $E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E_d(K_w)$ is trivial if v splits in K , the right-hand side of (1.4) does not depend on the choice of $w \mid v$.

Remark 1.5. In Section 5, we study the behaviour of the right-hand side of (1.4). 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 $\text{Sel}^2(E_d/K)$ as d varies. In particular, provided that $\mathbb{Q}(E[2]) \cap K = \mathbb{Q}$ we show in

Corollary 5.11 that for any fixed real number z , the dimension of $\text{Sel}^2(E_d/K)$ exceeds z for 100% of twists d . For the remainder of the introduction however, we continue to assume $E[2] \subseteq E(\mathbb{Q})$.

Remark 1.6. The statement of Theorem 1.3 is very reminiscent of a recent result of Fouvry–Koymans–Pagano [7]. There it is shown that, for 100% of odd positive squarefree integers n , the class group of the Dirichlet biquadratic field $\mathbb{Q}(\sqrt{n}, i)$ has 4-rank equal to $\omega_3(n) - 1$, where $\omega_3(n)$ is the number of primes dividing n that are congruent to 3 modulo 4 (that is, are inert in $\mathbb{Q}(i)$). The similarity with the statement of Theorem 1.3 is made apparent by Proposition 5.6. This can be viewed as an instance of the known analogy between 4-ranks of class groups and 2-Selmer ranks of elliptic curves apparent in the works of Heath–Brown [12, 13] and Fouvry–Klüners [8], and extended to higher 2-power ranks in the recent work of Smith [34].

It is natural to ask if the description in Theorem 1.3 simply holds for *all* d . This is, however, not the case. We discuss examples where the Galois action is non-trivial in Section 1.4.

Since the group $E_d(K)/2E_d(K)$ sits inside $\text{Sel}^2(E_d/K)$, we can deduce some consequences for Mordell–Weil groups from the above results. Specifically, for a squarefree integer d , write $\Lambda(E_d/\mathbb{Q})$ for the finite rank free \mathbb{Z} -module given by the quotient of $E_d(\mathbb{Q})$ by its torsion subgroup:

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

We view this as a G -module with trivial action. Write $\Lambda(E_d/\mathbb{Q})(-1)$ for the G -module with underlying abelian group $\Lambda(E_d/\mathbb{Q})$ on which the generator of G acts as multiplication by -1 . Further, write $K = \mathbb{Q}(\sqrt{\theta})$. We have the following result, giving a complete description of the G -module structure of $E_d(K)$ for 100% of d .

Theorem 1.7 (Corollary 6.13). *For 100% of squarefree d ordered by absolute value, we have an isomorphism of $\mathbb{Z}[G]$ -modules*

$$E_d(K) \cong (\mathbb{Z}/2\mathbb{Z})^2 \oplus \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1), \quad (1.8)$$

where here $(\mathbb{Z}/2\mathbb{Z})^2$ carries trivial G -action.

1.3 | Twists of the Weil restriction of scalars

Write $A = \text{Res}_{K/\mathbb{Q}} E$ for the Weil restriction of scalars of E from K to \mathbb{Q} . This is a principally polarised abelian surface over \mathbb{Q} . For each squarefree integer d we have (see Lemma 4.20)

$$\text{Sel}^2(E_d/K) \cong \text{Sel}^2(A_d/\mathbb{Q}).$$

In particular, we can view Theorem 1.1 as giving the distribution of 2-Selmer groups in the quadratic twist family over \mathbb{Q} of the abelian surface A . We state this formally as Theorem 6.15.

It is also possible to use this perspective to draw parallels between our work and existing work in the literature. Specifically, we show in Section 4.3 that for each d , the twist A_d admits an isogeny $\phi_d : A_d \rightarrow E_d \times E_{d\theta}$ whose kernel is a subgroup of $A_d[2]$. The order of the Selmer group $\text{Sel}^{\phi_d}(A_d/\mathbb{Q})$ associated to ϕ_d is then, up to a quantity bounded independent of d , a lower bound

for the size of the Selmer group $\text{Sel}^2(A_d/\mathbb{Q})$. In turn, writing $\widehat{\phi_d}$ for the dual isogeny, a lower bound for the size of $\text{Sel}^{\phi_d}(A_d/\mathbb{Q})$ is given by the *Tamagawa ratio*

$$\mathcal{T}(\phi_d) = \frac{|\text{Sel}^{\phi_d}(A_d/\mathbb{Q})|}{|\text{Sel}^{\widehat{\phi_d}}(E_d \times E_{d\theta}/\mathbb{Q})|}.$$

For any isogeny between abelian varieties, the Tamagawa ratio is known to admit a local formula, and in our case this is essentially given by the right-hand side of (1.4) (see Section 4.3 for details). Consequently, one explanation for the unbounded growth of $\dim \text{Sel}^2(E_d/K)$ seen in Theorem 1.1 is that the Tamagawa ratios $\mathcal{T}(\phi_d)$ tend to grow with d . Similarly, growth of the relevant Tamagawa ratios is the phenomenon underlying the behaviour of 2-isogeny Selmer groups of quadratic twist families of certain elliptic curves seen in work of Klagsbrun–Lemke Oliver [18] and Xiong–Zaharescu [39]. Thus, the behaviour we uncover can be viewed as an extension of those works to a special class of abelian surfaces.

1.4 | Prime twists of the congruent number curve

As a complement to our main results, we provide examples of thin subfamilies of quadratic twists in which significantly different behaviour occurs to that exhibited by the full family. Specifically, take E to be the congruent number curve:

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

Further, take $K = \mathbb{Q}(\sqrt{\theta})$ to be an imaginary quadratic extension of class number 1 in which 2 is inert. Thus, $\theta \in \{-3, -11, -19, -43, -67, -163\}$. For a prime p , 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

$$\text{Sel}^2(E_p/K) \cong \mathbb{F}_2^{e_1(E_p/K)} \oplus \mathbb{F}_2[G]^{e_2(E_p/K)}.$$

Theorem 1.9 (Theorem 9.13). *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:*

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

In particular, the proportion of prime twists for which the G -action on $\text{Sel}^2(E_p/K)$ is non-trivial is equal to $5/16$.

1.5 | Overview of the proofs

The proofs of the results outlined above require a combination of algebraic and analytic methods. Where possible we have tried to decouple these, so that the algebraic results stand alone.

The algebraic work is largely carried out in Sections 4 and 7, and is based on work of Kramer [20]. For a squarefree integer d , a key role in our results is played by the group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ of Definition 4.1. This is a subgroup of the 2-Selmer group $\text{Sel}^2(E_d/\mathbb{Q})$ of E_d over \mathbb{Q} . Our key algebraic result is Corollary 4.8 which shows that the Selmer group $\text{Sel}^2(E_d/K)$ admits the explicit description of Theorem 1.3 as soon as this auxiliary Selmer group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ vanishes.

The main statistical theorems of the paper then depend on proving Theorem 6.1, which shows that $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is trivial for 100% of d . To do this we draw on analytic techniques developed by Heath–Brown, and used to determine the distribution of the 2-Selmer groups of quadratic twists of the congruent number curve [12, 13]. 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 Proposition 7.8, we similarly give an explicit description of $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ as a subgroup of $(\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^2$.

In fact, for the analytic part of the argument we have opted to replace $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ with a certain subgroup S_d of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ (see Definition 8.5) whose vanishing implies the vanishing of $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$, but which admits a simpler explicit description. In Section 8.5, 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. An alternative method at this point might be to draw on the alternative approaches of Kane [16] or Smith [34].

It is worth remarking that the passage from $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ to S_d is somewhat wasteful. By following the work of Heath–Brown [12] more closely, one can similarly describe the order of $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ as a sum of Jacobi symbols. This would likely lead to significant improvements to the error bounds in Theorem 6.1. We have opted not to do this in favour of working with the simpler and more explicit sums arising from S_d . In this respect, the resulting analysis is much closer to that carried out by Fouvry–Klüners in [8] to determine the distribution of 4-ranks of class groups of quadratic fields.

1.6 | Layout of the paper

In Section 2, we introduce some notation that will be in use throughout.

In Section 3, we review some basic properties of Selmer structures and their associated Selmer groups which we use in later sections.

In Section 4, we study algebraically the behaviour of 2-Selmer groups of elliptic curves in quadratic extensions, building on work of Kramer [20]. Along the way we give two reinterpretations of Kramer’s work, one in the language of Selmer structures, and another in terms of the Weil restriction of scalars.

In Section 5, we study the analytic properties of the function $g(d)$ of Notation 5.5 (essentially the right-hand side of (1.4)) which gives a lower bound for $\dim \text{Sel}^2(E_d/K)$. In particular, we show in Proposition 5.8 that $g(d)$ follows an Erdős–Kac type distribution.

In Section 6, we state our main technical result, Theorem 6.1, on the vanishing of the auxiliary Selmer group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ for 100% of twists d . From this we deduce Theorems 1.1, 1.3 and 1.7, along with related results.

The proof of Theorem 6.1 is carried out across Sections 7 and 8. In Section 7, we give some algebraic preliminaries. In Section 8, we build on this by describing the order of $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ as a sum of Jacobi symbols, before following closely the strategy of [8, Section 5] to study the behaviour of these sums as d varies.

In Section 9, we prove Theorem 1.9 concerning the behaviour over certain quadratic extensions of the 2-Selmer groups of prime twists of the congruent number curve.

2 | NOTATION AND CONVENTIONS

In this section, we detail some notation and conventions which will be used throughout the paper.

2.1 | Arithmetic functions

Given a positive integer n we write $\omega(n)$ for the number of distinct prime factors of n . We denote by μ the Möbius function, and for coprime integers m and n with n odd and positive, we write $(\frac{m}{n})$ for the corresponding Jacobi symbol.

2.2 | Galois cohomology

For a field F of characteristic 0, we write \bar{F} for a (fixed once and for all) algebraic closure of F , and denote its absolute Galois group by $G_F = \text{Gal}(\bar{F}/F)$. For a positive integer n we write μ_n for the G_F -module of n th roots of unity in \bar{F} , and write $\mu = \cup_{n \geq 1} \mu_n$.

By a G_F -module M we mean a discrete module M on which G_F acts continuously. For $i \geq 0$ we write $H^i(F, M)$ as a shorthand for the continuous cohomology groups $H^i(G_F, M)$. We define the *dual* of M to be

$$M^* := \text{Hom}(M, \mu).$$

This is a G_F -module with action given by setting, for $\sigma \in G_F$ and $\phi \in M^*$,

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

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

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

and

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

respectively. When L/F is Galois and the action of G_F on M factors through $\text{Gal}(L/F)$, we write $H^i(L/F, M)$ as a shorthand for the cohomology group $H^i(\text{Gal}(L/F), M)$.

2.3 | Number fields and completions

For a number field F and a place v of F , we write F_v for the completion of F at v . We implicitly fix embeddings $\bar{F} \hookrightarrow \bar{F}_v$ for each place v and in this way view G_{F_v} as a subgroup of G_F for each

v . In this way, for a G_F -module M , we obtain restriction maps on cohomology $\text{res}_v : H^i(F, M) \rightarrow H^i(F_v, M)$ for each v . When v is non-archimedean we denote by F_v^{nr} the maximal unramified extension of F_v , and write

$$H_{\text{nr}}^1(F_v, M) := \ker \left(H^1(F_v, M) \xrightarrow{\text{res}} H^1(F_v^{\text{nr}}, M) \right)$$

for the subgroup of unramified classes in $H^1(F_v, M)$.

2.4 | The Kummer image for abelian varieties

Still taking F to be a number field, for an abelian variety A over F , and for a place v of F , we denote by $\mathcal{S}(A/F_v)$ the image of the coboundary map

$$\delta_v : A(F_v)/2A(F_v) \hookrightarrow H^1(F_v, A[2]) \quad (2.1)$$

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

$$0 \longrightarrow A[2] \longrightarrow A(\bar{F}_v) \xrightarrow{2} A(\bar{F}_v) \longrightarrow 0. \quad (2.2)$$

2.5 | 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 \bar{F} -isomorphism

$$\psi_d : A \xrightarrow{\sim} A_d \quad (2.3)$$

such that for all σ in G_F , $\psi_d^{-1} \circ \sigma \psi_d$ is multiplication by $\chi_d(\sigma)$ on A . Here $\sigma \psi_d$ is the unique isomorphism $A \rightarrow A_d$ sending any $P \in A(\bar{F})$ to $\sigma \psi_d(\sigma^{-1}P)$. Note in particular that ψ_d is defined over $F(\sqrt{d})$, so that A is isomorphic to A_d over $F(\sqrt{d})$.

3 | SELMER STRUCTURES

In this section, we review the properties of Selmer structures and their associated Selmer groups which will be used later. For details see, for example, [25, 37], and the references therein.

Throughout this section, we take F to be a number field. We take M to be a finite G_F -module annihilated by 2, so that M is a finite-dimensional \mathbb{F}_2 -vector space. All dimensions will be taken over \mathbb{F}_2 .

3.1 | Local duality

For each place v of F , we have the *local Tate pairing*

$$\langle , \rangle_v : H^1(F_v, M) \times H^1(F_v, M^*) \longrightarrow H^2(F_v, \mu_2) = \text{Br}(F_v)[2] \hookrightarrow \mathbb{Q}/\mathbb{Z}$$

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

Theorem 3.1 (Tate local duality). *For each place v of F the pairing \langle , \rangle_v is non-degenerate. Moreover, for each non-archimedean place $v \nmid 2$ such that the inertia group I_{F_v} acts trivially on M , $H_{\text{nr}}^1(F_v, M)$ and $H_{\text{nr}}^1(F_v, M^*)$ are orthogonal complements under this pairing.*

Proof. See [29, Corollary 7.2.6] for non-archimedean v and [29, Theorem 7.2.17] for archimedean v . The claim concerning the unramified subspaces is [29, Theorem 7.2.15]. \square

Example 3.2. Take $M = \mu_2$, which is self-dual. For each place v of F , Kummer theory gives a canonical isomorphism $H^1(F_v, \mu_2) \cong F_v^\times / F_v^{\times 2}$ (and we have the corresponding isomorphism globally also). For any non-archimedean place $v \nmid 2$ of F we have

$$H_{\text{nr}}^1(F_v, \mu_2) = \mathcal{O}_{F_v}^\times / \mathcal{O}_{F_v}^{\times 2} \subseteq F_v^\times / F_v^{\times 2}.$$

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 $(x, y) \mapsto (x, y)_v \in \{\pm 1\} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

3.2 | Selmer structures

Definition 3.3. A *Selmer structure* $\mathcal{L} = \{\mathcal{L}_v\}_v$ for M is a collection of subspaces

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

for each place v of F , such that $\mathcal{L}_v = H_{\text{nr}}^1(F_v, M)$ for all but finitely many places. The associated *Selmer group* $\text{Sel}_{\mathcal{L}}(F, M)$ is defined by the exactness of

$$0 \longrightarrow \text{Sel}_{\mathcal{L}}(F, M) \longrightarrow H^1(F, M) \longrightarrow \prod_{v \text{ place of } F} H^1(F_v, M) / \mathcal{L}_v.$$

It is a finite-dimensional \mathbb{F}_2 -vector space.

For each place v we write \mathcal{L}_v^* for the orthogonal complement of \mathcal{L}_v under the local Tate pairing, so that \mathcal{L}_v^* is a subspace of $H^1(F_v, M^*)$. We define the *dual Selmer structure* \mathcal{L}^* for M^* by taking $\mathcal{L}^* = \{\mathcal{L}_v^*\}_v$. We refer to $\text{Sel}_{\mathcal{L}^*}(F, M)$ as the *dual Selmer group*.

3.3 | The Greenberg–Wiles formula

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

Theorem 3.4. *Let $\mathcal{L} = \{\mathcal{L}_v\}_v$ be a Selmer structure for M . Then we have*

$$\begin{aligned} \dim \operatorname{Sel}_{\mathcal{L}}(F, M) - \dim \operatorname{Sel}_{\mathcal{L}^*}(F, M^*) \\ = \dim M^{G_F} - \dim (M^*)^{G_F} + \sum_{v \text{ place of } F} (\dim \mathcal{L}_v - \dim M^{G_{F_v}}). \end{aligned}$$

Proof. This is [38, Proposition 1.6]. See also [37, Theorem 2]. □

Example 3.5 (The 2-Selmer group of an elliptic curve). Let E/F be an elliptic curve. For each place v of F we have the Kummer image

$$\mathcal{S}(E/F_v) \subseteq H^1(F_v, E[2])$$

defined in Section 2.4. The collection $\mathcal{S} = \{\mathcal{S}(E/F_v)\}_v$ defines a Selmer structure for $E[2]$. This is a consequence of the fact that, for a non-archimedean place $v \nmid 2$ of F at which E has good reduction, we have

$$\mathcal{S}(E/F_v) = H_{\text{nr}}^1(F_v, E[2]).$$

Using the Weil pairing $(,)_{e_2} : E[2] \times E[2] \rightarrow \mu_2$ to identify $E[2]$ with its dual, the resulting Selmer structure is self-dual (see, for example, [30, Proposition 4.10]). That is, each $\mathcal{S}(E/F_v)$ is a maximal isotropic subspace of $H^1(F_v, E[2])$ with respect to the local Tate pairing. We note that Theorem 3.4 gives

$$\sum_{v \text{ place of } F} (\dim E(F_v)/2E(F_v) - \dim E(F_v)[2]) = 0. \quad (3.6)$$

One can also give an elementary proof of this by computing the local terms individually (see, for example, [31, Proposition 3.9]).

4 | 2-SELMER GROUPS OVER QUADRATIC EXTENSIONS

For the rest of the paper, we fix a quadratic extension K/\mathbb{Q} . Write $K = \mathbb{Q}(\sqrt{\theta})$ for a squarefree integer θ , and write $G = \operatorname{Gal}(K/\mathbb{Q})$. Moreover, we fix an elliptic curve E/\mathbb{Q} . Note that at this point we make no assumption on the 2-torsion of E . In later sections (Section 6 onwards) it will be necessary to reduce to the case of full 2-torsion but we shall be clear when this restriction is made. Denote by $\operatorname{Sel}^2(E/K)$ the 2-Selmer group of E/K . The conjugation action of G on $H^1(K, E[2])$ makes $\operatorname{Sel}^2(E/K)$ into an $\mathbb{F}_2[G]$ -module.

The structure of $\operatorname{Sel}^2(E/K)$ has been studied by Kramer in [20]. 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 [23, 26] 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 our applications are carried out.

As in Section 2.5, associated to the squarefree integer θ is the quadratic twist E_θ , which comes equipped with the isomorphism $\psi = \psi_\theta$ from E to E_θ . While this isomorphism is only defined over K , it restricts to an isomorphism of $G_{\mathbb{Q}}$ -modules from $E[2]$ to $E_\theta[2]$. We use this to identify $H^1(\mathbb{Q}_v, E[2])$ and $H^1(\mathbb{Q}_v, E_\theta[2])$ for each place v , and identify the corresponding global cohomology groups similarly. In particular, for each place v of \mathbb{Q} we may view both the Kummer images $\mathcal{S}(E/\mathbb{Q}_v)$ and $\mathcal{S}(E_\theta/\mathbb{Q}_v)$ (cf. Section 2.4) as subgroups of $H^1(\mathbb{Q}_v, E[2])$. Similarly, we view both $\text{Sel}^2(E/\mathbb{Q})$ and $\text{Sel}^2(E_\theta/\mathbb{Q})$ as subgroups of $H^1(\mathbb{Q}, E[2])$.

4.1 | Selmer structures associated to E/K

We begin by defining two Selmer structures for $E[2]$ over \mathbb{Q} , each of which will capture a part of $\text{Sel}^2(E/K)$.

Definition 4.1. Define the Selmer structure \mathcal{F} for the $G_{\mathbb{Q}}$ -module $E[2]$ by setting, for each place v of \mathbb{Q} ,

$$\mathcal{F}_v = \mathcal{F}(E/\mathbb{Q}_v) := \text{res}_{K_w/\mathbb{Q}_v}^{-1}(\mathcal{S}(E/K_w)) \leq H^1(\mathbb{Q}_v, E[2]),$$

where w is any choice of place of K extending v (the definition does not depend on this choice). Let $\text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) \leq H^1(\mathbb{Q}, E[2])$ denote the resulting Selmer group. We further define the Selmer structure \mathcal{C} for $E[2]$ as the dual of \mathcal{F} , and denote the local conditions by $\mathcal{C}(E/\mathbb{Q}_v)$. We denote the resulting Selmer group $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$.

Lemma 4.2. We have $\text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) = \text{res}_{K/\mathbb{Q}}^{-1}(\text{Sel}^2(E/K))$.

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

Recall the definition of the local norm map from Notation 1.2.

Lemma 4.3. The following properties hold for the Selmer structure \mathcal{C} .

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

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

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

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

$$\mathcal{C}(E/\mathbb{Q}_v) = \delta_v(N_{K_w/\mathbb{Q}_v} E(K_w)) = \mathcal{S}(E/\mathbb{Q}_v) \cap \mathcal{S}(E_\theta/\mathbb{Q}_v),$$

where $\delta_v : E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \hookrightarrow H^1(\mathbb{Q}_v, E[2])$ is the local Kummer map (2.1) and the intersection takes place in $H^1(\mathbb{Q}_v, E[2])$.

(iii) Globally, we have $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = \text{Sel}^2(E/\mathbb{Q}) \cap \text{Sel}^2(E_{\theta}/\mathbb{Q})$. Moreover, we have

$$\text{cor}_{K/\mathbb{Q}}(\text{Sel}^2(E/K)) \subseteq \text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]).$$

Proof.

- (i) That $\text{cor}_{K_w/\mathbb{Q}_v}(\mathcal{S}(E/K_w))$ and $\text{res}_{K_w/\mathbb{Q}_v}^{-1}(\mathcal{S}(E/K_w))$ are orthogonal complements under the local Tate pairing is noted by Kramer in the paragraph following [20, Equation (10)]. Specifically, it follows from [1, Proposition 9; 29, Corollary 7.1.4] that $\text{res}_{K_w/\mathbb{Q}_v}$ and $\text{cor}_{K_w/\mathbb{Q}_v}$ are adjoints with respect to the local Tate pairings. It follows that we have inclusions

$$\text{cor}_{K_w/\mathbb{Q}_v}(\mathcal{S}(E/K_w)) \subseteq \mathcal{F}_v^*$$

and

$$\text{res}_{K_w/\mathbb{Q}_v}(\text{cor}_{K_w/\mathbb{Q}_v}(\mathcal{S}(E/K_w))^*) \subseteq \mathcal{S}(E/K_w)^*.$$

Since $\mathcal{S}(E/K_w)$ is its own orthogonal complement, the result follows.

- (ii) The first equality follows from the fact that the coboundary maps arising from the respective Kummer sequences (2.2) over K_w and \mathbb{Q}_v commute with corestriction. The second equality is [20, Proposition 7].
- (iii) The claim that $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = \text{Sel}^2(E/\mathbb{Q}) \cap \text{Sel}^2(E_{\theta}/\mathbb{Q})$ is a formal consequence of (ii). The inclusion

$$\text{cor}_{K/\mathbb{Q}}(\text{Sel}^2(E/K)) \subseteq \text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$$

follows from (i) and compatibility of the local and global corestriction maps. \square

Remark 4.4. Let v be a place of \mathbb{Q} . Since the Selmer structure \mathcal{F} is dual to \mathcal{C} , it follows formally from Lemma 4.3 and the fact that $\mathcal{S}(E/\mathbb{Q}_v)$ is its own orthogonal complement, that we have

$$\mathcal{F}(E/\mathbb{Q}_v) = \mathcal{S}(E/\mathbb{Q}_v) + \mathcal{S}(E_{\theta}/\mathbb{Q}_v),$$

where the sum is taken inside $H^1(\mathbb{Q}_v, E[2])$.

We may use Theorem 3.4 to determine the difference between the dimensions of the Selmer groups $\text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2])$ and $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$.

Lemma 4.5. *We have*

$$\dim \text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) - \dim \text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = \sum_{v \text{ place of } \mathbb{Q}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

Proof. Since for each place v of \mathbb{Q} , the groups $\mathcal{C}(E/\mathbb{Q}_v)$ and $\mathcal{F}(E/\mathbb{Q}_v)$ are orthogonal complements under the local Tate pairing, we have

$$\dim \mathcal{F}(E/\mathbb{Q}_v) = \dim H^1(\mathbb{Q}_v, E[2]) - \dim \mathcal{C}(E/\mathbb{Q}_v).$$

Moreover, since $\mathcal{S}(E/\mathbb{Q}_v)$ is its own orthogonal complement we have

$$\dim H^1(\mathbb{Q}_v, E[2]) = 2 \dim E(\mathbb{Q}_v)/2E(\mathbb{Q}_v).$$

Along with Lemma 4.3(ii) this gives

$$\begin{aligned} \dim \mathcal{F}_v &= 2 \dim E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) - \dim N_{K_w/\mathbb{Q}_v} E(K_w)/2E(\mathbb{Q}_v) \\ &= \dim E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) + \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w). \end{aligned}$$

Theorem 3.4 then gives

$$\begin{aligned} \dim \text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) - \dim \text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) &= \sum_{v \text{ place of } \mathbb{Q}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w) \\ &\quad + \sum_{v \text{ place of } \mathbb{Q}} (\dim E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) - \dim E(\mathbb{Q}_v)[2]). \end{aligned}$$

and the result follows from (3.6). \square

4.2 | The 2-Selmer group of E/K

We now apply the results above to study the 2-Selmer group of E/K .

Lemma 4.6 (cf. [20, Lemma 3]). *We have an exact sequence*

$$0 \longrightarrow H^1(K/\mathbb{Q}, E(K)[2]) \xrightarrow{\inf} \text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2]) \xrightarrow{\text{res}_{K/\mathbb{Q}}} \text{Sel}^2(E/K) \xrightarrow{\text{cor}_{K/\mathbb{Q}}} \text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]). \quad (4.7)$$

Proof. We first claim that the sequence

$$H^1(\mathbb{Q}, E[2]) \xrightarrow{\text{res}} H^1(K, E[2]) \xrightarrow{\text{cor}} H^1(\mathbb{Q}, E[2])$$

is exact. To see this, consider the exact sequence of $G_{\mathbb{Q}}$ -modules

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

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

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

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

Having shown the claim, the result now follows by combining the inflation-restriction exact sequence with Lemmas 4.2 and 4.3(iii). \square

Corollary 4.8. *If $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = 0$, then all of the following hold.*

(i) *There is a short exact sequence*

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

where the first map is inflation.

(ii) *We have*

$$\dim \text{Sel}^2(E/K) = -\dim \left(\frac{E(\mathbb{Q})[2]}{N_{K/\mathbb{Q}}(E(K)[2])} \right) + \sum_{v \text{ place of } \mathbb{Q}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

(iii) *The G -action on $\text{Sel}^2(E/K)$ is trivial.*

Proof.

(i) Follows immediately from Corollary 4.6.

(ii) Follows from (i) and Lemma 4.5 upon noting that, since $\text{Gal}(K/\mathbb{Q})$ is cyclic, we have

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

(See, for example, [1, 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 $H^1(\mathbb{Q}, E[2])$ to $H^1(K, E[2])$ is contained in the invariant subspace $H^1(K, E[2])^G$. \square

For a similar result to Corollary 4.8(ii) which holds when K/\mathbb{Q} is replaced by a cyclic degree p extension for an odd prime p , see [3, Theorem 1.2].

Remark 4.9. Combining Lemma 4.5 with Corollary 4.6 allows one to recover the formula for the rank of E/K given in [20, Theorem 1]. In the second part of that theorem, Kramer studies the group $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])/\text{cor}_{K/\mathbb{Q}}(\text{Sel}^2(E/K))$, 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 pairings on $\text{Sel}^2(E/\mathbb{Q})$ and $\text{Sel}^2(E_{\theta}/\mathbb{Q})$ (recall from Lemma 4.3(iii) that $\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = \text{Sel}^2(E/\mathbb{Q}) \cap \text{Sel}^2(E_{\theta}/\mathbb{Q})$). In particular, this group has even dimension.

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

Lemma 4.10. *We have*

$$\dim \text{Sel}^2(E/K) \geq -2 + \sum_{v \text{ place of } \mathbb{Q}} \dim E(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E(K_w).$$

Proof. From Corollary 4.6 we find

$$\dim \mathrm{Sel}^2(E_d/K) \geq \dim \mathrm{Sel}_{\mathcal{F}_d}(\mathbb{Q}, E_d[2]) - \dim \mathrm{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E[2]) - \dim H^1(K/\mathbb{Q}, E(K)[2]).$$

The result now follows from Lemma 4.5, noting that

$$\dim H^1(K/\mathbb{Q}, E(K)[2]) \leq 2,$$

which is a consequence of the explicit description of cohomology of cyclic groups. \square

4.3 | The Weil restriction of scalars

Here we give a slight reinterpretation of the above material in terms of the restriction of scalars of E from K to \mathbb{Q} . The material of this section is closely related to, and inspired by, that appearing in [26, Section 3]. Following Milne [27, Section 2], the restriction of scalars may be described as a special case of a general construction of twists of powers of E , which we now recall. In what follows, for abelian varieties A and B defined over \mathbb{Q} , we endow $\mathrm{Hom}_{\bar{\mathbb{Q}}}(A, B)$ (the group of $\bar{\mathbb{Q}}$ -homomorphisms from A to B) with the $G_{\mathbb{Q}}$ action $\varphi \mapsto {}^{\sigma}\varphi$, where for $\sigma \in G_{\mathbb{Q}}$ the homomorphism ${}^{\sigma}\varphi$ sends $P \in A(\bar{\mathbb{Q}})$ to $\sigma\varphi(\sigma^{-1}P)$.

Definition 4.11. 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

$$(P_1, \dots, P_n) \mapsto \left(\sum_{j=1}^n m_{1,j} P_j, \dots, \sum_{j=1}^n m_{n,j} P_j \right).$$

In this way we view $\mathrm{GL}_n(\mathbb{Z})$ as a subgroup of $\mathrm{Aut}_{\bar{\mathbb{Q}}}(E^n)$. 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 $\mathrm{Aut}_{\bar{\mathbb{Q}}}(E^n)$. The class of ρ_{Λ} in $H^1(\mathbb{Q}, \mathrm{Aut}_{\bar{\mathbb{Q}}}(E^n))$ 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 $\bar{\mathbb{Q}}$ -isomorphism $\varphi_{\Lambda} : E^n \rightarrow \Lambda \otimes E$ satisfying $\varphi_{\Lambda}^{-1} \circ {}^{\sigma}\varphi_{\Lambda} = \rho_{\Lambda}(\sigma)$ for all $\sigma \in G_{\mathbb{Q}}$.

The relevant restriction of scalars can then be defined as follows.

Definition 4.12. Denote by $\mathbb{Z}[G]$ the integral group ring of $G = \mathrm{Gal}(K/\mathbb{Q})$. We define the restriction of scalars of E relative to K/\mathbb{Q} to be the abelian surface $E \otimes \mathbb{Z}[G]$. We denote it $\mathrm{Res}_{K/\mathbb{Q}} E$. By the above, it comes equipped with an isomorphism $\varphi : E \times E \rightarrow \mathrm{Res}_{K/\mathbb{Q}} E$, defined over K , and such that for all $\sigma \in G_{\mathbb{Q}}$, and all $P, Q \in E(\bar{\mathbb{Q}})$, we have

$$(\varphi^{-1} \circ {}^{\sigma}\varphi)(P, Q) = \begin{cases} (P, Q) & \chi_{\theta}(\sigma) = 1, \\ (Q, P) & \chi_{\theta}(\sigma) = -1. \end{cases}$$

In particular, φ^{-1} composed with projection onto the first coordinate gives an isomorphism

$$\mathrm{Res}_{K/\mathbb{Q}} E(\mathbb{Q}) \cong E(K).$$

Remark 4.13. The restriction of scalars $\mathrm{Res}_{K/\mathbb{Q}}(E)$ is more typically defined as the unique scheme over \mathbb{Q} representing the functor on \mathbb{Q} -schemes

$$T \longmapsto E(T \times_{\mathbb{Q}} K).$$

As in [26, Section 2], this is equivalent to the construction given above.

Notation 4.14. To ease notation, in what follows we write $A = \mathrm{Res}_{K/\mathbb{Q}}(E)$. Thus, A is an abelian surface defined over \mathbb{Q} .

One has

$$\mathrm{Sel}^2(E/K) \cong \mathrm{Sel}^2(A/\mathbb{Q}). \quad (4.15)$$

Indeed, the corresponding result for Shafarevich–Tate groups is given in [27, Proof of Theorem 1], and the same argument works here (see also [26, Proposition 3.1]). In particular, in the case that $\mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]) = 0$, Corollary 4.8 can be interpreted as giving a description of the 2-Selmer group over \mathbb{Q} of the abelian surface A .

Moreover, it turns out that the groups $\mathrm{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])$ and $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2])$ are the Selmer groups associated to a certain isogeny between A and $E \times E_{\theta}$ as we now explain.

Definition 4.16. Consider the isogeny $\phi_0 : E \times E \rightarrow E \times E$ given by the formula

$$\phi_0(P, Q) = (P + Q, P - Q).$$

Let $\varphi : E \times E \rightarrow A$ be as in Definition 4.12, and let $\psi = \psi_{\theta} : E \xrightarrow{\sim} E_{\theta}$ be as in (2.3). Now define the isogeny (*a priori* over K)

$$\phi = (1 \times \psi) \circ \phi_0 \circ \varphi^{-1} : A \longrightarrow E \times E_{\theta}.$$

One readily computes that in fact ϕ is defined over \mathbb{Q} .

We denote by $\mathrm{Sel}^{\phi}(A/\mathbb{Q})$ the Selmer group associated to ϕ . For each place v of \mathbb{Q} , we denote by $\delta_{\phi,v}$ the coboundary map

$$\delta_{\phi,v} : E(\mathbb{Q}_v) \times E_{\theta}(\mathbb{Q}_v) \rightarrow H^1(\mathbb{Q}_v, A[\phi])$$

associated to the short exact sequence

$$0 \longrightarrow A[\phi] \longrightarrow A(\bar{\mathbb{Q}}_v) \xrightarrow{\phi} (E \times E_{\theta})(\bar{\mathbb{Q}}_v) \longrightarrow 0.$$

Then the collection $\{\mathrm{im}(\delta_{\phi,v})\}_v$ defines a Selmer structure for $A[\phi]$, whose associated Selmer group is $\mathrm{Sel}^{\phi}(A/\mathbb{Q})$.

Lemma 4.17. *We have a canonical isomorphism $\mathrm{Sel}^\phi(A/\mathbb{Q}) \cong \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2])$.*

Proof. With $\varphi : E \times E \rightarrow A$ as in Definition 4.12, one readily checks that φ^{-1} restricts to a $G_{\mathbb{Q}}$ -isomorphism between $A[\phi]$ and the diagonal embedding of $E[2]$ into $E \times E$. In this way, we identify $H^1(\mathbb{Q}, A[\phi])$ and $H^1(\mathbb{Q}, E[2])$. We make corresponding identifications locally at each place of \mathbb{Q} also. We will show that this identification maps $\mathrm{Sel}^\phi(A/\mathbb{Q})$ onto $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2])$.

For $i = 1, 2$ write $\Delta_i : E \rightarrow E \times E$ for the homomorphisms defined by

$$\Delta_1(P) = (P, P) \quad \text{and} \quad \Delta_2(P) = (P, -P).$$

This gives maps

$$\varphi \circ \Delta_1 : E \longrightarrow A \quad \text{and} \quad \varphi \circ \Delta_2 \circ \psi^{-1} : E_\theta \longrightarrow A,$$

which are readily checked to be defined over \mathbb{Q} . For each place v of \mathbb{Q} these maps fit into a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E[2] & \longrightarrow & E(\bar{\mathbb{Q}}_v) & \xrightarrow{2} & E(\bar{\mathbb{Q}}_v) \longrightarrow 0 \\ & & \parallel & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A[2] & \longrightarrow & A(\bar{\mathbb{Q}}_v) & \xrightarrow{\phi} & E(\bar{\mathbb{Q}}_v) \times E_\theta(\bar{\mathbb{Q}}_v) \longrightarrow 0 \\ & & \parallel & & \uparrow & & \uparrow \\ 0 & \longrightarrow & E_\theta[2] & \longrightarrow & E_\theta(\bar{\mathbb{Q}}_v) & \xrightarrow{2} & E_\theta(\bar{\mathbb{Q}}_v) \longrightarrow 0, \end{array}$$

where the right-most vertical maps are induced by the natural inclusions into the respective factors. On cohomology this induces a commutative diagram

$$\begin{array}{ccc} E(\bar{\mathbb{Q}}_v) & \xrightarrow{\delta_v} & H^1(\mathbb{Q}_v, E[2]) \\ \downarrow & & \parallel \\ E(\bar{\mathbb{Q}}_v) \times E_\theta(\bar{\mathbb{Q}}_v) & \xrightarrow{\delta_{\phi,v}} & H^1(\mathbb{Q}_v, A[\phi]) \\ \uparrow & & \parallel \\ E_\theta(\bar{\mathbb{Q}}_v) & \xrightarrow{\delta_v} & H^1(\mathbb{Q}_v, E_\theta[2]). \end{array}$$

The result now follows from Remark 4.4. □

Remark 4.18. One can show that the product polarisation on $E \times E$ descends to a polarisation on A defined over \mathbb{Q} rather than just K as is *a priori* the case (this follows from the material in [15, Section 2]). Thus, A is a principally polarised abelian surface. We can then view the dual isogeny to ϕ as an isogeny

$$\hat{\phi} : E \times E_\theta \longrightarrow A.$$

Denote by $\text{Sel}^{\hat{\phi}}(E \times E_{\theta}/\mathbb{Q})$ the associated Selmer group. It follows formally from Lemma 4.17 and the fact that the Selmer structure \mathcal{C} is dual to \mathcal{F} , that we have

$$\text{Sel}^{\hat{\phi}}(E \times E_{\theta}/\mathbb{Q}) \cong \text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2]).$$

With more work, one can show that the composition (in either direction) of ϕ and $\hat{\phi}$ is multiplication by 2, and that the maps

$$A \xrightarrow{\phi} E \times E_{\theta} \xrightarrow{\hat{\phi}} A$$

induce the sequence (4.7).

Remark 4.19. In the terminology of [17, Section 2], the quantity

$$\frac{|\text{Sel}^{\phi}(A/\mathbb{Q})|}{|\text{Sel}^{\hat{\phi}}(E \times E_{\theta}/\mathbb{Q})|} \stackrel{\text{Lemma 4.17}}{=} \frac{|\text{Sel}_{\mathcal{F}}(\mathbb{Q}, E[2])|}{|\text{Sel}_{\mathcal{C}}(\mathbb{Q}, E[2])|}$$

is called the *Tamagawa ratio* associated to the isogeny ϕ . That the Tamagawa ratio for elliptic curves is given by a local formula goes back to Cassels [4, Theorem 1.1]. The corresponding result for abelian varieties, which in particular can be applied to A and ϕ , is given by Milne in [28, Section I.7]. This gives an alternative approach to the local formula of Lemma 4.5. We remark though that Milne's result is very closely related to Theorem 3.4, so this is not really a different proof.

In the next section, we will consider the 2-Selmer groups $\text{Sel}^2(E_d/K)$ associated to quadratic twists of E by squarefree integers d . As the next lemma shows, this is equivalent to considering the 2-Selmer groups associated to the quadratic twist family over \mathbb{Q} of A .

Lemma 4.20. *Let d be a square free integer. Let E_d denote the quadratic twist of E by d , and let A_d denote the quadratic twist of A by d . Then we have a \mathbb{Q} -isomorphism*

$$\text{Res}_{K/\mathbb{Q}}(E_d) \cong A_d$$

of abelian surfaces. In particular, we have

$$\text{Sel}^2(E_d/K) \cong \text{Sel}^2(A_d/\mathbb{Q}).$$

Proof. Both $\text{Res}_{K/\mathbb{Q}}(E_d)$ and A_d are twists of $E \times E$, so we need only show that the resulting classes in $H^1(G_{\mathbb{Q}}, \text{Aut}_{\bar{\mathbb{Q}}}(E \times E))$ agree. Write χ_d and χ_{θ} for the quadratic characters associated to $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ and K/\mathbb{Q} , respectively.

Fix $\sigma \in G_{\mathbb{Q}}$. Fix an isomorphism $\phi_1 : E \xrightarrow{\sim} E_d$ such that $\phi_1^{-1} \circ \sigma \phi_1 = \chi_d(\sigma)$, and write φ_2 for the isomorphism $E_d \times E_d \xrightarrow{\sim} \text{Res}_{K/\mathbb{Q}}(E_d)$ of Definition 4.12. This gives a $\bar{\mathbb{Q}}$ -isomorphism

$$Y = \varphi_2 \circ (\phi_1 \times \phi_1) : E \times E \xrightarrow{\sim} \text{Res}_{K/\mathbb{Q}}(E_d).$$

The resulting cocycle satisfies, for $P, Q \in E(\bar{\mathbb{Q}}) \times E(\bar{\mathbb{Q}})$,

$$(Y^{-1} \circ^\sigma Y)(P, Q) = \begin{cases} (\chi_d(\sigma)P, \chi_d(\sigma)Q) & \chi_\theta(\sigma) = 1, \\ (\chi_d(\sigma)Q, \chi_d(\sigma)P) & \chi_\theta(\sigma) = -1. \end{cases}$$

On the other hand, fix $\psi_1 : E \times E \xrightarrow{\sim} A$ as in Definition 4.12, and fix also $\psi_2 : A \xrightarrow{\sim} A_d$ such that $\psi_2^{-1}\psi_1 = \chi_d$. Writing $Y' = \psi_2 \circ \psi_1$, one readily computes that $Y'^{-1} \circ^\sigma Y'$ is given by the same formula as $Y^{-1} \circ^\sigma Y$, giving the result. \square

Remark 4.21. For each squarefree integer d , Definition 4.16 gives an isogeny

$$\phi_d : \text{Res}_{K/\mathbb{Q}}(E_d) \longrightarrow E_d \times E_{d\theta}.$$

Via Lemma 4.20, we view ϕ_d as an isogeny from A_d to $E_d \times E_{d\theta}$. One readily checks that the standard identification of $A[2]$ with $A_d[2]$ identifies $A[\phi]$ and $A_d[\phi_d]$.

5 | QUADRATIC TWISTS AND A DISTRIBUTION RESULT

Recall that $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ is a quadratic extension, $G = \text{Gal}(K/\mathbb{Q})$ 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 \mathcal{F}_d and \mathcal{C}_d the Selmer structures of the previous section with local conditions $\mathcal{F}(E_d/\mathbb{Q}_v)$ and $\mathcal{C}(E_d/\mathbb{Q}_v)$, respectively. We have associated Selmer groups $\text{Sel}_{\mathcal{F}_d}(\mathbb{Q}, E_d[2])$ and $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$. For a squarefree integer d we write $\chi_d : G_{\mathbb{Q}} \rightarrow \{\pm 1\}$ for the associated quadratic character defined by

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

5.1 | 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 5.1. 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 5.2. *Let $p \notin \Sigma$ be a prime divisor of d . Then $E_d(\mathbb{Q}_p^{\text{nr}})$ 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 $E[4]$ is unramified at p (that is, the inertia group I_p at p acts trivially on $E[4]$). Thus, any element σ of I_p acts on $E_d[4]$ as 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

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

giving the result. \square

Lemma 5.3. *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 [24, Corollary 4.4] that $N_{K_{\mathfrak{p}}/\mathbb{Q}_p}$ 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 5.2 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

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

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

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

We thus have

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

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

Remark 5.4. 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 [20] or [19] 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 5.5. For a squarefree integer d , write

$$g(d) := \sum_{v \text{ place of } \mathbb{Q}} \dim E_d(\mathbb{Q}_v) / N_{K_w/\mathbb{Q}_v} E_d(K_w)$$

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

$$\omega_{E,K}(d) := \# \left\{ p \mid d : \begin{array}{l} p \notin \Sigma \\ p \text{ inert in } K/\mathbb{Q} \\ \dim E(\mathbb{Q}_p)[2] = 2 \end{array} \right\}.$$

Note that by Lemma 4.10, the function $g(d) - 2$ gives a lower bound for $\dim \text{Sel}^2(E_d/K)$.

Proposition 5.6. 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 5.3. \square

5.2 | The distribution of $g(d)$

Notation 5.7. 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:

$\text{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$	$\{1\}$	$\frac{\mathbb{Z}/2\mathbb{Z}}{K \neq \mathbb{Q}(E[2])}$	$\frac{\mathbb{Z}/2\mathbb{Z}}{K = \mathbb{Q}(E[2])}$	$\mathbb{Z}/3\mathbb{Z}$	$\frac{S_3}{K \not\subseteq \mathbb{Q}(E[2])}$	$\frac{S_3}{K \subseteq \mathbb{Q}(E[2])}$
$\delta_{E,K}$	$1/2$	$1/4$	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 $\dim \text{Sel}^2(E_d/K) \geq g(d) - 2$ by Lemma 4.10, this shows that $\dim \text{Sel}^2(E_d/K)$ is (in a precise sense) typically at least as large as a constant times $\log \log(d)$.

Proposition 5.8. 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

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

Proof. Let $\gamma(d) := 2\omega_{E,K}(d)$. Since by Proposition 5.6 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 [10, Proposition 4]. Specifically, in the notation of that proposition, take

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

and

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

for a function $\epsilon(X) = o(1)$ 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 [10, Proposition 4] we can take

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

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 [21], standard arguments give

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

Taking X sufficiently large in the conclusion of [10, Proposition 4] shows that for any $k \geq 0$ we have

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

In particular, the k th moments of $(\gamma_p - \mu_p(\gamma))/\sigma_p(\gamma)$ converge to those of a normal random variable with mean 0 and variance 1. Note that for $n \leq X$ we have

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

Induction on k (cf. [10, Deduction of Theorem 1]) now shows that, taking $\epsilon(X) = \log \log \log(X)^{-1}$, we have

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

Thus, the k th moments of $(\gamma - 2\delta_{E,K} \log \log(X))/\sqrt{4\delta_{E,K} \log \log(X)}$ converge as $X \rightarrow \infty$ to those of the standard normal distribution. It then follows from [2, Theorem 30.2 and 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 $X \rightarrow \infty$, that is,

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

The result now follows. \square

Remark 5.9. In the last step of the proof we have used the standard result that a function f becomes normal as $X \rightarrow \infty$ 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 $X \rightarrow \infty$ with mean 0 and variance 1. This can be proved directly.

Remark 5.10. In the case that $K \subseteq \mathbb{Q}(E[2])$, the function $\gamma(d)$ in the proof of Proposition 5.8 is 0. In particular, by Proposition 5.6, we have that the k th moments of $g(d)$ are bounded.

We have the following basic corollary showing that, for 100% of d , $\dim \text{Sel}^2(E_d/K)$ is larger than any fixed integer whenever the 2-torsion field of E does not interact with K . This is in stark contrast with the situation for the Selmer groups $\text{Sel}^2(E_d/\mathbb{Q})$, whose distribution is determined by Kane in [16, Theorem 3].

Corollary 5.11. *If $K \cap \mathbb{Q}(E[2]) = \mathbb{Q}$, then for any $z \in \mathbb{R}$ we have*

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

Proof. By Lemma 4.10, we have $\dim \text{Sel}^2(E_d/K) \geq g(d) - 2$. The result now follows from Proposition 5.8. \square

Remark 5.12. By Lemma 4.20, Corollary 5.11 also applies with $\text{Sel}^2(E_d/K)$ replaced by the Selmer groups $\text{Sel}^2((\text{Res}_{K/\mathbb{Q}} E)_d/\mathbb{Q})$ associated to the quadratic twists of the Weil restriction of E from K to \mathbb{Q} .

6 | MAIN RESULTS

Recall that $K = \mathbb{Q}(\sqrt{\theta})/\mathbb{Q}$ is a quadratic extension with $G = \text{Gal}(K/\mathbb{Q})$. 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 4.5 and 4.6 is that, roughly speaking, the auxiliary Selmer group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ controls the discrepancy between $\dim \text{Sel}^2(E_d/K)$ and the function $g(d)$ of Notation 5.5. Thus, to improve on Proposition 5.8 and gain full control of the Selmer groups $\text{Sel}^2(E_d/K)$ 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 7 and 8 we will prove that, under this assumption, the Selmer group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is trivial for 100% of d .

Theorem 6.1. *We have*

$$\lim_{X \rightarrow \infty} \frac{\#\{d \text{ squarefree} \mid |d| < X, \text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0\}}{\#\{d \text{ squarefree} \mid |d| < X\}} = 1.$$

Remark 6.2. We will in fact show that the number of squarefree d with $|d| < X$ for which $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) \neq 0$ is $\ll X \log(X)^{-0.0394}$. See Theorem 8.2. It is likely that with more work this bound could be improved significantly, however we have not attempted to do so.

Remark 6.3. By Lemma 4.3, we have

$$\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = \text{Sel}^2(E_d/\mathbb{Q}) \cap \text{Sel}^2(E_{d\theta}/\mathbb{Q})$$

where the intersection is taken inside $H^1(\mathbb{Q}, E[2])$. Thus, Theorem 6.1 shows that for 100% of squarefree d , the groups $\text{Sel}^2(E_d/\mathbb{Q})$ and $\text{Sel}^2(E_{d\theta}/\mathbb{Q})$ share only the identity element.

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

6.1 | Statistical results for 2-Selmer groups

An immediate consequence of Theorem 6.1 is that the conclusion of Corollary 4.8 holds for 100% of squarefree d when we have full 2-torsion.

Corollary 6.4. *For 100% of squarefree d (ordered by absolute value), the $\text{Gal}(K/\mathbb{Q})$ -action on $\text{Sel}^2(E_d/K)$ is trivial, and we have*

$$\dim \text{Sel}^2(E_d/K) = -2 + \sum_{v \text{ place of } \mathbb{Q}} \dim E_d(\mathbb{Q}_v)/N_{K_w/\mathbb{Q}_v} E_d(K_w). \quad (6.5)$$

As a consequence, we can upgrade Proposition 5.8 to the following Erdős–Kac type result determining the distribution of the full 2-Selmer group.

Corollary 6.6. *The quantity*

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

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

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

Proof. By Corollary 6.4, among all squarefree integers d with $|d| < X$, outside a set of cardinality $o(X)$ we have

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

The result now follows from Proposition 5.8 noting that since $E[2] \subseteq E(\mathbb{Q})$, we have that $\delta_{E,K} = 1/2$. \square

6.2 | Statistical results for Shafarevich–Tate groups

A consequence of Corollary 6.6 is that $\dim \operatorname{Sel}^2(E_d/K)$ typically has size around $\log \log |d|$. By contrast, when E has no cyclic 4-isogeny defined over \mathbb{Q} , 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 [16, Theorem 3]. Thus, in this case the majority of $\dim \operatorname{Sel}^2(E_d/K)$ is attributable to the Shafarevich–Tate group. Formalising this observation allows us to prove the analogue of Corollary 6.6 for Shafarevich–Tate groups also.

Corollary 6.7. *Assume that E has no cyclic 4-isogeny defined over \mathbb{Q} . Then the quantity*

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

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

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

Proof. Since $\dim \operatorname{III}(E_d/K)[2] \leq \dim \operatorname{Sel}^2(E_d/K)$ for all d , by Corollary 6.6 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 6.6 thanks to [16, Theorem 3], which gives adequate control of the Mordell–Weil component of $\operatorname{Sel}^2(E_d/K)$. First, for any squarefree integer d , the standard short

exact sequence

$$0 \longrightarrow E_d(K)/2E_d(K) \longrightarrow \text{Sel}^2(E_d/K) \longrightarrow \text{III}(E_d/K)[2] \longrightarrow 0$$

gives

$$\dim \text{III}(E_d/K)[2] = \dim \text{Sel}^2(E_d/K) - \dim E_d(K)/2E_d(K).$$

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

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

giving the equality

$$\dim \text{III}(E_d/K)[2] = \dim \text{Sel}^2(E_d/K) - \text{rk}(E_d/\mathbb{Q}) - \text{rk}(E_{d\theta}/\mathbb{Q}) - 2.$$

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

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

we find

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

Dividing through by the number of squarefree integers d with $|d| \leq X$, taking the $\limsup_{X \rightarrow \infty}$, and applying Kane's theorem [16, Theorem 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 6.6 that

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

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 $M \rightarrow \infty$ gives the result. \square

Remark 6.8. It seems reasonable to expect that Corollary 6.7 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.

6.3 | 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 $G = \text{Gal}(K/\mathbb{Q})$.

Notation 6.9. We write

$$\Lambda(E_d/K) := E_d(K)/E_d(K)_{\text{tors}}.$$

We refer to this as the Mordell–Weil lattice. The action of G on $E_d(K)$ makes $\Lambda(E_d/K)$ into a G -module.

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

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

Lemma 6.10. *If $\text{Sel}_{\mathcal{E}_d}(\mathbb{Q}, E_d[2]) = 0$ 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 [5, 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

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

The right-hand side has trivial G -action, as follows from the vanishing of $\text{Sel}_{\mathcal{E}_d}(\mathbb{Q}, E_d[2])$ combined with Corollary 4.8(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. \square

Proposition 6.11. *Suppose we have $E_d(K)_{\text{tors}} = E_d[2]$ and $\text{Sel}_{\mathcal{E}_d}(\mathbb{Q}, E_d[2]) = 0$. 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 6.10, we must have

$$\Lambda(E_d/K) \cong \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1). \quad (6.12)$$

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 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 $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0$, the G -action on $E_d(K)/2E_d(K)$ is trivial by Corollary 4.8(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 $\Lambda(E_d/K) \rightarrow E_d(K)$ 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 (6.12). \square

Corollary 6.13. *For 100% of squarefree d , there is an isomorphism of $\mathbb{Z}[G]$ -modules*

$$E_d(K) \cong \mathbb{F}_2^2 \oplus \Lambda(E_d/\mathbb{Q}) \oplus \Lambda(E_{d\theta}/\mathbb{Q})(-1). \quad (6.14)$$

More precisely, we have

$$\lim_{X \rightarrow \infty} \frac{\#\{d \text{ squarefree} \mid |d| < X, (6.14) \text{ holds}\}}{\#\{d \text{ squarefree} \mid |d| < X\}} = 1.$$

Proof. Note that for each odd prime p , at most two 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 [22, Theorem 8], outside of a finite set of d we have $E_d(K)_{\text{tors}} \subseteq E[2^\infty]$. Moreover, by Lemma 5.2, only finitely many quadratic twists have a point of order 4. The result now follows from Theorem 8.2 and Proposition 6.11. \square

6.4 | Twists of the Weil restriction of scalars

In light of Section 4.3, we can recast the above results in terms of the restriction of scalars $\text{Res}_{K/\mathbb{Q}}(E)$ of E from K to \mathbb{Q} . To ease notation we write A in place of $\text{Res}_{K/\mathbb{Q}}(E)$. Thus, A is a principally polarised abelian surface over \mathbb{Q} . For a squarefree integer d , we write A_d for the quadratic twist of A by d . For each d , write

$$\phi_d : A_d \longrightarrow E_d \times E_{d\theta}$$

for the isogeny of Remark 4.21, write $\hat{\phi}_d$ for its dual, and denote by $\text{Sel}^\phi(A_d/\mathbb{Q})$ and $\text{Sel}^{\hat{\phi}_d}(E_d \times E_{d\theta}/\mathbb{Q})$ the associated Selmer groups.

Theorem 6.15. *In the notation above, we have the following.*

(i) *The quantity*

$$\frac{\dim \text{Sel}^2(A_d/\mathbb{Q}) - \log \log |d|}{\sqrt{2 \log \log |d|}}$$

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

$$\lim_{X \rightarrow \infty} \frac{\#\left\{|d| \leq X \text{ squarefree} : \frac{\dim \text{Sel}^2(A_d/\mathbb{Q}) - \log \log |d|}{\sqrt{2 \log \log |d|}} \leq z\right\}}{\#\{|d| \leq X \text{ squarefree}\}} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^z e^{-t^2/2} dt.$$

(ii) *For 100% of squarefree d ordered by absolute value, the group $\text{Sel}^{\hat{\phi}_d}(E_d \times E_{d\theta}/\mathbb{Q})$ is trivial. Moreover we have*

$$\dim \text{Sel}^2(A_d/\mathbb{Q}) = \dim \text{Sel}^{\hat{\phi}_d}(A_d/\mathbb{Q}) - 2,$$

and $\dim \text{Sel}^2(A_d/\mathbb{Q})$ is given by the formula on the right-hand side of (6.5).

Proof. The first part follows from Corollary 6.6 and Lemma 4.20. Using Lemma 4.17, Remark 4.18 and Lemma 4.20, the second part is then an immediate consequence of Theorem 6.1, Corollary 4.8(i) and Corollary 6.4. \square

Remark 6.16. Assume that E has no cyclic 4-isogeny defined over \mathbb{Q} . Then, since $\text{III}(A_d/\mathbb{Q}) \cong \text{III}(E_d/K)$, as a consequence of Corollary 6.7 we can replace $\text{Sel}^2(A_d/\mathbb{Q})$ with $\text{III}(A_d/\mathbb{Q})[2]$ in Theorem 6.15.

7 | EXPLICIT LOCAL CONDITIONS FOR FULL 2-TORSION

In this section, we make preparations for the proof of Theorem 6.1 by making the results of Section 4 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

$$E/\mathbb{Q} : y^2 = (x - a_1)(x - a_2)(x - a_3) \tag{7.1}$$

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 5.1, 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 $2\alpha\beta\gamma$.

7.1 | 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 $\mathcal{C}(E_d/\mathbb{Q}_v)$ of Definition 4.1 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 (2.2) with $A = E_d$ and $F = \mathbb{Q}$.

Lemma 7.2. *Let p be a prime with $p \notin \Sigma$. Then:*

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

$$\mathcal{C}(E_d/\mathbb{Q}_p) = \mathcal{S}(E_d/\mathbb{Q}_p) = H_{\text{nr}}^1(\mathbb{Q}_p, E_d[2]),$$

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

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

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

$$\mathcal{C}(E_d/\mathbb{Q}_p) = 0.$$

Proof. Let \mathfrak{p} be a prime of K lying over p .

(i) By Lemma 5.3, we have $N_{K_{\mathfrak{p}}/\mathbb{Q}_p} E_d(K_{\mathfrak{p}}) = E_d(\mathbb{Q}_p)$. The first equality in Lemma 4.3(ii) thus gives

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

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 $\mathcal{C}(E_d/\mathbb{Q}_p) = \mathcal{S}(E_d/\mathbb{Q}_p)$ by definition. For the second equality, since $p \nmid 2\infty$, we have $\dim \mathcal{S}(E_d/\mathbb{Q}_p) = \dim E_d[2]$. In particular, it suffices to show that the restriction of $\delta_{d,p}$ to $E_d[2]$ is injective, which follows from Lemma 5.2.

(iii) By Lemma 5.3 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 Lemma 4.3. \square

Remark 7.3. Taking orthogonal complements, the above result also determines the local groups $\mathcal{F}(E_d/\mathbb{Q}_p)$ for $p \notin \Sigma$.

7.2 | Explicit local conditions

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

Let $\lambda_{i,d} : E_d[2] \rightarrow \mu_2$ be the map $P \mapsto (P, P_{i,d})_{e_2}$, where $(\ , \)_{e_2} : E_d[2] \times E_d[2] \rightarrow \mu_2$ is the Weil pairing. This induces an isomorphism

$$(\lambda_{1,d}, \lambda_{2,d}) : E_d[2] \xrightarrow{\sim} \mu_2 \times \mu_2.$$

Via this map, we identify $H^1(\mathbb{Q}, E_d[2])$ with $H^1(\mathbb{Q}, \mu_2) \oplus H^1(\mathbb{Q}, \mu_2) = (\mathbb{Q}^\times / \mathbb{Q}^{\times 2})^2$ (cf. Example 3.2). 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

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

becomes the pairing $(\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2})^2 \times (\mathbb{Q}_v^\times / \mathbb{Q}_v^{\times 2})^2 \rightarrow \frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \mu_2$ given by

$$((x_1, x_2), (y_1, y_2)) \mapsto (x_1, y_2)_v (x_2, y_1)_v, \quad (7.4)$$

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

$$(x, y) \mapsto \begin{cases} (x - da_1, x - da_2) & x \notin \{da_1, da_2\}, \\ (\alpha\beta, d\alpha) & (x, y) = (da_1, 0), \\ (-d\alpha, -\alpha\gamma) & (x, y) = (da_2, 0). \end{cases} \quad (7.5)$$

See, for example, [33, Proposition X.1.4].

7.3 | The group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$

We now define a further Selmer structure, whose associated Selmer group contains $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ as a subgroup, and which admits a cleaner explicit description.

Definition 7.6. Define the Selmer structure $\tilde{\mathcal{C}}_d$ for $E_d[2]$ (viewed as a $G_{\mathbb{Q}}$ -module) via the local conditions

$$\tilde{\mathcal{C}}(E_d/\mathbb{Q}_v) = \begin{cases} \mathcal{C}(E_d/\mathbb{Q}_v) & v \notin \Sigma, \\ H^1(\mathbb{Q}_v, E[2]) & v \in \Sigma. \end{cases}$$

Denote by $\text{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ the associated Selmer group.

Note that by construction, $\text{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ contains $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ as a subgroup. In particular, if $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ is trivial, then so is $\text{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$. The advantage of considering $\text{Sel}_{\tilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ is that now Lemma 7.2 describes all non-trivial Selmer conditions.

Notation 7.7. 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 Section 7.2, 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 7.8. *With the notation and identifications of Notation 7.7, the Selmer group $\text{Sel}_{\tilde{\mathcal{E}}_d}(\mathbb{Q}, E_d[2])$ 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 7.2 and the definition of the local groups $\tilde{\mathcal{E}}(E_d/\mathbb{Q}_p)$, we have $\tilde{\mathcal{E}}(E_d/\mathbb{Q}_p) = 0$ for all primes p with $p \notin \Sigma$ such that both $p \mid d$ and p is inert in K/\mathbb{Q} , and $\tilde{\mathcal{E}}(E_d/\mathbb{Q}_p) = H_{\text{nr}}^1(\mathbb{Q}_p, E_d[2])$ 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 $\text{Sel}_{\tilde{\mathcal{E}}_d}(\mathbb{Q}, E_d[2])$ there are no conditions imposed at primes $p \in \Sigma$, in light of Lemma 7.2(ii) it suffices to show that condition (iii) is equivalent to the condition that

$$(x_1, x_2) \in \mathcal{S}(E_d/\mathbb{Q}_p) = \delta_{d,p}(E_d[2])$$

for each prime $p \mid d$ such that both $p \notin \Sigma$ and p splits in K/\mathbb{Q} . Since $\mathcal{S}(E_d/\mathbb{Q}_p)$ is its own orthogonal complement under the local Tate pairing, (x_1, x_2) is in $\mathcal{S}(E_d/\mathbb{Q}_p)$ 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 (7.5) 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 (7.4), (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. □

8 | PROOF OF THEOREM 6.1

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

$$E/\mathbb{Q} : y^2 = (x - a_1)(x - a_2)(x - a_3) \tag{8.1}$$

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 5.1.

The aim of this section is to prove Theorem 6.1. Specifically, we will show the following, strictly stronger, result.

Theorem 8.2. *We have*

$$\#\{d \text{ squarefree} : |d| < X, \text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) \neq 0\} \ll X \log(X)^{-0.0394}.$$

In particular

$$\lim_{X \rightarrow \infty} \frac{\#\{d \text{ squarefree} : |d| < X, \text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2]) = 0\}}{\#\{d \text{ squarefree} : |d| < X\}} = 1.$$

8.1 | First reduction

To prove Theorem 8.2, it suffices to prove the identical result for $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ (cf. Definition 7.6) in place of $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$, 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 7.8. We first introduce some notation.

Notation 8.3. We introduce the following three sets of primes:

$$\mathcal{P}_0 := \{p \notin \Sigma, \text{ } p \text{ split in } K/\mathbb{Q}, \text{ and } p \text{ non-split } \mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}\},$$

$$\mathcal{P}_1 := \{p \notin \Sigma, \text{ } p \text{ split in } K/\mathbb{Q}, \text{ and } p \text{ split in } \mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}\},$$

$$\mathcal{P}_2 := \{p \notin \Sigma, \text{ } p \text{ inert in } K/\mathbb{Q}\}.$$

(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 8.4. 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 8.5. For d a squarefree integer, define the subgroup S_d of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ as follows. First, write (uniquely) $d = ad_0 d_1 d_2$ 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

$$S_d := \left\{ x \text{ squarefree} : \begin{array}{l} x \mid N d_0 d_1, \\ \left(\frac{x}{p}\right) = 1 \text{ for all } p \mid d_2, \\ (x, d\alpha)_p = 1 \text{ for all } p \mid d_1 \end{array} \right\}.$$

We allow x to be either positive or negative.

Lemma 8.6. *If a pair of squarefree integers (x_1, x_2) is in $\text{Sel}_{\widetilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$, then $x_1 \in S_d$.*

Proof. Immediate from Proposition 7.8, noting that for $p \mid d_1$, since p is split in $\mathbb{Q}(\sqrt{\alpha\beta})/\mathbb{Q}$ by assumption, the condition $(x_1, d\alpha)_p(x_2, \alpha\beta)_p = 1$ simply becomes $(x_1, d\alpha)_p = 1$. \square

We will show the following. As explained below, this is sufficient to prove Theorem 8.2.

Theorem 8.7. *We have*

$$\#\{d \text{ squarefree} \mid |d| < X, S_d \neq \emptyset\} \ll X \log(X)^{-0.0394}.$$

Proof of Theorem 8.2 assuming Theorem 8.7. Theorem 8.7 combined with Lemma 8.6 shows that the x_1 -coordinate of any element of $\text{Sel}_{\widetilde{\mathcal{C}}_d}(\mathbb{Q}, E_d[2])$ 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 Equation (7.1) for our elliptic curve in order to interchange the roles of x_1 and x_2 . This shows the limit statement of Theorem 8.2, and running the same argument but keeping track of error terms proves the general result. \square

We now begin preparations for the proof of Theorem 8.7.

8.2 | Notation and preparations

Notation 8.8. 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 8.9. *Let a_0, a_1 and a_2 be non-negative real numbers. Then we have*

$$\sum_{\substack{X-Y < n \leq X \\ n \text{ squarefree}}} a_0^{\omega_0(n)} a_1^{\omega_1(n)} a_2^{\omega_2(n)} \ll \begin{cases} Y \log(X)^{\frac{a_0}{4} + \frac{a_1}{4} + \frac{a_2}{2} - 1} & \mathbb{Q}(\sqrt{\alpha\beta}) \not\subseteq K, \\ Y \log(X)^{\frac{a_1}{2} + \frac{a_2}{2} - 1} & \mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K, \end{cases}$$

uniformly for $2 \leq X \exp(-\sqrt{\log(X)}) \leq Y \leq X$.

Proof. This follows from a (significantly more general) result of Shiu [32]. Define the multiplicative function $f : \mathbb{Z} \rightarrow \mathbb{R}_{\geq 0}$ 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 8.4 that we have

$$\sum_{p \leq X} \frac{f(p)}{p} \sim \begin{cases} \left(\frac{a_0}{4} + \frac{a_1}{4} + \frac{a_2}{2} \right) \log \log(X) & \mathbb{Q}(\sqrt{\alpha\beta}) \not\subseteq K, \\ \left(\frac{a_1}{2} + \frac{a_2}{2} \right) \log \log(X) & \mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K. \end{cases}$$

The result now follows from [32, Theorem 1] (conditions (i) and (ii) needed for that theorem follow in our setting from well-known bounds on the divisor function). \square

8.3 | Reduction to computing a weighted average

To prove Theorem 8.7, we will compute bounds for a certain weighted average of $\#(S_d \setminus \{1\})$. Specifically, we will prove the following.

Proposition 8.10. *For any $1 < \gamma < 7/8 + \sqrt{17}/8 = 1.3903\dots$, we have*

$$\sum_{|d| < X, d \text{ squarefree}} \gamma^{\omega_2(d) - \omega_0(d)} (\#S_d - 1) = o(X). \quad (8.11)$$

Moreover, for $\gamma = 1/4 + \sqrt{17}/4$ the left-hand side of (8.11) is $\ll X \log(X)^{-0.0394}$.

We begin by showing that this is sufficient to prove Theorem 8.7.

Proof of Theorem 8.7 assuming Proposition 8.10. 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 8.9, 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

$$\begin{aligned} \#\{|d| \leq X \mid S_d \neq 0\} &\leq \#\{|d| \leq X \mid \omega_0(d) \geq \omega_2(d)\} + \\ &\quad \#\{|d| \leq X \mid S_d \neq 0, \omega_2(d) > \omega_0(d)\} \\ &\ll X \log(X)^{-0.042} + \sum_{|d| \leq X} \gamma^{\omega_2(d) - \omega_0(d)} (\#S_d - 1), \end{aligned}$$

where above d is implicitly taken squarefree. The result now follows from Proposition 8.10. \square

Remark 8.12. The reason for the introduction of the weight γ is that, in passing from the group $\text{Sel}_{\mathcal{C}_d}(\mathbb{Q}, E_d[2])$ 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.

8.4 | Strategy of the proof of Proposition 8.10

The proof of Proposition 8.10 follows closely the argument of [8, Section 5], which has its origins in the work of Heath–Brown [12, 13]. 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 8.10 as a sum of Jacobi symbols. We do this in Lemma 8.14, using ideas from [8, Lemma 16]. The resulting sum, given in (8.22), is structurally similar to the one in [8, 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, while 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 [8, Section 5.6] can be avoided. On the other hand, the variables D_i in [8, Section 5] are allowed to vary over all positive squarefree integers, while 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 Sections 8.6.7 and 8.6.6, respectively.

8.5 | Expressing the sum in terms of Jacobi symbols

We now begin preparations for the proof of Proposition 8.10 by expressing the relevant sum in terms of Jacobi symbols. We first define the following sums which will be ubiquitous in what follows.

Definition 8.13. 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 odd 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

$$S_\gamma(\lambda, \eta, X) := \sum_{\substack{D_0, D_1 \in \mathcal{F}_0 \\ D_2, D_3, D_4, D_5 \in \mathcal{F}_1 \\ D_6, D_7 \in \mathcal{F}_2 \\ \prod_i D_i \leq X \\ D_i \text{ coprime}}} \gamma^{-\omega(D_0 D_1)} 2^{-\omega(D_2 D_3 D_4 D_5)} (2/\gamma)^{-\omega(D_6 D_7)} \mathcal{J}_{\eta, \lambda}((D_i)_{0 \leq i \leq 7}),$$

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 8.14. For any positive real number γ , we have

$$\sum_{|d| < X, d \text{ squarefree}} \gamma^{\omega_2(d) - \omega_0(d)} (\#S_d - 1) = \sum_{a|N} \sum_{x_N|N} S_\gamma(x_N, -ax_N \alpha, X/a), \quad (8.15)$$

where the right-hand sums run over both positive and negative divisors of N .

Proof. Fix d squarefree. As in Definition 8.5, we write $d = ad_0d_1d_2$ where $d_i \in \mathcal{F}_i$ for $i = 0, 1, 2$, so that

$$S_d = \left\{ x \text{ squarefree} : \begin{array}{l} x|Nd_0d_1, \\ \left(\frac{x}{p}\right)=1 \text{ for all } p|d_2, \\ (x, d\alpha)_p=1 \text{ for all } p|d_1. \end{array} \right\}.$$

Now fix $x | Nd_0d_1$ and note that we have

$$2^{-\omega(d_2)} \sum_{z_2|d_2} \left(\frac{x}{z_2}\right) = 2^{-\omega(d_2)} \prod_{p|d_2} \left(1 + \left(\frac{x}{p}\right)\right) = \begin{cases} 1 & \left(\frac{x}{p}\right) = 1 \text{ for all } p | d_2 \\ 0 & \text{else,} \end{cases} \quad (8.16)$$

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 $x_N | N$ (and may be negative) $x_0 | d_0$ and $x_1 | d_1$. Say $d_0 = x_0 y_0$ and $d_1 = x_1 y_1$. Then for $p | d_1$, we have (noting that d_1 and α are coprime and that all $p | d_1$ are odd)

$$(x, d\alpha)_p = \begin{cases} \left(\frac{x}{p}\right) & p | y_1 \\ (x, -x d\alpha)_p = \left(\frac{-a x_N y_0 y_1 d_2 \alpha}{p}\right) & p | x_1. \end{cases}$$

Thus, similarly to (8.16), we have

$$2^{-\omega(x_1 y_1)} \sum_{\substack{w_1|x_1 \\ z_1|y_1}} \left(\frac{x}{z_1}\right) \left(\frac{-a x_N y_0 y_1 d_2 \alpha}{w_1}\right) = \begin{cases} 1 & (x, d\alpha)_p = 1 \text{ for all } p | d_1 \\ 0 & \text{else.} \end{cases} \quad (8.17)$$

We now multiply (8.16) and (8.17), write $d_2 = z_2 z'_2$, $x_1 = w_1 w'_1$, and $y_1 = z_1 z'_1$, and sum over all $x = x_N x_0 x_1$ dividing Nd_0d_1 to find

$$\#S_d = \sum_{x_N|N} \sum_{\substack{x_0 y_0 = d_0 \\ w_1 w'_1 z_1 z'_1 = d_1 \\ z_2 z'_2 = d_2}} 2^{-\omega(w_1 w'_1 z_1 z'_1 z_2 z'_2)} \left(\frac{x_N x_0 w_1 w'_1}{z_2}\right) \left(\frac{x_N x_0 w_1 w'_1}{z_1}\right) \left(\frac{-a x_N y_0 z_1 z'_1 z_2 z'_2 \alpha}{w_1}\right),$$

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 $\omega_0(d) = \omega(x_0 y_0)$ and $\omega_2(d) = \omega(z_2 z'_2)$. Moreover, the identity element in S_d corresponds to $x_N = x_0 = w_1 = w'_1 = 1$. Thus, 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 $|d| \leq X$, weighted by $\gamma^{\omega_2(d) - \omega_0(d)}$, and relabel variables $(x_0, y_0, w_1, w'_1, z_1, z'_1, z_2, z'_2) = (D_0, D_1, D_2, D_3, D_4, D_5, D_6, D_7)$. \square

Remark 8.18. The proof above shows that the reason for excluding the terms where $\lambda = D_0 = D_2 = D_3 = 1$ in the definition of $S_\gamma(\lambda, \eta, X)$ 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 8.10. In light of Lemma 8.14, we want to study the sums $S_\gamma(\lambda, \eta, X)$.

Definition 8.19. 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

$$\{1, 2\}, \{2, 5\}, \{2, 7\}, \{0, 4\}, \{3, 4\}, \{0, 6\}, \{3, 6\}. \quad (8.20)$$

Notation 8.21. To write the sums $S_\gamma(\lambda, \eta, X)$ 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 $\mathcal{D}(X)$ denote the set of tuples of pairwise coprime positive integers (D_0, \dots, 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

$$S_\gamma(\lambda, \eta, X) = \sum_{(D_i) \in \mathcal{D}(X)} \prod_i \kappa_i^{-\omega(D_i)} \prod_i \left(\frac{\eta}{D_i}\right)^{\mu_i} \left(\frac{\lambda}{D_i}\right)^{\nu_i} \prod_{i \neq j} \left(\frac{D_i}{D_j}\right)^{\Phi(i, j)}. \quad (8.22)$$

We also define n_i ($0 \leq i \leq 7$), so that the D_i are required to lie in \mathcal{F}_{n_i} (for example, $n_0 = n_1 = 0$).

8.6 | Bounds on the sums $S_\gamma(\lambda, \eta, X)$

Proposition 8.23. For any $1 < \gamma < 7/8 + \sqrt{17}/8$, and for any (positive or negative) divisors λ and η of N , we have $S_\gamma(\lambda, \eta, X) = o(X)$. Moreover, when $\gamma = 1/4 + \sqrt{17}/4$ we have

$$S_\gamma(\lambda, \eta, X) \ll X \log(X)^{-0.0394}.$$

It is immediate from Lemma 8.14 that Proposition 8.23 implies Proposition 8.10 and so, via Theorem 8.7, we obtain Theorem 8.2. The rest of the section is occupied with the proof of Proposition 8.23.

8.6.1 | 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 $S_\gamma(\theta, \eta, X)$ 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 (8.22) 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 $(\frac{\theta}{n}) = \mu(n)$. On the other hand, we similarly have $(\frac{\theta}{n}) = 1$ for all $n \in \mathcal{F}_1$. Consequently, the contribution to $S_\gamma(\theta, \eta, X)$ from tuples with $D_0 = D_2 = D_3 = 1$ is given by

$$\sum_{\substack{(D_i) \in \mathcal{D}(X) \\ D_0, D_2, D_3 = 1}} \mu(D_6) \prod_{i \neq 0, 2, 3} \kappa_i^{-\omega(D_i)} = \sum_{\substack{r \in \mathcal{F}_0 \cdot \mathcal{F}_1 \\ r \leq X}} \gamma^{-\omega_0(r)} \sum_{\substack{n \in \mathcal{F}_2 \\ n \leq X/r}} \gamma^{\omega(n)} \sum_{m|n} \mu(m). \quad (8.24)$$

In the above, to pass from the left-hand side to the right-hand side we have set $r = D_1 D_4 D_5$ and $n = D_6 D_7$, noting that, for example, given $r \in \mathcal{F}_0 \cdot \mathcal{F}_1$ there are $2^{\omega_1(r)}$ ways of writing r as a product $D_1 D_4 D_5$ 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

$$|\text{RHS of (8.24)}| = \sum_{\substack{r \in \mathcal{F}_0 \cdot \mathcal{F}_1 \\ r \leq X}} \gamma^{-\omega_0(r)} \ll X \log(X)^{-1/2} \quad (8.25)$$

where for the bound we are using Lemma 8.9.

8.6.2 | 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 in Section 8.6.6. Set $\Omega = 4e \cdot (\log \log(X) + B_0)$ with B_0 as in [8, Lemma 11], and let Σ_1 be the contribution to $S_\gamma(\lambda, \eta, X)$ from the tuples $(D_i) \in \mathcal{D}(X)$ satisfying

$$\omega(D_i) \geq \Omega \quad \text{for some } 0 \leq i \leq 7. \quad (8.26)$$

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 [11, Lemma A] as in [8, Section 5.3] (paragraph above Equation (30)) we find $\Sigma_1 \ll X \log(X)^{-1}$.

8.6.3 | Ranges of the variables

We now divide the ranges of summation into intervals, and treat these intervals separately. Specifically, we set

$$\Delta := 1 + \frac{1}{\log(X)^2} \quad (8.27)$$

and divide the ranges of the variables into intervals $[\Delta^n, \Delta^{n+1}]$ for $n = 0, 1, 2, \dots$, noting that 1 is the only integer in the $n = 0$ interval. For $i = 0, \dots, 7$ 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

$$S_\gamma(\lambda, \eta, X, \mathbf{A}) = \sum_{\substack{(D_i) \in \mathcal{D}'(X) \\ A_i \leq D_i \leq \Delta A_i}} \prod_i \kappa_i^{-\omega(D_i)} \prod_i \left(\frac{\eta}{D_i} \right)^{\mu_i} \left(\frac{\lambda}{D_i} \right)^{\nu_i} \prod_{i \neq j} \left(\frac{D_i}{D_j} \right)^{\Phi(i,j)}, \quad (8.28)$$

where, in light of Section 8.6.2 and (8.25), we define $\mathcal{D}'(X)$ to be the subset of $\mathcal{D}(X)$ 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 (8.28) as \mathbf{A} varies.

Following [8, Section 5.4], we split the collection of all \mathbf{A} into families and treat each in turn.

8.6.4 | First family: $\prod_i A_i$ large

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 $\prod_i D_i \leq X$ is relevant. Specifically, the first family of the \mathbf{A} is defined by the condition

$$\prod_{0 \leq i \leq 7} A_i \geq \Delta^{-8} X. \quad (8.29)$$

The argument here is essentially identical to that occurring between Equations (33) and (34) of [8]: we have

$$\begin{aligned} \sum_{\mathbf{A} \text{ satisfies (8.29)}} |S_\gamma(\lambda, \eta, X, \mathbf{A})| &\leq \sum_{\mathbf{A} \text{ satisfies (8.29)}} \sum_{\substack{(D_i) \in \mathcal{D}'(X) \\ A_i \leq D_i \leq \Delta A_i}} \prod_i \kappa_i^{-\omega(D_i)} \\ &\leq \sum_{\Delta^{-8} X \leq n \leq X} 2^{\omega(n)} \\ &\ll (1 - \Delta^{-8}) X \log(X) \\ &\ll X \log(X)^{-1} \end{aligned}$$

where for the last inequality we are using

$$1 - \Delta^{-8} = 1 - (1 + \log(X)^{-2})^{-8} = 1 - (1 - 8 \log(X)^{-2} + O(\log(X)^{-4})) \ll \log(X)^{-2}.$$

Note that if \mathbf{A} does not satisfy (8.29) 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.

8.6.5 | 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

$$\prod_{0 \leq k \leq 7} A_k \leq \Delta^{-8} X, \text{ and there exist linked indices } i \neq j \text{ with } A_i, A_j \geq X^\dagger. \quad (8.30)$$

Here the argument is almost identical to that given between Equations (40) and (42) in [8], ultimately relying on a result of Heath-Brown exploiting double oscillations of characters [14, Corollary 4]. For such \mathbf{A} , since i and j are linked we have (swapping i and j if necessary)

$$|S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll \sum_{\substack{A_k \leq D_k \leq \Delta A_k \\ k \neq i, j}} \prod_{k \neq i, j} \kappa_k^{-\omega(D_k)} \left| \sum_{\substack{1 \leq D_i \leq \Delta A_i \\ 1 \leq D_j \leq \Delta A_j}} f(D_i; (D_k)_{k \neq i, j}) g(D_j; (D_k)_{k \neq i, j}) \left(\frac{D_i}{D_j} \right) \right|,$$

where in the inner sum D_i and D_j are odd coprime integers with no further constraints,

$$f(D_i; (D_k)_{k \neq i, j}) = 1_{\substack{D_i \in \mathcal{F}_{n_i} \\ D_i \geq A_i \\ \omega(D_i) \leq \Omega}} \cdot \kappa_i^{-\omega(D_i)} \mu^2 \left(D_i \prod_{k \neq i, j} D_k \right) \left(\frac{\eta}{D_i} \right)^{\mu_i} \left(\frac{\lambda}{D_i} \right)^{v_i} \prod_{k \neq i, j} \left(\frac{D_i}{D_k} \right)^{\Phi(i, k)} \left(\frac{D_k}{D_i} \right)^{\Phi(k, i)}$$

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 [8, Lemma 15] (with $\epsilon = 1/6$) to the inner sum above, and summing over the remaining variables, gives

$$|S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll \Delta^2 A_i A_j (X^\dagger)^{-1/3} \cdot \prod_{k \neq i, j} \Delta A_k \leq X (X^\dagger)^{-1/3}. \quad (8.31)$$

Summing over each of the $\ll \log(X)^{24}$ possibilities for \mathbf{A} we find

$$\sum_{\mathbf{A} \text{ satisfies (8.30)}} |S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll X \log(X)^{-1}. \quad (8.32)$$

8.6.6 | Third family: One large and one small factor corresponding to linked indices

We introduce a further parameter $X^\ddagger = \exp(\log(X)^\epsilon)$ for fixed $\epsilon > 0$ (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

$$\text{Neither (8.29) nor (8.30) hold, and } \exists i \neq j \text{ linked with } 1 < A_j < X^\dagger \text{ and } A_i \geq X^\ddagger. \quad (8.33)$$

This section of the argument corresponds to the treatment of Fouvry–Klüners fourth family [8, Equations (43)–(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 [9, Section 7.5].

Fix such an \mathbf{A} . In the definition of $S_\gamma(\lambda, \eta, X, \mathbf{A})$, 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

$$\left(\frac{\eta}{D_i}\right)^{\mu_i} \left(\frac{\lambda}{D_i}\right)^{\nu_j} \prod_{k \neq i} \left(\frac{D_i}{D_k}\right)^{\Phi(i,k)} \left(\frac{D_k}{D_i}\right)^{\Phi(k,i)} = \chi_{i, (D_k)_{k \neq i}}(D_i) \prod_{k \neq i} \left(\frac{D_i}{D_k}\right)^{\Phi(i,k) + \Phi(k,i)} \quad (8.34)$$

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

$$|S_\gamma(\lambda, \eta, X, \mathbf{A})| \leq \sum_{\substack{A_k \leq D_k \leq \Delta A_k \\ k \neq i}} \prod_{k \neq i} \kappa_k^{-\omega(D_k)} \left| \sum_{\substack{A_i \leq D_i \leq \Delta A_i \\ D_i \text{ coprime to } (D_k)_{k \neq i}}} \kappa_i^{-\omega(D_i)} \chi_{i, (D_k)_{k \neq i}}(D_i) \left(\frac{D_i}{d}\right) \right| \quad (8.35)$$

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 (8.30) does not hold.

Replacing the inner sum in (8.35) with its maximum possible value we have

$$|S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll \frac{X}{\Delta A_i} \cdot \max_{a, \chi, q} \left| \sum_{\substack{A_i \leq D_i \leq \Delta A_i \\ (a, D_i) = 1 \\ D_i \in \mathcal{F}_{n_i}, \omega(D_i) \leq \Omega}} \kappa_i^{-\omega(D_i)} \chi(D_i) \right|, \quad (8.36)$$

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

$$\max_{a, \chi, q} \left| \sum_{\substack{A_i \leq D_i \leq \Delta A_i \\ (a, D_i) = 1 \\ D_i \in \mathcal{F}_{n_i}, \omega(D_i) \leq \Omega}} \kappa_i^{-\omega(D_i)} \chi(D_i) \right| \leq \sum_{1 \leq l \leq \Omega} \sum_{\substack{n \\ \omega(n) = l-1}} \max_{a, \chi, q} \left| \sum_{\substack{\max(P^+(n), A_i/n) < p < \Delta A_i/n \\ (a, p) = 1 \\ p \in \mathcal{P}_{n_i}}} \chi(p) \right|, \quad (8.37)$$

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

$$\left| \sum_{p|a} \mathbb{1}_{\mathcal{P}_{n_i}}(p) \chi(p) \right| \leq \omega(a) \ll \log(X)$$

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 (8.37) 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 $3 \leq q' \ll (\Delta X^\dagger)^7$ also. By the triangle inequality and [8, Lemma 13] (a consequence of the Siegel–Walfisz theorem) we conclude that for all constants $A > 0$ we have

$$\begin{aligned} \max_{a, \chi, q} \left| \sum_{\substack{\max(P^+(n), A_i/n) < p < \Delta A_i/n \\ (a, p)=1 \\ p \in \mathcal{P}_{n_i}}} \chi(p) \right| &\ll \max_{a, \chi, q} \left| \sum_{\max(P^+(n), A_i/n) < p < \Delta A_i/n} \chi(p) \right| + \log(X) \quad (8.38) \\ &\ll_A (X^\dagger)^4 \cdot \frac{\Delta A_i}{n} \cdot \log(A_i/n)^{-A} + \log(X). \end{aligned}$$

Now n has at most Ω prime factors, so the sum on the left of (8.38) is non-empty only if $n \leq \Delta A_i^{1-1/\Omega}$, in which case

$$\log(A_i/n)^{-A} \ll \log(A_i^{1/\Omega})^{-A} \ll \left(\frac{1}{\Omega} \log(X)^\epsilon \right)^{-A} \ll \log(X)^{-\epsilon A}.$$

We now insert this into Equation (8.38), and insert the result into Equation (8.37) and finally Equation (8.36), to find

$$\begin{aligned} |S_\gamma(\lambda, \eta, X, \mathbf{A})| &\ll_A \frac{X}{\Delta A_i} \cdot \sum_{1 \leq n \leq \Delta A_i^{1-1/\Omega}} \left[(X^\dagger)^4 \cdot \frac{\Delta A_i}{n} \cdot \log(X)^{-\epsilon A} + \log(X) \right] \\ &\ll_A X \log(X)^{1-\epsilon A} (X^\dagger)^4 + \frac{X \log(X)^1}{(X^\dagger)^{1/\Omega}}. \end{aligned}$$

Summing over the $\ll \log(X)^{24}$ possibilities for \mathbf{A} and recalling that $\Omega \ll \log \log(X)$, we find

$$\sum_{\mathbf{A} \text{ satisfies (8.33)}} |S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll X \log(X)^{-1}$$

provided A is chosen large enough (compared to ϵ).

8.6.7 | Remaining families

We now consider those \mathbf{A} such that

$$\text{none of (8.29), (8.30), or (8.33) hold.} \quad (8.39)$$

Here the argument deviates significantly from that in [8]. Fix such an \mathbf{A} , and define

$$\mathcal{I}_{\mathbf{A}} := \{0 \leq i \leq 7 \mid A_i \geq X^{\frac{1}{2}}\}.$$

Recalling that $X^{\frac{1}{2}} > X^{\frac{1}{4}}$ (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

$$|S_{\gamma}(\lambda, \eta, X, \mathbf{A})| \leq \sum_{\substack{(D_i) \in \mathcal{D}'(X) \\ A_i \leq D_i \leq \Delta A_i}} \prod_i \kappa_i^{-\omega(D_i)}. \quad (8.40)$$

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

$$\sum_{\substack{\mathbf{A} \text{ satisfies (8.39)} \\ \mathcal{I}_{\mathbf{A}} = I}} |S_{\gamma}(\lambda, \eta, X, \mathbf{A})| \leq \sum_{n \leq (\Delta X^{\frac{1}{2}})^8} 2^{\omega(n)} \sum_{m \leq X/n} \frac{i_0^{\omega_0(m)}}{\gamma^{\omega_0(m)}} \cdot \frac{i_1^{\omega_1(m)}}{2^{\omega_1(m)}} \cdot \frac{i_2^{\omega_2(m)}}{(2/\gamma)^{\omega_2(m)}}. \quad (8.41)$$

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 (8.41) we apply Lemma 8.9. Here the argument splits 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 8.48.

Assumption 8.42. Assume henceforth that $\mathbb{Q}(\sqrt{\alpha\beta}) \not\subseteq K$.

Applying Lemma 8.9 to the right-hand side of (8.41), we obtain

$$\begin{aligned} \sum_{\substack{\mathbf{A} \text{ satisfies (8.39)} \\ \mathcal{I}_{\mathbf{A}} = I}} S_{\gamma}(\lambda, \eta, X, \mathbf{A}) &\ll \sum_{n \leq (\Delta X^{\frac{1}{2}})^8} 2^{\omega(n)} \frac{X}{n} \log(X/n)^{i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1} \\ &\ll X \log(X)^{i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1} \sum_{n \leq (\Delta X^{\frac{1}{2}})^8} \frac{2^{\omega(n)}}{n} \\ &\ll X \log(X)^{i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon} \end{aligned}$$

with the last \ll following from the bound $\sum_{n \leq Y} \frac{2^{\omega(n)}}{n} \ll \log(Y)^2$ (to prove this, for example, square the bound $\sum_{n \leq Y} \frac{1}{n} \ll \log(Y)$). We now study the exponent $i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon$

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 have 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

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon \leq -1/4 + 2\epsilon.$$

- $I \subseteq \mathcal{I}_2$. Here $i_0 \leq 1, i_1 \leq 2$ and $i_2 = 0$, so that

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon \leq -1/2 + 2\epsilon.$$

- $I \subseteq \mathcal{I}_3$. Here $i_0 \leq 2, i_1 \leq 2$ and $i_2 \leq 1$. Then

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon \leq 1/(2\gamma) + \gamma/4 - 3/4 + 2\epsilon = \frac{(\gamma-1)(\gamma-2)}{4\gamma} + 2\epsilon.$$

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 three cases. First assume that $i_0 = 0$. Then

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon \leq \gamma/2 - 3/4 + 2\epsilon.$$

This is strictly negative for sufficiently small $\epsilon > 0$ since $\gamma < 3/2$. Next, assume that $i_1 \leq 1$. Then

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon \leq 1/(4\gamma) + \gamma/2 - 7/8 + 2\epsilon = \frac{4\gamma^2 - 7\gamma + 2}{8\gamma} + 2\epsilon.$$

The numerator has roots at $\gamma = 7/8 \pm \sqrt{17}/8 \approx 0.36, 1.39$. This is strictly negative for sufficiently small $\epsilon > 0$ 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

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon \leq 1/(4\gamma) + \gamma/4 - 3/4 + 2\epsilon = \frac{\gamma^2 - 3\gamma + 1}{4\gamma} + 2\epsilon.$$

In the range considered, the function $\frac{\gamma^2 - 3\gamma + 1}{4\gamma}$ is always less than its value at, for example, 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

$$\sum_{\substack{\mathbf{A} \text{ satisfies (8.39) \\ I_{\mathbf{A}}=I}} |S_{\gamma}(\lambda, \eta, X, \mathbf{A})| \ll X \log(X)^{-r_{\gamma}} \quad (8.43)$$

for some $r_{\gamma} > 0$, provided that $1 < \gamma < 7/8 + \sqrt{17}/8$.

Remark 8.44. Optimising the exponent r_γ over $1 < \gamma < 7/8 + \sqrt{17}/8$, we find that the best uniform upper bound for $i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon$ 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

$$i_0/(4\gamma) + i_1/8 + \gamma i_2/4 - 1 + 2\epsilon = \frac{1}{16}(3\sqrt{17} - 13) + 2\epsilon = 2\epsilon - 0.0394 \dots$$

8.6.8 | Completing the argument

Finally, it remains to consider \mathbf{A} satisfying eq. 8.39 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 $\mathcal{D}'(X)$ then excludes $\lambda = 1$ or $\lambda = \theta$. Putting $D_0 = D_2 = D_3 = 1$ into the definition of $S_\gamma(\lambda, \eta, X, \mathbf{A})$ we find

$$S_\gamma(\lambda, \eta, X, \mathbf{A}) = \sum_{\substack{(D_i) \in \mathcal{D}'(X) \\ A_i \leq D_i \leq \Delta A}} \left(\frac{\lambda}{D_4}\right) \left(\frac{\lambda}{D_6}\right) \prod_i \kappa_i^{-\omega(D_i)}, \quad (8.45)$$

where $A_4, A_6 \geq X^\dagger$ by assumption. We get cancellation in this sum via the Siegel–Walfisz theorem as in Section 8.6.6, 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 Section 8.6.6, we find

$$|S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll \frac{X \log(X)}{\Delta A_6} \max_{1 \leq a \leq X} \left| \sum_{\substack{A_6 \leq D_6 \leq \Delta A_6 \\ (a, D_6)=1}} \kappa_6^{-\omega(D_6)} \left(\frac{\lambda}{D_6}\right) \right|$$

and that the inner sum satisfies

$$\left| \sum_{\substack{A_6 \leq D_6 \leq \Delta A_6 \\ (a, D_6)=1}} \kappa_6^{-\omega(D_6)} \left(\frac{\lambda}{D_6}\right) \right| \leq \sum_{1 \leq l \leq \Omega} \sum_{\omega(n)=l-1}^n \left| \sum_{\substack{\max(P^+(n), A_6/n) < p < \Delta A_6/n \\ (a, p)=1 \\ p \in \mathcal{P}_3}} \left(\frac{\lambda}{p}\right) \right|. \quad (8.46)$$

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 $\frac{1}{2}(1 - (\frac{\theta}{p}))$. Inserting this into the sum, we may apply [8, Lemma 13] as in Section 8.6.6 since $\lambda \neq 1, \theta$ means that both $D \mapsto (\frac{\lambda}{D})$ and $D \mapsto (\frac{\lambda\theta}{D})$ are non-principal. Continuing to argue as in Section 8.6.6 yields

$$\sum_{\substack{\mathbf{A} \text{ satisfies (8.39) \\ \mathcal{I}_{\mathbf{A}} = \{1, 4, 5, 6, 7\}}} |S_\gamma(\lambda, \eta, X, \mathbf{A})| \ll X \log(X)^{-1}, \quad (8.47)$$

which completes the proof of Proposition 8.23.

Remark 8.48. Suppose instead (of Assumption 8.42) we have $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$. This time applying Lemma 8.9 to the right-hand side of (8.41) gives the bound

$$\sum_{\substack{\mathbf{A} \text{ satisfies (8.39)} \\ I_{\mathbf{A}}=I}} S_{\gamma}(\lambda, \eta, X, \mathbf{A}) \ll X \log(X)^{i_1/4 + i_2\gamma/4 - 1 + 2\epsilon}.$$

Splitting into cases according to which maximal unlinked subset I is contained in, one finds that in the first 3 cases, namely $I \subseteq I_i$ for $i = 1, 2, 3$, the exponent satisfies

$$i_1/4 + i_2\gamma/4 - 1 + 2\epsilon \leq -1/8 + 2\epsilon$$

provided $\gamma < 3/2$. In the final case where $I \subseteq I_4$, we note that $\mathbb{Q}(\sqrt{\alpha\beta}) \subseteq K$ forces $F_0 = \emptyset$, 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, for example, equal to $(\sqrt{17} - 5)/8 = -0.1096 \dots$ if one takes $\gamma = 1/4 + \sqrt{17}/4$ as in Remark 8.44. 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 in Section 8.6.8.

9 | PRIME TWISTS OF THE CONGRUENT NUMBER CURVE

In this section, we prove Theorem 1.9. That is, 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 4.8, $\text{Sel}_{\mathcal{E}_d}(\mathbb{Q}, E_d[2])$ 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 $\text{Sel}^2(E_p/K)$ as a $G = \text{Gal}(K/\mathbb{Q})$ -module.

For a place v of K , we will identify the local Kummer images $\mathcal{S}_v(E_p/K)$ of Section 2.4 with their image under the 2-descent map (7.5) (in our case, $a_1 = 0, a_2 = 1, a_3 = -1$), so that

$$\mathcal{S}_v(E_p/K) \subseteq K_v^\times / K_v^{\times 2} \times K_v^\times / K_v^{\times 2}.$$

We view the Selmer group $\text{Sel}^2(E_p/K)$ as a subgroup of $K^\times / K^{\times 2}$ similarly, noting that this identification respects the G -action.

For a vector space V and $v_1, \dots, v_n \in V$ we write $\langle v_1, v_2, \dots, v_n \rangle$ for the subspace generated by v_1, \dots, v_n .

9.1 | 2-Descent

Our primary goal is to characterise the groups $\text{Sel}^2(E_p/K)$ for p prime, which we do via 2-Descent. We first begin by identifying the local Kummer images at each prime.

Lemma 9.1. *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*

$$\mathcal{S}_v(E_p/K) = 0;$$

(ii) *if $v \nmid 2p$, then*

$$\mathcal{S}_v(E_p/K) = \langle (1, u), (u, 1) \rangle,$$

where u is any nonsquare unit in K_v ;

(iii) *if $v \mid p$, then*

$$\mathcal{S}_v(E_p/K) = \langle (-1, -p), (p, 2) \rangle;$$

(iv) *if $v = 2$ and $\zeta \in K_2$ is a primitive third root of unity, then*

$$\mathcal{S}_2(E_p/K) = \langle T_1, T_2, T_3, T_4 \rangle,$$

where

$$T_1 := (-1, -p),$$

$$T_3 := (\zeta + 3, \zeta + 3(1 + p)),$$

$$T_2 := (1, 2),$$

$$T_4 := (1, 4\zeta + 5).$$

Proof. Since K is imaginary, if $v \mid \infty$ the group $H^1(K_v, E[2])$ is trivial and so (i) holds. Lemma 7.2 then provides (ii) as $p \notin \Sigma$. To prove (iii), it is enough to note that by Lemma 5.2, since $\dim \mathcal{S}_v(E_p/K) = 2$, $\mathcal{S}_v(E_p/K) = \delta_v(E_p[2])$.

For $v = 2$, note first that $\dim((K_2^\times/K_2^{\times 2})^2) = 8$, so, as in Example 3.5, since $\mathcal{S}_p(E_p/K)$ is maximal isotropic with respect to the local Tate pairing we have $\dim \mathcal{S}_2(E_p/K) = 4$.

Let $x_3 = -(\zeta + 3)/3$ and $x_4 = -(3\zeta + 2)/3$. It is elementary to compute that

$$x_3^3 - p^2 x_3 \equiv -3\zeta \pmod{8} \quad x_4^3 - p^2 x_4 \equiv \zeta^2 \pmod{8}.$$

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 $\mathcal{S}_2(E_p/K)$. Since T_1, T_2, T_3 and T_4 are readily checked to be linearly independent, the result follows. \square

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 9.1, $p \nmid 2\theta$ is a prime, and we denote by ζ a fixed primitive third root of unity in K_2 . For x in K we denote its conjugate under the action of G as \bar{x} .

Lemma 9.2. *Suppose that p splits in K/\mathbb{Q} , and write $p = \epsilon\bar{\epsilon}$ for some $\epsilon \in \mathcal{O}_K$. Then in K_2^\times we have*

$$\epsilon \equiv \pm(\zeta + 2 - p) \pmod{K_2^{\times 2}}.$$

(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 $\mathbb{Z}_2[\zeta]^\times$ 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 $\epsilon \pmod{K_2^{\times 2}}$ in this form we find that, in $K_2^\times/K_2^{\times 2}$, we have

$$p = N_{K_2/\mathbb{Q}_2}(\epsilon) = (a \pm \zeta)(a \pm \zeta^2) = 2 \mp a.$$

Thus, $a \equiv \pm(2 - p) \pmod{8}$ and the result follows. \square

We are now ready to describe the Selmer groups. In the statement, all isomorphisms are as $\mathbb{F}_2[G]$ -modules.

Proposition 9.3. *Let p be an odd prime not dividing θ . Then:*

(i) *if p is inert in K/\mathbb{Q} , we have*

$$\text{Sel}^2(E_p/K) \cong \mathbb{F}_2^4;$$

(ii) *if p is split in K/\mathbb{Q} and $\epsilon \in \mathcal{O}_K$ has norm p , we have*

$$\text{Sel}^2(E_p/K) \cong \begin{cases} \mathbb{F}_2^2 \oplus \mathbb{F}_2[G] & p \equiv 5, 7 \pmod{8}, \\ \mathbb{F}_2^2 & p \equiv 3 \pmod{8}, \\ \mathbb{F}_2^2 \oplus \mathbb{F}_2[G]^2 & p \equiv 1 \pmod{8} \text{ and } \bar{\epsilon} \in K_\epsilon^{\times 2}, \\ \mathbb{F}_2^4 & p \equiv 1 \pmod{8} \text{ and } \bar{\epsilon} \notin K_\epsilon^{\times 2}. \end{cases}$$

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

$$((-1)^{a_1} 2^{a_2} p^{a_3}, (-1)^{b_1} 2^{b_2} p^{b_3}) \quad (9.4)$$

lies in both of the local groups $\mathcal{S}_p(E_p/K)$ and $\mathcal{S}_2(E_p/K)$ described in Lemma 9.1. 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 (9.4) lie in $\mathcal{S}_p(E_p/K)$. 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 (9.4) which lies in $\text{Sel}^2(E_p/K)$ necessarily maps to the subspace of $\mathcal{S}_2(E_p/K)$ generated by $T_1 = (-1, -p)$ and $T_2 = (1, 2)$. Restricting to elements of the form (9.4) which do map to this space gives

$$\text{Sel}^2(E_p/K) = \langle (p, 2), (-1, -p), (1, (-1)^\delta p), ((-1)^\delta p, 1) \rangle \cong \mathbb{F}_2^4$$

where $\delta = 1$ if $p \notin K_2^{\times 2}$ and $\delta = 0$ otherwise.

Now suppose p splits in K/\mathbb{Q} , and fix $\epsilon \in K^\times$ such that $\epsilon\bar{\epsilon} = p$. As above, the 2-Selmer elements are unramified outside $\{2, \epsilon, \bar{\epsilon}\}$, so we want to find all $a_i, b_i \in \{0, 1\}$ for which

$$((-1)^{a_1} 2^{a_2} \epsilon^{a_3} \bar{\epsilon}^{a_4}, (-1)^{b_1} 2^{b_2} \epsilon^{b_3} \bar{\epsilon}^{b_4}) \quad (9.5)$$

lies in each of the groups $\mathcal{S}_\epsilon(E_p/K)$, $\mathcal{S}_{\bar{\epsilon}}(E_p/K)$ and $\mathcal{S}_2(E_p/K)$ described in Lemma 9.1. 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 9.1:

$$\mathcal{S}_2(E_p/K) = \langle (-1, -p), (1, 2), (\zeta + 3, \zeta + 3(1 + p)), (1, 4\zeta + 5) \rangle$$

$$\mathcal{S}_\epsilon(E_p/K) = \langle (-1, -\epsilon\bar{\epsilon}), (\epsilon\bar{\epsilon}, 2),$$

$$\mathcal{S}_{\bar{\epsilon}}(E_p/K) = \langle (-1, -\epsilon\bar{\epsilon}), (\epsilon\bar{\epsilon}, 2) \rangle.$$

We now break into cases.

$p \equiv -1 \pmod{8}$: Here -1 is nonsquare in K_ϵ . Replacing ϵ with $-\epsilon$ if necessary, we assume $\bar{\epsilon} \in K_\epsilon^{\times 2}$. Note also that 2 is a square in K_ϵ . By symmetry, this gives $2, \epsilon \in K_\epsilon^{\times 2}$. The elements of the form (9.5) which lie in $\mathcal{S}_\epsilon(E_p/K)$ are then those of the shape

$$((-1)^{a_1} 2^{a_2} \epsilon^{a_3} \bar{\epsilon}^{a_4}, (-\epsilon)^{a_1} 2^{b_2} \bar{\epsilon}^{b_4}).$$

Reducing further to those that satisfy the conditions of $\mathcal{S}_{\bar{\epsilon}}(E_p/K)$ we are left with elements of the shape

$$((-1)^{a_1} 2^{a_2} \epsilon^{a_3} \bar{\epsilon}^{a_4}, (-\epsilon\bar{\epsilon})^{a_1} 2^{b_2}). \quad (9.6)$$

Finally, as $p \equiv -1 \pmod{8}$ we have

$$\mathcal{S}_2(E_p/K) = \langle (-1, 1), (1, 2), (\zeta + 3, 1), (1, 4\zeta + 5) \rangle.$$

Since the first coordinate of each of these basis vectors has valuation 0, we must have $a_2 = 0$. Further, Lemma 9.2 gives $\epsilon \equiv \pm(\zeta + 2 - p) \equiv \pm(\zeta + 3)$ in $K_2^\times/K_2^{\times 2}$, and since $\epsilon\bar{\epsilon} = p \equiv -1 \pmod{K_2^{\times 2}}$ we have $\bar{\epsilon} \equiv \mp(\zeta + 3)$. It follows that each of the elements

$$(\epsilon, 1), (\bar{\epsilon}, 1), (1, 2), (-1, -\epsilon\bar{\epsilon})$$

are in $\text{Sel}^2(E_p/K)$. Since each element of the form (9.6) with $a_2 = 0$ can be written as a linear combination of these Selmer elements, we have

$$\begin{aligned}\text{Sel}^2(E_p/K) &= \langle (1, 2), (-1, -\epsilon\bar{\epsilon}), (\epsilon, 1), (\epsilon\bar{\epsilon}, 1) \rangle \\ &\cong \mathbb{F}_2^2 \oplus \mathbb{F}_2[G].\end{aligned}$$

$p \equiv 3 \pmod{8}$: Again, -1 is nonsquare in K_ϵ so we assume $\bar{\epsilon} \in K_\epsilon^{\times 2}$. Additionally, 2 is nonsquare in K_ϵ , hence -2 is a square. With ϵ and $\bar{\epsilon}$ swapped this all remains true.

The elements of the form (9.5) which lie in $\mathcal{S}_\epsilon(E_p/K)$ are thus those of the shape

$$((-2)^{a_2}\bar{\epsilon}^{a_4}(-1)^{b_3}\epsilon^{a_3}, (-2)^{b_2}\bar{\epsilon}^{b_4}(-1)^{a_3}(-\epsilon)^{b_3}).$$

Reducing further to those that satisfy the conditions of $\mathcal{S}_\epsilon(E_p)$ we are left with

$$((-2)^{a_2}(-1)^{b_3}(\epsilon\bar{\epsilon})^{a_3}, (-2)^{b_2}(-\epsilon\bar{\epsilon})^{b_3}(-1)^{a_3}). \quad (9.7)$$

Finally, we apply the conditions at 2 . By Lemma 9.2 we have $\epsilon \equiv \pm(\zeta - 1) \pmod{K_2^{\times 2}}$. As $p \equiv 3 \pmod{8}$ we have

$$\mathcal{S}_2(E_p/K) = \langle (-1, 1), (1, 2), (\zeta + 3, \zeta + 4), (1, 4\zeta + 5) \rangle.$$

Since the first coordinate of each basis element is a unit, we must have $a_2 = 0$. Considering the second coordinate, and noting that $\epsilon\bar{\epsilon} \equiv -1 \pmod{K_2^{\times 2}}$, 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

$$\begin{aligned}\text{Sel}^2(E_p/K) &= \langle (-1, -p), (p, 2) \rangle \\ &\cong \mathbb{F}_2^2.\end{aligned}$$

$p \equiv 5 \pmod{8}$: Here -1 is square in both K_ϵ and $K_{\bar{\epsilon}}$, and 2 is a nonsquare unit in both K_ϵ and $K_{\bar{\epsilon}}$. We now split into two cases according to whether $\bar{\epsilon}$ is in $(K_\epsilon^\times)^2$. To capture this, we fix

$$\delta = \begin{cases} 1 & \bar{\epsilon} \notin K_\epsilon^{\times 2} \\ 0 & \text{else.} \end{cases}$$

Note that if $\bar{\epsilon} \notin K_\epsilon^{\times 2}$ then we necessarily have $2 \equiv \bar{\epsilon} \pmod{K_\epsilon^{\times 2}}$. Acting by $\text{Gal}(K/\mathbb{Q})$, we see that $\bar{\epsilon}$ is in $(K_\epsilon^\times)^2$ if and only if ϵ is in $(K_\epsilon^\times)^2$.

The elements of the form (9.5) which lie in $\mathcal{S}_\epsilon(E_p/K)$ are thus those of the shape

$$((-1)^{a_1}(2^\delta\bar{\epsilon})^{a_4}(2^\delta\epsilon)^{a_3}, (-1)^{b_1}(2^\delta\bar{\epsilon})^{b_4}2^{a_3}(2^\delta\epsilon)^{b_3}).$$

Reducing further to those that lie in $\mathcal{S}_\epsilon(E_p)$ forces $a_3 = a_4$, leaving those of the shape

$$((-1)^{a_1}(\epsilon\bar{\epsilon})^{a_3}, (-1)^{b_1}(2^\delta\bar{\epsilon})^{b_4}2^{a_3}(2^\delta\epsilon)^{b_3}). \quad (9.8)$$

Finally, we apply the conditions at 2. By Lemma 9.2 we have $\epsilon \equiv \pm(\zeta - 3) \equiv \mp(4\zeta + 5) \pmod{K_2^{\times 2}}$. Moreover, as $p \equiv 5 \pmod{8}$ we have

$$\mathcal{S}_2(E_p/K) = \langle (-1, -1), (1, 2), (\zeta + 3, \zeta + 2), (1, 4\zeta + 5) \rangle.$$

Since $\epsilon\bar{\epsilon} = p \equiv 1 \pmod{K_2^{\times 2}}$, we have $\bar{\epsilon} \equiv \epsilon \equiv \mp(4\zeta + 5)$. Thus, the elements

$$(-1, -1), (\epsilon\bar{\epsilon}, 2), (1, \mp 2^\delta \epsilon), (1, \mp 2^\delta \bar{\epsilon})$$

all lie in $\text{Sel}^2(E/K)$, and are visibly linearly independent. Noting that $(1, -1)$ is not in $\mathcal{S}_2(E_p/K)$, we conclude that

$$\begin{aligned} \text{Sel}^2(E_p/K) &= \langle (-1, -1), (\epsilon\bar{\epsilon}, 2), (1, \mp 2^\delta \epsilon), (1, \mp 2^\delta \bar{\epsilon}) \rangle \\ &\cong \mathbb{F}_2^2 \oplus \mathbb{F}_2[G]. \end{aligned}$$

$p \equiv 1 \pmod{8}$: Here both -1 and 2 are squares in both K_ϵ and $K_{\bar{\epsilon}}$. As before, set

$$\delta = \begin{cases} 1 & \bar{\epsilon} \notin K_\epsilon^{\times 2} \\ 0 & \text{else.} \end{cases}$$

The elements of the form (9.5) which lie in $\mathcal{S}_\epsilon(E_p/K)$ are those of the shape

$$\left((-1)^{a_1} 2^{a_2} (\epsilon\bar{\epsilon}^\delta)^{c_1} \bar{\epsilon}^{(1-\delta)c_2}, (-1)^{b_1} 2^{b_2} (\epsilon\bar{\epsilon}^\delta)^{d_1} \bar{\epsilon}^{(1-\delta)d_2} \right), \quad (9.9)$$

for some c_1, c_2, d_1, d_2 in $\{0, 1\}$. For either value of δ these elements all lie in $\mathcal{S}_{\bar{\epsilon}}(E_p)$.

Finally, we apply the conditions at 2. By Lemma 9.2. we have

$$\epsilon \equiv \pm(-\zeta - 1) \equiv \pm\zeta^2 \equiv \pm 1 \pmod{K_2^{\times 2}},$$

and as $\epsilon\bar{\epsilon} = p$ with have $\epsilon \equiv \bar{\epsilon} \pmod{K_2^{\times 2}}$. Moreover, with $p \equiv 1 \pmod{8}$ we have

$$\mathcal{S}_2(E_p/K) = \langle (-1, -1), (1, 2), (\zeta + 3, \zeta + 6), (1, 4\zeta + 5) \rangle.$$

As the first coordinate of each of these basis elements has trivial valuation, we have $a_2 = 0$.

Suppose $\delta = 1$. Then we see that an element of the form (9.9) is in the Selmer group if and only if, in addition to $a_2 = 0$, we have $a_1 = b_1$. Thus, we find

$$\begin{aligned} \text{Sel}^2(E_p/K) &= \langle (-1, -1), (1, 2), (1, \epsilon\bar{\epsilon}), (\epsilon\bar{\epsilon}, 1) \rangle \\ &\cong \mathbb{F}_2^4. \end{aligned}$$

Now suppose that $\delta = 0$. Setting $a_2 = 0$ in (9.9) leaves a 7-dimensional space of candidate Selmer elements. Further, one readily checks that $(-1, 1)$, which has the form (9.9) for $a_1 = 1$ and all other variables 0, is not in $\mathcal{S}_2(E_p/K)$. Thus, $\text{Sel}^2(E_p/K)$ is at most 6-dimensional. However, using the fact that $\epsilon \equiv \bar{\epsilon} \equiv \pm 1 \pmod{K_2^{\times 2}}$, one readily checks that the six linearly independent elements

$$\{(-1, -1), (1, 2), (1, \pm\epsilon), (\pm\epsilon, 1), (1, \pm\bar{\epsilon}), (\pm\bar{\epsilon}, 1)\},$$

each of which are of the form (9.9), map to $\mathcal{S}_2(E_p/K)$ after localising at 2. Thus,

$$\begin{aligned} \mathrm{Sel}^2(E_p/K) &= \langle (-1, -1), (1, 2), (1, \pm\epsilon), (\pm\epsilon, 1), (1, \pm\bar{\epsilon}), (\pm\bar{\epsilon}, 1) \rangle \\ &\cong \mathbb{F}_2^2 \oplus \mathbb{F}_2[G]^2. \end{aligned}$$

This completes the proof. \square

Remark 9.10. 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, for example, Proposition 5.6.

9.2 | 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 9.3. We refer the reader to [35] for definitions concerning Rédei symbols.

Lemma 9.11. *Let $p \equiv 1 \pmod{8}$ be a prime which splits in K/\mathbb{Q} , and let $\epsilon \in \mathcal{O}_K$ have norm p . Then $\bar{\epsilon} \in (K_\epsilon^\times)^2$ 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 $-\epsilon$. By Lemma 9.2, we may thus assume that we have

$$\bar{\epsilon} \equiv -(\zeta + 1) = \zeta^2 \equiv 1 \pmod{K_2^{\times 2}}.$$

Now consider the diagram of fields

$$\begin{array}{ccc} & F = \mathbb{Q}(\sqrt{\theta}, \sqrt{\epsilon}, \sqrt{\bar{\epsilon}}) & \\ & \swarrow \quad \searrow & \\ K(\sqrt{\bar{\epsilon}}) & & L = \mathbb{Q}(\sqrt{\theta}, \sqrt{p}) \\ & \swarrow \quad \searrow & \\ K = \mathbb{Q}(\sqrt{\theta}) & & K' = \mathbb{Q}(\sqrt{\theta p}) \\ & \swarrow \quad \searrow & \\ & \mathbb{Q} & \end{array}$$

Since ϵ ramifies in L/K , we see that $\bar{\epsilon} \in (K_\epsilon^\times)^2$ 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, $\bar{\epsilon}$ 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 $F = L(\sqrt{\bar{\epsilon}})/L$ is unramified at such \mathfrak{p}' . Thus, F/K' is unramified at \mathfrak{p} . We now conclude that $\bar{\epsilon} \in (K_\epsilon^\times)^2$ if and only if the Artin symbol $(\frac{F/K'}{\mathfrak{p}})$ 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 $\bar{\epsilon}$ to be a square in K_2 , the extension $K(\sqrt{\bar{\epsilon}})/K$ is split at 2. Thus, as the compositum of $K(\sqrt{\bar{\epsilon}})$ 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 $F = K'(\sqrt{p}, \sqrt{\epsilon})/K'$ 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, while 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 [35, Definition 7.8]). Writing $\epsilon = x + y\sqrt{\theta}$ 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

$$\sqrt{\epsilon} = \sqrt{x + y\sqrt{\theta}}.$$

Further, by Claim 1 the extension F/K' is minimally ramified in the sense of [35, Definition 7.6]. Thus, we may take $a = \theta$, $b = p$ and $F_{a,b} = F$ in [35, Definition 7.8], giving $[\theta, p, p] = (\frac{F/K'}{\mathfrak{p}})$. Consequently, we see that $\bar{\epsilon} \in K_\epsilon^{\times 2}$ if and only if the Rédei symbol $[\theta, p, p]$ is trivial.

By [35, Proposition 7.10], the Rédei symbol $[p, \theta, -\theta p]$ exists and is trivial (to see that θp is a second kind decomposition, use [35, Proposition 4.2(4)] and our computations of Hilbert symbols above). Now, using the trilinearity and reciprocity of Rédei symbols [35, 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 $\text{Sel}^2(E_p/K)$. First we introduce some notation.

Notation 9.12. For p a prime, we define non-negative integers $e_1(E_p/K)$ and $e_2(E_p/K)$ such that we have a G -module isomorphism

$$\text{Sel}^2(E_p/K) \cong \mathbb{F}_2^{e_1(E_p/K)} \oplus \mathbb{F}_2[G]^{e_2(E_p/K)}.$$

Theorem 9.13. *The density of primes p for which $e_1(E_p/K) = e_1$ and $e_2(E_p/K) = e_2$ is as follows:*

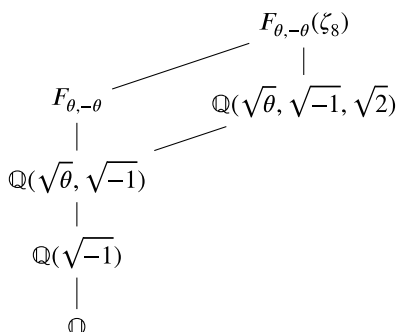
$$\lim_{X \rightarrow \infty} \frac{\#\{p \leq X \text{ prime} : e_1(E_p/K) = e_1 \text{ and } e_2(E_p/K) = e_2\}}{\#\{p \leq X \text{ prime}\}} = \begin{cases} 9/16 & \text{if } (e_1, e_2) = (4, 0), \\ 1/16 & \text{if } (e_1, e_2) = (2, 2), \\ 1/4 & \text{if } (e_1, e_2) = (2, 1), \\ 1/8 & \text{if } (e_1, e_2) = (2, 0). \end{cases}$$

Proof. As a consequence of Lemma 9.11, and the Chebotarev density theorem applied to Proposition 9.3, 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 [35, 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

$$\left(\frac{F_{\theta, -\theta}/\mathbb{Q}(\sqrt{-1})}{\mathfrak{p}} \right), \quad (9.14)$$

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 (9.14) 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 $F_{\theta, -\theta}(\zeta_8)$, among those that split completely in $\mathbb{Q}(\sqrt{\theta}, \zeta_8)$. By the Chebotarev density theorem, this is equal to $1/2$. \square

ACKNOWLEDGEMENTS

We would like to thank Alex Bartel for suggesting that we look at the behaviour of 2-Selmer groups in quadratic extensions from a statistical point of view, and for countless helpful comments. We would also like to thank Peter Koymans, Carlo Pagano and Efthymios Sofos for helpful discussions, and the anonymous referee for carefully reading the paper and providing several helpful corrections and suggestions.

Throughout this work, Adam Morgan was supported by the Max-Planck-Institut für Mathematik in Bonn, and Ross Paterson was supported by a PhD scholarship from the [Carnegie Trust for the Universities of Scotland](#).

JOURNAL INFORMATION

The *Journal of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. M. F. Atiyah and C. T. C. Wall, *Cohomology of groups, Algebraic number theory* (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, DC, 1967, pp. 94–115.
2. P. Billingsley, *Probability and measure*, 3rd ed., Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, New York, 1995 (A Wiley-Interscience Publication).
3. J. Brau, *Selmer groups of elliptic curves in degree p extensions*, arXiv:1401.3304, 2014.
4. J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **217** (1965), 180–199.
5. C. W. Curtis and I. Reiner, *Methods of representation theory*, vol. I, Wiley Classics Library, John Wiley & Sons, New York, 1990 (with applications to finite groups and orders, reprint of the 1981 original, a Wiley-Interscience Publication).
6. P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742.
7. É. Fouvry, P. Koymans, and C. Pagano, *On the 4-rank of class groups of dirichlet biquadratic fields*, J. Inst. Math. Jussieu (2020), 1–28. <https://doi.org/10.1017/S1474748020000651>.
8. É. Fouvry and J. Klüners, *On the 4-rank of class groups of quadratic number fields*, Invent. Math. **167** (2007), no. 3, 455–513.
9. É. Fouvry and J. Klüners, *On the negative Pell equation*, Ann. of Math. (2) **172** (2010), no. 3, 2035–2104.
10. A. Granville and K. Soundararajan, *Sieving and the erdős–kac theorem, Equidistribution in number theory, an introduction*, Springer, Berlin, 2007, pp. 15–27.
11. G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n* , Q. J. Math. **48** (1917), 76–92 (Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 262–275).
12. D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195.
13. D. R. Heath-Brown, *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).
14. D. R. Heath-Brown, *A mean value estimate for real character sums*, Acta Arith. **72** (1995), no. 3, 235–275.
15. E. W. Howe, *Isogeny classes of abelian varieties with no principal polarizations, Moduli of abelian varieties* (Texel Island, 1999) Progress in Mathematics, vol. 195 (Birkhäuser, Basel, 2001), pp. 203–216.
16. 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.
17. Z. Klagsbrun, *Selmer ranks of quadratic twists of elliptic curves with partial rational two-torsion*, Trans. Amer. Math. Soc. **369** (2017), no. 5, 3355–3385.
18. 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.
19. K. Kramer and J. Tunnell, *Elliptic curves and local ε -factors*, Compos. Math. **46** (1982), no. 3, 307–352.
20. K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135.
21. 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.

22. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1977), 33–186 (with an appendix by Mazur and M. Rapoport).
23. B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575.
24. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
25. B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.
26. B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612.
27. J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.
28. J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006.
29. J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 323, Springer, Berlin, 2008.
30. B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269.
31. E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114.
32. P. Shiu, *A Brun-Titchmarsh theorem for multiplicative functions*, J. Reine Angew. Math. **313** (1980), 161–170.
33. J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
34. A. Smith, *2^∞ -Selmer groups, 2^∞ -class groups, and goldfeld's conjecture*, arXiv:1702.02325, 2017.
35. P. Stevenhagen, *Redei reciprocity, governing fields and negative Pell*, Math. Proc. Cambridge Philos. Soc. (2021), 1–28. <https://doi.org/10.1017/S0305004121000335>.
36. P. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Mathematical Proceedings of the Cambridge Philosophical Society, vol. 145, Cambridge University Press, 2008, pp. 513–526.
37. L. C. Washington, *Galois cohomology, Modular forms and Fermat's last theorem* (Boston, MA, 1995), Springer, New York, 1997, pp. 101–120.
38. A. Wiles, *Modular elliptic curves and fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.
39. 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.