Rational points of small height on elliptic curves

Inauguraldissertation
zur
Erlangung der Würde eines Doktors der Philosophie
vorgelegt der
Philosophisch-Naturwissenschaftlichen Fakultät
der Universität Basel

von

Gaston Joachim Petit

2021

Genehmigt von der Philosophisch-Naturwissenschaftlichen Fakultät
auf Antrag von

Prof. Pierre Le Boudec, Prof. Philipp Habegger, Prof. Arul Shankar

Basel, 25.05.2021

Prof. Dr. Marcel Mayor
The Dean of Faculty

Abstract

In this thesis, we are interested in counting problems concerning quadratic twists of a fixed elliptic curve defined over the field of rational numbers.
Inspired by of the analogy that exists between quadratic twists and real quadratic fields, we show an estimate for the number of quadratic twists having a nontorsion rational point whose canonical height is almost minimal. This establishes an analogue of a result of Hooley about the fundamental solution of the Pell equation.
Building upon this result, we then show that the average analytic rank is greater than one in the family of quadratic twists having a nontorsion rational point of almost minimal height.

Keywords

Elliptic curves, rational points, ranks.

Contents

Introduction

This thesis investigates the existence and the properties of rational points on elliptic curves defined over the field of rational numbers. Specifically, we study families of quadratic twists of a given elliptic curve and focus our attention mainly on the twists which have a nontorsion rational point of almost minimal height.
Let E be the elliptic curve defined over $\mathbb{Q}$ by the equation

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

where A and B are integers satisfying $4A^3 + 27B^2 \neq 0$. The classical Mordell–Weil Theorem asserts that the abelian group $E(\mathbb{Q})$ of rational points of E is finitely generated, meaning that one has

$$E(\mathbb{Q}) \simeq \mathbb{Z}^{\mathrm{rank}(E(\mathbb{Q}))} \times E(\mathbb{Q})_{\mathrm{tors}},$$

where $\mathrm{rank}(E(\mathbb{Q})$ is a nonnegative integer and $E(\mathbb{Q})_{\mathrm{tors}}$ is a finite abelian group. Despite its obvious interest, the integer $\mathrm{rank}(E(\mathbb{Q}))$ remains extremely mysterious.
To each square-free integer $d \geq 1$ corresponds a quadratic twist E_d of E, defined by the equation

$$E_d : dy^2 = x^3 + Ax + B.$$

One can show that the canonical height of nontorsion rational points on E_d satisfies the sharp lower bound

$$\hat{h}_{E_d}(P) \gg d^{1/8}, \tag{1}$$

for all $P \in E_d(\mathbb{Q})$. Here the implied constant may depend on E but not on d or P. It is natural to introduce the quantity $\eta_d(A, B)$ defined through

$$\log \eta_d(A, B) = \min\{\hat{h}_{E_d}(P) : P \in E_d(\mathbb{Q}) \smallsetminus E_d(\mathbb{Q})_{\mathrm{tors}}\},$$

when $\mathrm{rank}(E_d(\mathbb{Q})) \geq 1$ and by $\eta_d(A, B) = \infty$ when $\mathrm{rank}(E_d(\mathbb{Q})) = 0$. The quantity $\log \eta_d(A, B)$ is of particular interest when the rank of E_d is one, in which case is is half the regulator of E_d.
Denote by $\mathcal{S}(X)$ the set of positive square-free integers $d \leq X$. For a parameter $\alpha > 0$, we define

$$\mathcal{D}_{A,B}(\alpha; X) = \{d \in \mathcal{S}(X) : \eta_d(A, B) \leq d^{1/8+\alpha}\}.$$

Each integer d in this set corresponds to a quadratic twist E_d of E having a nontorsion rational point whose canonical height is almost minimal in the sense that it is only slightly larger than the lower bound (1).
The investigation of the cardinality of the set $\mathcal{D}_{A,B}(\alpha; X)$ is motivated by the work of Hooley [Hoo84] on indefinite quadratic forms. In his paper, Hooley studies the number of nonsquare integers $d \geq 1$ for which the fundamental solution ϵ_d of the Pell equation

$$X^2 - dY^2 = 4$$

is almost minimal, relative to the sharp lower bound $\epsilon_d \gg d^{1/2}$. The class number $h(d)$ of inequivalent binary quadratic forms of discriminant d and the quantity $\log \epsilon_d$ appear intrinsically linked in Dirichlet's Class Number Formula, meaning that it is likely that information about the class number can be gathered from the study of the fundamental unit; an approach simultaneously but independently taken by Sarnak [Sar82], [Sar85].

One of the main results of Hooley's article is the asymptotic estimate

$$\#\left\{d \leq X : \begin{array}{l} d \text{ nonsquare} \\ \epsilon_d \leq d^{1/2+\alpha} \end{array}\right\} \sim c(\alpha) X^{1/2} \log X, \tag{2}$$

in the range $\alpha \in (0, 1/2]$, with $c(\alpha)$ an explicit constant depending on α.
There exists an analogy between rank one quadratic twists of a given elliptic curve and real quadratic fields, as described in Table 1. It may be worth noting that this analogy can be read off the similarities between the Class Number Formula and the (conjectural) Birch and Swinnerton-Dyer formula, both predicted by the conjectures of Bloch and Kato [BK90] on special values of L-functions.

rank one quadratic twist E_d of E		real quadratic field $K = \mathbb{Q}(\sqrt{d})$
group $E(\mathbb{Q}) \simeq \mathbb{Z} \times E_d(\mathbb{Q})_{\text{tors}}$	$\longleftrightarrow$	group $\mathcal{O}_K^\times \simeq \mathbb{Z} \times \{\pm 1\}$
generator P_d of the free part of $E_d(\mathbb{Q})$	$\longleftrightarrow$	fundamental unit u_d
regulator $\mathrm{Reg}(E_d) = 2 \log \eta_d(A, B)$	$\longleftrightarrow$	regulator $\mathrm{Reg}(K) = \log u_d$
Tate–Shafarevich group $Ш(E_d)$	$\longleftrightarrow$	class group $C(K)$

Table 1: Analogy between rank one quadratic twists and real quadratic fields

The first result of this thesis is an asymptotic estimate for the cardinality of the set $\mathcal{D}_{A,B}(\alpha; X)$ when the parameter α is small, analogous to Hooley's estimate (2). We show that for $\alpha \in (0, 1/120)$, there exists a positive constant $c(\alpha)$ such that one has

$$\#\mathcal{D}_{A,B}(\alpha; X) \sim c(\alpha) X^{1/2} (\log X)^{\lambda_{A,B}}, \tag{3}$$

where $\lambda_{A,B}$ denotes the number of irreducible factors of the polynomial $x^3 + Ax + B$ over $\mathbb{Q}$.
This is achieved by considering first a modified counting function which counts all points of almost minimal height on each quadratic twist. This modified counting function is of lesser significance but easier to estimate, and we show that it is of the order of magnitude of the estimate (3). Passing to the modified counting function induces an error corresponding to the quadratic twists having rank at least two, as the number of points counted for these curves might be larger. Note that the conjecture of Goldfeld predicts that quadratic twists with rank at least two have density zero, so this error should be negligible. Using a result of Salberger [Sal08] based on the determinant method, we then show that this is the case unconditionally, giving the estimate (3).
The second result of this thesis is a lower bound for the average analytic rank in the family of quadratic twists having a rational point of almost minimal height. This is motivated by a recent paper of Le Boudec [LB18] who showed that when the quadratic twists of E are ordered by the size of $\eta_d(A, B)$, the average analytic rank is greater than one. We show that for $\alpha \in (0, 1/120)$, one has

$$\liminf_{X \to \infty} \frac{1}{\#\mathcal{D}_{A,B}(\alpha; X)} \sum_{d \in \mathcal{D}_{A,B}(\alpha; X)} \mathrm{rank}_{\mathrm{an}}(E_d) > 1. \tag{4}$$

It is important to note that for every $d \in \mathcal{D}_{A,B}(\alpha; X)$, the quadratic twist E_d has algebraic (and thus also analytic) rank at least one. Therefore, guided by Goldfeld's Conjecture [Gol79], one might have expected the average analytic rank to be exactly one. The estimate (4) shows that this is not the case.
The work of this thesis has resulted in two articles [Pet20b], [Pet20a].

Organisation of the thesis

This thesis is divided into four chapters; the first two chapters introduce the necessary background material while the last two constitute the heart of this thesis and respectively contain the proofs of the estimates (3) and (4).
Chapter 1 is comprised of a brief introduction to classical results of the theory of binary quadratic forms with emphasis on the indefinite case, as well as a presentation to more recent relevant results. Of particular importance is Section 1.3 which summarises the work of Hooley serving as a base for our first result (3).

Chapter 2 introduces elliptic curves defined over the rationals, the main objects attached to them, as well as several results and conjectures related to their ranks. Section 2.6 contains the main definitions and results concerning quadratic twists and Section 2.7 introduces the analogy existing between elliptic curves and number fields, both of which are at the heart of both of the results of this thesis.
Chapter 3 contains the proof of our first result (3), which appeared in a first article [Pet20b], and Chapter 4 is concerned with the proof of our second result (4), corresponding to a second article [Pet20a].

Notation

Throughout Chapters 3 and 4, the constants implied by the notations $\ll$ and O may depend on the choice of elliptic curve E (or equivalently on the integers A and B). All other dependencies are specified.
We denote by $\mu(n)$ the usual Möbius function and by $\zeta(s)$ the Riemann zeta function. For an arithmetic function $f(n)$, we denote the corresponding L-series by

$$L(f,s) = \sum_{n \geq 1} \frac{f(n)}{n^s}.$$

Chapter 1

Quadratic forms and the Pell equation

This chapter gives an overview of some results of the theory of binary quadratic forms, the associated class numbers and the relation they bear to the Pell equation. In particular, Section 1.3 introduces the work of Hooley which serves as a foundation for the contents of Chapter 3. Reference texts for the material presented here are the book by Zagier [Zag81] for the classical theory of quadratic forms and the book by Jacobson and Williams [JW09] for matters specific to the Pell equation.

1.1 Basic definitions and results

Let d be a integer that is not a square.

Definition. The **Pell equation** is the equation

$$X^2 - dY^2 = 4. \tag{1.1.1}$$

Solutions (x, y) of the Pell equation correspond to elements of the ring $\mathbb{Z}[\sqrt{d}]$ with norm four and are therefore usually written in the form $x + y\sqrt{d}$.

Definition. The **fundamental solution** of the Pell equation is the smallest solution $x_0 + y_0\sqrt{d}$ with $x_0, y_0 > 0$.

It is well-known that when $d > 0$, the Pell equation possesses infinitely many solutions which can all be expressed in terms of the fundamental solution; in this case the set of solutions of (1.1.1) is

$$\left\{ \pm 2 \left(\frac{x_0 + y_0\sqrt{d}}{2} \right)^n : n \in \mathbb{Z} \right\}.$$

The Pell equation is closely related to the topic of binary quadratic forms, which has occupied a central place in the development of algebraic number theory over the years.

Definition. A **primitive binary quadratic form** is a homogeneous polynomial of degree two, given by

$$f(x, y) = ax^2 + bxy + cy^2,$$

where a, b and c are coprime integers. The **discriminant** of the quadratic form f is the integer

$$d = b^2 - 4ac.$$

Note that the discriminant of a binary quadratic form is congruent to zero or one modulo four and that conversely, for every d congruent to zero or one modulo four, there exists at least one quadratic form with discriminant d. This justifies the following definition.

Definition. A **discriminant** is an integer congruent to either 0 or 1 modulo 4.

The discriminant is the main invariant associated to a binary quadratic form. It is straightforward to check that a quadratic form factors into a product of linear terms if and only if its discriminant is a perfect square.

Definition. Two binary quadratic forms $f(x, y)$ and $g(x, y)$ are **equivalent** if there exist a matrix γ in $\mathrm{SL}_2(\mathbb{Z})$ such that

$$g(x, y) = (f \circ \gamma)(x, y).$$

It is easily seen that two equivalent forms share the same discriminant, meaning that the discriminant is invariant over equivalence classes.

Definition. Let d be a discriminant that is not a perfect square. The **class number** $h(d)$ is the number of equivalence classes of primitive binary quadratic forms with discriminant d.

Considerations about the class number are greatly influenced by the sign of the discriminant and our focus here will be mainly on quadratic forms with positive discriminant. These are known as indefinite forms as they represent both positive and negative integers, as opposed to forms with negative discriminant (known as positive or negative definite forms) which only represent positive or negative integers.
It is a well-known fact that the number of equivalence classes of a given discriminant is finite. Let χ_d denote the Kronecker symbol

$$\chi_d(m) = \left(\frac{d}{m}\right),$$

and let

$$\epsilon_d = \frac{1}{2}(x_0 + y_0\sqrt{d}), \tag{1.1.2}$$

where $x_0 + y_0\sqrt{d}$ is the fundamental solution of the Pell equation (1.1.1). For $d < 0$ a discriminant, let

$$w_d = \begin{cases} 2, & d < -4, \\ 4, & d = -4, \\ 6, & d = -3. \end{cases}$$

The class number was computed by Dirichlet, who proved the following result.

Theorem 1.1 (Dirichlet Class Number Formula)**.** *Let d be a discriminant that is not a square. For $d > 0$, one has*

$$L(\chi_d, 1) = \frac{h(d)\log\epsilon_d}{\sqrt{d}}, \tag{1.1.3}$$

and for $d < 0$, one has

$$L(\chi_d, 1) = \frac{2\pi h(d)}{w_d\sqrt{|d|}}. \tag{1.1.4}$$

The difference between the two formulae above gives an indication as to where the main difficulty resides when working with positive discriminants. The fact that the class number $h(d)$ and the quantity $\log\epsilon_d$ appear intrinsically linked in (1.1.3) makes it difficult to obtain information about the class number alone. In comparison, every term other than $h(d)$ in the right-hand side of (1.1.4) is easily understood.

1.2 Asymptotic estimates and size of the fundamental solution

In this section, d and k always denote integers that are not perfect squares. The asymptotic behaviour of the class number $h(d)$ as d grows to infinity was established by Siegel [Sie35].

Theorem 1.2 (Siegel)**.** *One has*

$$\lim_{d\to\infty} \frac{\log(h(d)\log\epsilon_d)}{\log\sqrt{d}} = 1, \tag{1.2.1}$$

and

$$\lim_{d\to\infty} \frac{\log h(-d)}{\log\sqrt{d}} = 1. \tag{1.2.2}$$

Just as in (1.1.3), the fundamental solution appears alongside the class number in (1.2.1). In comparison, the equality (1.2.2) immediately implies that $h(d)$ tends to infinity as $d \to -\infty$. Average formulae for the class number were already formulated by Gauss [Gau66], who stated (without proof) the following estimates

$$\sum_{k\leq X} h(4k)\log\epsilon_{4k} \sim \frac{4\pi^2}{21\zeta(3)}X^{3/2}, \tag{1.2.3}$$

and

$$\sum_{k\leq X} h(-4k) \sim \frac{4\pi}{21\zeta(3)}X^{3/2}, \tag{1.2.4}$$

as $X \to \infty$. The restriction to discriminants that are multiples of four is explained by the fact that Gauss used a different definition of quadratic form, requiring the middle coefficient to be even. The formulae (1.2.3) and (1.2.4) were subsequently proved by Siegel [Sie44], who also considered all discriminants to show the following theorem.

Theorem 1.3 (Siegel)**.** *One has*

$$\sum_{d\leq X} h(d)\log\epsilon_d \sim \frac{\pi^2}{18\zeta(3)}X^{3/2}, \tag{1.2.5}$$

and

$$\sum_{d\leq X} h(-d) \sim \frac{\pi}{18\zeta(3)}X^{3/2}, \tag{1.2.6}$$

as $X \to \infty$.

It is a difficult and unsolved problem to obtain an asymptotic formula similar to (1.2.4) and (1.2.6) for positive values of d. One possible approach to this problem is to attempt to understand the size of the fundamental solution of the Pell equation. This is however also a difficult problem as the size of ϵ_d can vary greatly. In fact, we have

$$\log\sqrt{d} < \log\epsilon_d < \frac{1}{2}\sqrt{d}(\log d + 2). \tag{1.2.7}$$

The lower bound appearing here follows easily from the Pell equation and the upper bound can be found in the book of Hua [Hua82]. Note that an upper bound of the form $\log\epsilon_d \ll \sqrt{d}\log d$ follows from the Dirichlet Class Number Formula (1.1.3) combined with the estimate $L(\chi_d, 1) \ll \log d$ (due to Siegel).

The large fluctuation between upper and lower bound cannot be avoided as the lower bound is sharp. This can be seen by considering discriminants of the form $d = m^2 - 4$ for which the size of ϵ_d is about m. The general belief is however that the upper bound is closer to the truth for most discriminants and that ϵ_d should be of size roughly $\exp(\sqrt{d})$ most of the time; a precise conjecture will be presented later.

Taking a different approach to understand the class number, Sarnak [Sar82] computed its average when ordered by the size of ϵ_d instead of d. In particular, he showed the following estimate.

Theorem 1.4 (Sarnak). *One has*

$$\sum_{\epsilon_d \leq X} h(d) \sim \frac{X^2}{2 \log X},$$

as $X \to \infty$.

The difference between the size of the sums in this theorem compared to that in (1.2.5) is explained by the fact that large class numbers are favored when ordering by the size of ϵ_d, as anticipated from (1.2.1).
In a second paper, Sarnak [Sar85] investigated the average class number of discriminants of the form $d = m^2 - 4$, for which the lower bound in (1.2.7) is sharp. In particular, he proves the following estimate, showing that these discriminants contribute greatly to the sums of his previous theorem.

Theorem 1.5 (Sarnak). *One has*

$$\sum_{m \leq X} h(m^2 - 4) \sim \frac{5\pi^2}{96} \prod_{p \neq 2} \left(1 - \frac{1}{p^2} - \frac{2}{p^3}\right) \frac{X^2}{\log X},$$

as $X \to \infty$.

1.3 The work of Hooley

The question of separating the class number and the fundamental solution of the Pell equation was concurrently but independently studied by Hooley [Hoo84], who investigated the number of discriminants for which the lower bound in (1.2.7) is almost attained. Hooley, just like Gauss, only considers quadratic forms with even middle coefficients, and thus discriminants which are multiples of four.
Let $\alpha > 0$ be a fixed parameter. At the heart of Hooley's article is the quantity

$$S_\alpha(X) = \# \left\{ k \leq X : \begin{array}{l} k \text{ nonsquare} \\ \epsilon_{4k} \leq (4k)^{1/2+\alpha} \end{array} \right\}, \tag{1.3.1}$$

for which he conjectures the following asymptotic estimate.

Conjecture 1.1 (Hooley). *Let* $\alpha > 0$. *There exists a positive constant* $c(\alpha)$ *such that one has*

$$S_\alpha(X) \sim c(\alpha) X^{1/2} (\log X)^2,$$

as $X \to \infty$.

The value of the constant $c(\alpha)$ is predicted by Hooley as part of the conjecture and its precise expression depends on the range of α. Progress towards this conjecture has been attained by Fouvry [Fou16] who shows that for $\alpha \in [1/2, 1]$, there exists a positive constant $c'(\alpha)$ such that one has

$$S_\alpha(X) \geq c'(\alpha) X^{1/2} (\log X)^2,$$

as $X \to \infty$. The constant in Fouvry's result is smaller than the one predicted by Hooley and has since been improved by both Bourgain [Bou15] and Xi [Xi18].
Hooley manages to prove the veracity of Conjecture 1.1 when the parameter α is small enough, a restriction which comes as a result of technical limitations of the estimation process.

Theorem 1.6 (Hooley). *Let* $\alpha \in (0, 1/2]$. *One has*

$$S_\alpha(X) \sim \frac{16\alpha^2}{\pi^2} X^{1/2} (\log X)^2,$$

as $X \to \infty$.

Another result of Hooley is an estimate for the average class number over the values of k for which the lower bound in (1.2.7) is almost attained.

Theorem 1.7 (Hooley). *Let $\alpha \in (0, 1/2)$. One has*

$$\sum_{\substack{k \leq X \\ \epsilon_{4k} \leq (4k)^{1/2+\alpha}}} h(4k) \sim \frac{16\{2\alpha - \log(1+2\alpha)\}}{\pi^2} X \log X,$$

as $X \to \infty$.

The ideas leading to the above theorem are then extended to formulate a conjecture about the average class number of indefinite quadratic forms.

Conjecture 1.2 (Hooley). *One has*

$$\sum_{k \leq X} h(4k) \sim \frac{25\pi^2}{3} X (\log X)^2,$$

as $X \to \infty$.

This estimate should be compared with the one in (1.2.3) where the fundamental solution appears, as well as with the one in (1.2.4) for the definite case. This gives an indication to how large the fundamental solution ϵ_d of the Pell equation should be on average compared to d and to the class number $h(d)$. It was remarked by Fouvry and Jouve [FJ13] that the results and conjectures of Hooley and Sarnak lead to the following conjecture about the size of ϵ_d.

Conjecture 1.3. *Let $\varepsilon > 0$. For almost all positive nonsquare discriminants d, one has*

$$\epsilon_d \geq \exp(d^{1/2-\varepsilon}).$$

This conjecture is far out of reach; Hooley's work leads to a lower bound of the form $\epsilon_d \geq d^{3/2-\varepsilon}$ and the current best result is due to Reuss [Reu12] and is of the form $\epsilon_d \geq d^{3-\varepsilon}$.

1.4 Results for fundamental discriminants

A related question of interest is to obtain similar results when considering fundamental discriminants only instead of all discriminants.

Definition. A **fundamental discriminant** is the discriminant of a quadratic field.

The analogue of the estimate of Siegel in (1.2.5) is due to Datskovsky [Dat93].

Theorem 1.8 (Datskovsky). *There exists a constant $c > 0$ such that one has*

$$\sum_{\substack{d \leq X \\ d \text{ fund. disc.}}} h(d) \log \epsilon_d \sim c X^{3/2},$$

as $X \to \infty$.

The result of Theorem 1.4 has been adapted by Raulf [Rau09].

Theorem 1.9 (Raulf). *One has*

$$\sum_{\substack{\epsilon_d \leq X \\ d \text{ fund. disc.}}} h(d) \sim \frac{25\zeta(3)}{32} \prod_p \left(1 - \frac{1}{p^2} - \frac{2}{p^3}\right) \frac{X^2}{\log X},$$

as $X \to \infty$.

Finally, Conjecture 1.3 can be adapted to fundamental discriminants as follows, as these form a subset of positive density of the set of all discriminants.

Conjecture 1.4. *Let $\varepsilon > 0$. For almost all positive fundamental discriminants, one has*

$$\epsilon_d \geq \exp(d^{1/2-\varepsilon}).$$

The best results towards this conjecture are of the same order of magnitude as those towards Conjecture 1.3 mentioned above. Yamamoto [Yam71] has shown that there are infinitely many fundamental discriminants d with $\epsilon_d \geq d^3$ and Fouvry and Jouve [FJ13] showed that for all $\varepsilon > 0$, a positive proportion of fundamental discriminants d satisfy $\epsilon_d \geq d^{3-\varepsilon}$.

1.5 Quadratic fields

Most of the theory about class numbers of positive fundamental discriminants can be reformulated in terms of class numbers of real quadratic fields.
Let K be a number field and let $\mathcal{O}_K$ be its ring of integers. Let r_1 and r_2 denote respectively the number of real embeddings and the number of pairs of complex embeddings of K in an algebraic closure, and let $\mu(K)$ denote the group of roots of unity of $\mathcal{O}_K$. The Dirichlet Unit Theorem states that the group of units $\mathcal{O}_K^\times$ is a finitely generated abelian group and gives its structure.

Theorem 1.10 (Dirichlet Unit Theorem)**.** *One has*

$$\mathcal{O}_K^\times \simeq \mathbb{Z}^{r_1+r_2-1} \times \mu(K).$$

Associated to K are several other objects: the discriminant Δ_K, the regulator $\mathrm{Reg}(K)$, the class group $C(K)$, the class number $h(K)$ and the Dedekind zeta function $\zeta_K(s)$. These are related via the Class Number Formula, which generalises the Dirichlet Class Number Formula from Theorem 1.1.

Theorem 1.11 (Class Number Formula)**.** *One has*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot \mathrm{Reg}(K)\cdot h(K)}{\#\mu(K)\cdot|\Delta_K|^{1/2}}.$$

Now, let d denote a positive fundamental discriminant and let $K=\mathbb{Q}(\sqrt{d})$ be the real quadratic field of discriminant d. The group of units of $\mathcal{O}_K$ has rank one and is given by

$$\mathcal{O}_K^\times = \{\pm u_d^n : n\in\mathbb{Z}\},$$

where the generator u_d can be chosen to be positive.

Definition. The positive generator u_d of $\mathcal{O}_K^\times$ is called the **fundamental unit** of K.

The fundamental unit is closely related to the fundamental solution ϵ_d defined in (1.1.2) through

$$\epsilon_d = \begin{cases} u_d, & N(u_d)=1,\\ u_d^2, & N(u_d)=-1.\end{cases}$$

Here $N(\alpha)$ denotes the norm of an element α of K. The number $h(d)$ of classes of indefinite binary quadratic forms is equal to the narrow class number of K, so

$$h(d) = \begin{cases} 2h(K), & N(u_d)=1,\\ h(K), & N(u_d)=-1.\end{cases}$$

Moreover, as the group of units has rank one, the regulator is simply the logarithm of the fundamental unit

$$\mathrm{Reg}(K) = \log u_d. \tag{1.5.1}$$

One therefore has

$$2\,\mathrm{Reg}(K)h(K) = h(d)\log\epsilon_d,$$

and since the discriminant of K is $\Delta_K = d$ and the Dedekind zeta function is given by the product $\zeta_K(s)=\zeta(s)L(\chi_d,s)$, the Dirichlet Class Number Formula (1.1.3) can indeed be obtained by specialising the Class Number Formula from Theorem 1.11 to real quadratic fields. One of course obtains the corresponding formula for negative discriminants (1.1.4) by specialising Theorem 1.11 to imaginary quadratic fields.
Statistical properties of class numbers of quadratic fields have been extensively studied by Cohen and Lenstra [CL84] who formulated various conjectures, known together as the Cohen–Lenstra Heuristics. These predict various probabilities of properties of the odd part of the class group, the properties of the even part being accessible through more elementary means.

For $k \in \mathbb{Z} \cup \{\infty\}$ and p prime, let

$$\eta_k(p) = \prod_{n=1}^{k} (1 - p^{-n}),$$

and define

$$C_\infty = \prod_{n=2}^{\infty} \zeta(n) \approx 2.25.$$

The heuristics for real quadratic fields are as follows.

Conjecture 1.5 (Cohen–Lenstra Heuristics for real quadratic fields)**.** *Let K be a real quadratic field and p an odd prime.*

1. *The probability that the odd part of the class group $C(K)$ is cyclic is*

$$\frac{3}{10\eta_\infty(2)C_\infty} \prod_p \left(\frac{p^3 - p^2 + 1}{(p-1)(p^2-1)} \right) \approx 0.9976.$$

2. *The probability that p divides $h(K)$ is*

$$1 - \frac{\eta_\infty(p)}{1 - p^{-1}}.$$

3. *Let $r \geq 0$. The probability that the p-rank of $C(K)$ equals r is*

$$\frac{\eta_\infty(p)}{p^{r(r+1)}\eta_r(p)\eta_{r+1}(p)}.$$

4. *One has*

$$\sum_{\substack{p \leq X \\ p \equiv 1 \bmod 4}} h(\mathbb{Q}(\sqrt{p})) \sim \frac{1}{8}X,$$

as $X \to \infty$.

The first of these conjectures does not appear in the original work of Cohen and Lenstra but can be found in the book by Jacobson and Williams [JW09] while the asymptotic estimate of the fourth conjecture was independently stated by Hooley [Hoo84]. The predictions of Conjecture 1.5 agree with the work of both Sarnak and Hooley described above as they all suggest that the class number should be small most of the time.
Adopting the standpoint of quadratic fields rather than that of quadratic forms will prove particularly useful when drawing comparison with the theory of elliptic curves in the following chapters, as the similarities are more apparent from this perspective.

Chapter 2

Elliptic curves defined over the rationals

This chapter contains a brief introduction to the theory of elliptic curves defined over the rationals as well as several results of interest for later chapters. Standard references include the books by Silverman [Sil09] and by Milne [Mil06].

2.1 Basic definitions

Definition. An **elliptic curve** is a smooth, projective, algebraic curve of genus one with a distinguished base point.

Let K be a field; in practice K will be either a finite extension, a completion or an algebraic closure of $\mathbb{Q}$, or a finite field.

Definition. An elliptic curve E is **defined over** K if it is the zero locus of a polynomial with coefficients in K.

An elliptic curve defined over a field K is therefore also defined over any extension of K. When needed, one usually writes E/K to specify that K is the field of definition of E.
It follows from the Riemann–Roch Theorem that elliptic curves are plane cubic curves, meaning that they arise as zero loci of cubic polynomials in the projective plane. When the field of definition is the field of rational numbers, these cubic polynomials can always be chosen to be of a specific type.

Definition. A **Weierstrass equation** is an equation of the form

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

with A and B integers.

Every Weierstrass equation gives a projective curve C defined over the rationals by the homogeneous equation

$$C : y^2z = x^3 + Axz^2 + Bz^3.$$

Whether such a curve has singularities or not can be read from the coefficients of the equation directly.

Definition. The **discriminant** of a Weierstrass equation is the integer

$$\Delta = -16(4A^3 + 27B^2).$$

The following result is easily verified.

Lemma 2.1. *A curve given by a Weierstrass equation is nonsingular if and only if the corresponding discriminant is nonzero.*

Every Weierstrass equation with nonzero discriminant therefore defines an elliptic curve over the field of rational numbers. The converse statement holds and can even be strengthened to include unicity when restricting to a specific kind of Weierstrass equation.

Definition. A **minimal Weierstrass equation** is a Weierstrass equation such that for any prime number p, one has

$$p^4 \mid A \quad \text{implies} \quad p^6 \nmid B.$$

Lemma 2.2. *An elliptic curve E defined over the rationals is isomorphic to a unique curve given by a minimal Weierstrass equation.*

The distinguished point on an elliptic curve is the only point obtained by setting $z = 0$ in the homogeneous equation.

Definition. The point $O = (0 : 1 : 0)$ is called the **point at infinity**.

2.2 The group of rational points

Let K denote a number field inside a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and let E be an elliptic curve defined over the rationals by a Weierstrass equation.

Definition. The **K-rational points** of E are the points of the projective plane $\mathbb{P}^2(K)$ lying on the curve. The set of K-rational points is denoted by $E(K)$.

When $K = \mathbb{Q}$, the field-specific prefix is often dropped and $\mathbb{Q}$-rational points are referred to simply as rational points of E.
A K-rational point of E is represented by a triple of homogeneous coordinates $(x : y : z)$ in $\mathbb{P}^2(K)$ satisfying the homogeneous Weierstrass equation. The set $E(K)$ comes equipped with a composition law motivated by a geometric construction and defined as follows

- the point at infinity O is the identity element,
- the inverse of a point $P = (x : y : 1) \neq O$ is the point $-P = (x : -y : 1)$,
- if $P_1 = (x_1 : y_1 : 1)$ and $P_2 = (x_2 : y_2 : 1)$ are two points such that $P_1 \neq \pm P_2$ and $P_1, P_2 \neq O$, their sum is the point $P_3 = (x_3 : y_3 : 1)$ whose coordinates are given by the formulae

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \qquad y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right) x_3 - \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

The formulae for the coordinates of the point $2P = P + P$ are similar to ones for the sum described above. All together, these properties define a composition law that is commutative and associative, thus giving $E(K)$ the structure of an abelian group.
A paramount property of this group concerns its structure and was first proven by Mordell [Mor22] in the case where K is the field fo rational numbers before being extended by Weil [Wei29] to the more general version presented here.

Theorem 2.3 (Mordell–Weil)**.** *The group $E(K)$ is finitely generated.*

An immediate consequence of this result is the group isomorphism

$$E(K) \simeq \mathbb{Z}^{\operatorname{rank}(E(K))} \times E(K)_{\text{tors}},$$

where $\operatorname{rank}(E(K))$ is a nonnegative integer and $E(K)_{\text{tors}}$ is the subgroup comprised of all points of finite order.

Definition. The **(algebraic) rank** of E is the rank of the group $E(\mathbb{Q})$.

The torsion subgroup is fairly well understood as there are only finitely many possibilities, as seen in the following result of Mazur [Maz77], [Maz78] and its extension by Merel [Mer96].

Theorem 2.4 (Mazur)**.** *The torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following fifteen groups*

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \text{with} & 1 \leq N \leq 10 \text{ or } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{with} & 1 \leq N \leq 4. \end{array}$$

Each of these groups occurs as the torsion group of some elliptic curve E defined over $\mathbb{Q}$.

The generalisation of this result to arbitrary number fields is as follows.

Theorem 2.5 (Merel)**.** *There exists a constant C_K depending only on the degree of K over $\mathbb{Q}$ such that*

$$\#E(K)_{\text{tors}} \leq C_K.$$

An important family of groups of torsion points is obtained by considering only points of certain orders.

Definition. For $n \geq 1$, the **n-torsion subgroup** is the subgroup of $E(K)_{\text{tors}}$ defined as

$$E(K)[n] = \{P \in E(K) : nP = O\}.$$

The simplest and perhaps most important example is the 2-torsion subgroup $E(K)[2]$. It contains the point O as well as all the points of $E(K)$ whose y-coordinate is zero, which correspond to the roots of the polynomial $x^3 + Ax + B$ in K. In particular, $E(K)[2]$ has order 1, 2 or 4 and is trivial if and only if the aforementioned polynomial is irreducible over K.
A final group to consider to end this section is the group $E(\overline{\mathbb{Q}})$ of $\overline{\mathbb{Q}}$-rational points. It is obtained by considering all number fields inside $\overline{\mathbb{Q}}$ at once and is comprised of all points of E having algebraic coordinates. Its torsion subgroup $E(\overline{\mathbb{Q}})_{\text{tors}}$ contains all algebraic points of finite order and the torsion subgroup $E(\overline{\mathbb{Q}})[n]$ is usually denoted simply by $E[n]$. Note that the Mordell–Weil Theorem does not apply here.

2.3 Height functions

Let E be an elliptic curve defined over the rationals. In order to define the necessary height functions, note that every point in $\mathbb{P}^1(\mathbb{Q})$ can be represented by a pair of homogeneous coordinates $(x : z)$ with (x, z) a primitive vector of $\mathbb{Z}^2$, meaning that $\gcd(x, z) = 1$.

Definition. The classical **logarithmic height** function on $\mathbb{P}^1(\mathbb{Q})$ is the function

$$h : \mathbb{P}^1(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$$

defined by

$$h(x : z) = \log \max\{|x|, |z|\},$$

where (x, z) is a primitive vector.

The x-coordinate function $x : E(\mathbb{Q}) \to \mathbb{Q}$ mapping a point $P = (x : y : z)$ different from O to $x(P) = x/z$ is more naturally seen as a projective map

$$x : E(\mathbb{Q}) \longrightarrow \mathbb{P}^1(\mathbb{Q}),$$

sending $P \neq O$ to $x(P) = (x : z)$ and O to $(0 : 1)$. Composing this coordinate map with the height function on $\mathbb{Q}$ presented above produces a height function on $E(\mathbb{Q})$.

Definition. The **logarithmic Weil height** is the function

$$h_x : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$$

defined by

$$h_x(P) = h(x(P)).$$

The main properties of the function h_x are the finiteness of the sets of points of bounded height, as well as a quasi-parallelogram law which reads

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1),$$

for all P and Q in $E(\mathbb{Q})$. Here, $O(1)$ denotes a constant depending on the curve E but crucially not on P or Q. The quasi-parallelogram law can be interpreted as saying that h_x is almost quadratic, up to the constant factor $O(1)$. While this is sufficient for some applications, for instance Mordell's original proof of the Mordell–Weil Theorem, it is desirable for others to dispose of the constant term and thus work with a quadratic height.

Definition. The **canonical height** of the elliptic curve E is the function

$$\hat{h}_E : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$$

defined by

$$\hat{h}_E(P) = \frac{1}{2} \lim_{n\to\infty} \frac{h_x(2^n P)}{4^n}.$$

This is a well-defined function as the limit always exists.

The canonical height enjoys several important properties eluding h_x, the first of which is the parallelogram law

$$\hat{h}_E(P+Q) + \hat{h}_E(P-Q) = 2\hat{h}_E(P) + 2\hat{h}_E(Q),$$

which holds for every P and Q in $E(\mathbb{Q})$. This means that $\hat{h}_E$ is a quadratic form on $E(\mathbb{Q})$; it satisfies

$$\hat{h}_E(mP) = m^2 \hat{h}_E(P) \tag{2.3.1}$$

for all P in $E(\mathbb{Q})$ and m in $\mathbb{Z}$. A byproduct of the averaging process is that the values taken on torsion points all become zero. In fact, one has the following equivalence

$$\hat{h}_E(P) = 0 \iff P \text{ is a torsion point.}$$

The canonical height differs only slightly from the Weil height, the two functions being related through the identity

$$\hat{h}_E = \frac{1}{2} h_x + O(1), \tag{2.3.2}$$

where here again the term $O(1)$ is a constant depending on E only. Moreover, the canonical height is the unique height function on $E(\mathbb{Q})$ satisfying (2.3.1) and (2.3.2), making it a very natural object to consider.
A final but relevant property of the canonical height is its invariance under $\overline{\mathbb{Q}}$-isomorphism. If E' is another elliptic curve defined over $\mathbb{Q}$ for which there exists an isomorphism $\phi : E \to E'$ defined over some number field, and if $\hat{h}_{E'}$ denotes the canonical height on E', then one has

$$\hat{h}_E(P) = \hat{h}_{E'}(\phi(P)),$$

for all $P \in E(\mathbb{Q})$. When considering families of curves all isomorphic to a base curve E, expressing all canonical heights solely in terms of $\hat{h}_E$ and the individual isomorphisms is crucial. This is particularly relevant for families of twists of a fixed curve, as will be seen later.

2.4 Further objects associated to an elliptic curve

Let E be an elliptic curve defined over the rationals given by a minimal Weierstrass equation

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

with discriminant Δ_E. This section contains descriptions of the main objects associated to E.

2.4.1 The j-invariant and the automorphism group

Besides the discriminant, there is another very useful quantity defined immediately from the coefficients of the Weierstrass equation.

Definition. The **j-invariant** of the curve E is defined as

$$j_E = -1728\frac{(4A)^3}{\Delta_E}.$$

As suggested by the name, the j-invariant is constant on isomorphism classes. In fact, two elliptic curves defined over $\mathbb{Q}$ are isomorphic over $\overline{\mathbb{Q}}$ if and only if they share the same j-invariant.

Definition. An **endomorphism** of E is a morphism

$$\phi : E \longrightarrow E \quad \text{satisfying} \quad \phi(O) = O.$$

Pointwise addition and composition turn the set of endomorphisms into a ring whose units are of particular interest.

Definition. The **automorphism group** of E, denoted by $\mathrm{Aut}(E)$, is the group of invertible endomorphisms of E.

While it is a nontrivial matter to determine the structure of the endomorphism ring, the automorphism group is much simpler and completely determined by the j-invariant. Write

$$n = \begin{cases} 2, & j_E \neq 0, 1728, \\ 4, & j_E = 1728, \\ 6, & j_E = 0, \end{cases}$$

and let $\boldsymbol{\mu}_n$ denote the group of n-th roots of unity. There is a canonical isomorphism

$$\mathrm{Aut}(E) \simeq \boldsymbol{\mu}_n,$$

with the automorphism corresponding to $\zeta \in \boldsymbol{\mu}_n$ given explicitly by

$$(x, y) \longmapsto (\zeta^2 x, \zeta^3 y).$$

Remark that the conditions $j_E = 0$ and $j_E = 1728$ correspond respectively to $B = 0$ and $A = 0$ in the Weierstrass equation for E.
The j-invariant occupies a central place in the study of elliptic curves and beyond. It plays a crucial rôle in the study of the endomorphism ring and especially in the theory of complex multiplication, where it has applications to Class Field Theory as a mean to construct certain field extensions. It is also a key component in the process of linking elliptic curves to modular forms, which has many surprising and beautiful applications. These two aspects will however not be discussed here as they have no direct impact on the work presented in the following chapters.

2.4.2 Reduction modulo primes and the conductor

Let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to the p-adic valuation v_p. Viewing the coefficients A and B in the definition of E as elements of the completion defines an elliptic curve over $\mathbb{Q}_p$, also denoted by E. Just as for the group of rational points, the group of $\mathbb{Q}_p$-rational points $E(\mathbb{Q}_p)$ is defined as the set of points of $\mathbb{P}^2(\mathbb{Q}_p)$ lying on the curve and equipped with the group law. These extended definitions allow for a reduction process from which local information about E can be gathered.

Definition. The **reduction of E modulo p** is the curve $\bar{E}$ defined over the residue field $\mathbb{F}_p$ by the equation

$$\bar{E} : y^2 = x^2 + \bar{A}x + \bar{B},$$

where $\bar{A}$ and $\bar{B}$ denote the reduction of A and B modulo p.

Although the curve E is nonsingular, the same need not hold for its reduction. The reduced curve $\bar{E}$ falls into one of three categories.

Definition. One says that

- E has **good reduction** at p if $\bar{E}$ is nonsingular,
- E has **multiplicative reduction** at p if $\bar{E}$ has a node,
- E has **additive reduction** at p if $\bar{E}$ has a cusp.

Moreover, E is said to have **bad reduction** at p if the reduction is either multiplicative or additive. If E has multiplicative reduction at p, the reduction is said to be **split** or **nonsplit** depending on whether the slopes of the tangent lines at the node belong to $\mathbb{F}_p$ or not.

The names of multiplicative and additive reduction come from the fact that the group of nonsingular $\overline{\mathbb{F}}_p$-rational points of $\bar{E}$ is isomorphic to either the multiplicative or additive group of $\overline{\mathbb{F}}_p$. The reduction type at p can easily be read from the coefficients A and B as follows

- E has good reduction at p if and only if $v_p(\Delta_E) = 0$,
- E has multiplicative reduction at p if and only if $v_p(\Delta_E) > 0$ and $v_p(A) = 0$,
- E has additive reduction at p if and only if $v_p(\Delta_E) > 0$ and $v_p(A) > 0$.

For $p \neq 2, 3$, let

$$f_p(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

The definitions for $f_2(E)$ and $f_3(E)$ are omitted here as they are more complicated to state, but one always has $f_3(E) \leq 3$ and $f_2(E) \leq 5$.

Definition. The **conductor** of E is the quantity

$$N_E = \prod_p p^{f_p(E)}.$$

The conductor is a crucial invariant of the curve. Just like the discriminant, it encodes information about the primes of bad reduction, the only difference being the exponent with which these primes appear. A deep conjecture made by Szpiro states that although the p-adic valuation of the discriminant can sometimes be large, this is a rare occurrence.

Conjecture 2.1 (Szpiro)**.** *For every $\epsilon > 0$ there exists a constant $c(\epsilon)$ such that one has*

$$|\Delta_E| \leq c(\epsilon) N_E^{6+\epsilon}$$

holds for all elliptic curves defined over $\mathbb{Q}$.

Another quantity of interest arises from the reduction of p-adic points on E. If P is a point of $E(\mathbb{Q}_p)$ represented by the homogeneous coordinates $P = (x : y : z)$ where x, y and z are coprime integers, the reduction map

$$E(\mathbb{Q}_p) \longrightarrow \bar{E}(\mathbb{F}_p)$$

sends P to $\bar{P} = (\bar{x} : \bar{y} : \bar{z})$, where $\bar{x}$, $\bar{y}$ and $\bar{z}$ denote the respective reductions modulo p of x, y and z. The set of points with nonsingular reduction is denoted by

$$E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \bar{P} \text{ is nonsingular}\},$$

and forms a group whose index in $E(\mathbb{Q}_p)$ is finite.

Definition. The **Tamagawa number** of E at p is the index

$$c_p(E) = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)].$$

Remark that $c_p(E) = 1$ whenever E has good reduction at p since in that case, the reduced curve $\bar{E}$ has no singularities.

2.4.3 The L-function and the analytic rank

Let p be a prime at which E has good reduction. Let $\bar{E}$ denote the reduction of E modulo p and let

$$a_p(E) = p + 1 - \#\bar{E}(\mathbb{F}_p).$$

This integer measures the difference between the number of $\mathbb{F}_p$-points of $\bar{E}$ and the number of points on the projective line $\mathbb{P}^1(\mathbb{F}_p)$, which is simply $p+1$. The Hasse–Weil bound, originally proven by Hasse [Has36a], [Has36b], [Has36c] for elliptic curves and subsequently generalised by Weil [Wei49] to curves of higher genus, asserts that these quantities cannot differ much.

Theorem 2.6 (Hasse–Weil Bound)**.** *One has*

$$a_p(E) \leq 2\sqrt{p}.$$

Define the polynomial

$$L_p(E,T) = 1 - a_p(E)T + pT^2,$$

and extend the definition to primes of bad reduction by setting

$$L_p(E,T) = \begin{cases} 1-T, & \text{if } E \text{ has split multiplicative reduction at } p, \\ 1+T, & \text{if } E \text{ has nonsplit multiplicative reduction at } p, \\ 1, & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

Definition. The **L-function** of E is the function defined by the Euler product

$$L(E,s) = \prod_p L_p(E, p^{-s})^{-1}.$$

This product converges absolutely and defines an analytic function for $\Re(s) > 3/2$ as an immediate consequence of the Hasse–Weil Bound in Theorem 2.6. Much more is true in fact, as this function can be extended meromorphically to the whole complex plane. Let N_E denote the conductor of E and let $\Gamma(s)$ denote the usual Euler Γ function.

Theorem 2.7 (Functional equation)**.** *The modified L-function*

$$\Lambda(E,s) = (2\pi)^{-s} N_E^{s/2} \Gamma(s) L(E,s)$$

has an analytic continuation to the whole complex plane and satisfies

$$\Lambda(E,s) = \omega(E)\Lambda(E, 2-s)$$

for some $\omega(E) = \pm 1$.

The functional equation is known to hold for modular forms and its validity for elliptic curves thus follows from the Modularity Theorem of Wiles [Wil95] and Breuil, Conrad, Diamond and Taylor [BCDT01].

Definition. The integer $\omega(E)$ is called the **root number** of E.

The extension of $L(E,s)$ to the whole complex plane implies in particular that the value of $L(E,s)$ at $s=1$ is well-defined as the function has no pole there.

Definition. The **analytic rank** of E, denoted by $\mathrm{rank}_{\mathrm{an}}(E)$, is the order of vanishing of the function $L(E,s)$ at the point $s=1$.

The parity of the analytic rank is determined by the root number through the equality

$$(-1)^{\mathrm{rank}_{\mathrm{an}}(E)} = \omega(E).$$

2.4.4 The elliptic regulator

The Mordell–Weil Theorem implies that $E(\mathbb{Q}) \otimes \mathbb{R}$ is a finite-dimensional real vector space, in which the quotient $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ sits as a lattice. The canonical height $\hat{h}_E$ extends to a positive definite quadratic form on $E(\mathbb{Q}) \otimes \mathbb{R}$ and the volume of this lattice computed with respect to the metric it induces is an important invariant of the curve E.

Definition. The **elliptic regulator** of E, denoted by $\text{Reg}(E)$, is the volume of a fundamental domain for $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ computed with respect to the quadratic form $\hat{h}_E$. By convention, $\text{Reg}(E) = 1$ when the rank of E is zero.

This volume can be computed explicitly from generators of the group $E(\mathbb{Q})$ through the use of a bilinear form associated to the quadratic form $\hat{h}_E$.

Definition. The **canonical height pairing** on E is the bilinear form

$$\langle \cdot, \cdot \rangle : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

defined by

$$\langle P, Q \rangle = \hat{h}_E(P + Q) - \hat{h}_E(P) - \hat{h}_E(Q).$$

If the rank of E is nonzero and $P_1, \ldots, P_r \in E(\mathbb{Q})$ are generators of the quotient $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$, the elliptic regulator is given explicitly by

$$\text{Reg}(E) = \det(\langle P_i, P_j \rangle).$$

As in the number field case, the regulator is a form of measure of the complexity of the group $E(\mathbb{Q})$. The elliptic regulator of an elliptic curve is conjecturally bounded above and below in terms of other invariants of the curve. The following conjecture originates in the work of Lang [Lan78] and formulates a precise lower bound for the canonical height of nontorsion raional points.

Conjecture 2.2 (Lang)**.** *There exists a constant $C > 0$ such that for any elliptic curve E defined over $\mathbb{Q}$ and every nontorsion point $P \in E(\mathbb{Q})$, one has*

$$\hat{h}_E(P) > C \max\{h(j_E : 1), \log |\Delta_E|, 1\}.$$

A second conjecture also due to Lang [Lan83] predicts an upper bound for the height of generators of the group of rational points.

Conjecture 2.3 (Lang)**.** *Let $\epsilon > 0$. There exists a constant C_ϵ depending only on ϵ such that for any elliptic curve E defined over $\mathbb{Q}$ with rank r, there exists a basis $P_1, \ldots, P_r$ for the free part of $E(\mathbb{Q})$ satisfying*

$$\max_{1 \le i \le r} \hat{h}_E(P_i) \le C_\epsilon^{r^2} |\Delta_E|^{1/12+\epsilon}.$$

2.4.5 The Selmer and Tate–Shafarevich groups

Let $n \ge 1$. A crucial step in the proof of the Mordell–Weil Theorem is showing the finiteness of the quotient $E(\mathbb{Q})/nE(\mathbb{Q})$. This is done by embedding this quotient into a larger group whose generators can be computed. Note that lifting generators of $E(\mathbb{Q})/nE(\mathbb{Q})$ to generators of $E(\mathbb{Q})$ can be done in a finite amount of computation so the difficulty in rank computations lies in finding generators for the quotient.
The multiplication-by-n map is surjective and therefore induces a short exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{n} E \longrightarrow 0.$$

Taking Galois cohomology, one obtains a Kummer exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E)[n] \longrightarrow 0.$$

The group $H^1(\mathbb{Q}, E[n])$ is usually infinite. One can however embed $E(\mathbb{Q})/nE(\mathbb{Q})$ in a subgroup defined by considering E as an elliptic curve over $\mathbb{Q}_p$ for every prime $p \le \infty$ simultaneously. There

is a short exact sequence for every prime and together, they form a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, E[n]) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_p E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E[n]) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E)[n] & \longrightarrow & 0. \end{array}$$

If an element of $H^1(\mathbb{Q}, E[n])$ comes from a point in $E(\mathbb{Q})$, then for every prime p the corresponding element in $H^1(\mathbb{Q}_p, E[n])$ is the image of a point in $E(\mathbb{Q}_p)$. This motivates the following definition.

Definition. The **n-Selmer group** of E is

$$\mathrm{Sel}_n(E) = \ker\left(H^1(\mathbb{Q}, E[n]) \to \prod_p H^1(\mathbb{Q}_p, E)\right).$$

This is a finite group, as can be shown by adapting the argument used to prove finiteness of the ideal class group, and it is computable. It is clear from the diagram that $E(\mathbb{Q})/nE(\mathbb{Q})$ injects into $\mathrm{Sel}_n(E)$ and the difference is measured by a third group.

Definition. The **Tate–Shafarevich group** of E is

$$Ш(E) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_p H^1(\mathbb{Q}_p, E)\right).$$

By definition, this group fits into the short exact sequence

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow \mathrm{Sel}_n(E) \longrightarrow Ш(E)[n] \longrightarrow 0. \tag{2.4.1}$$

If one is able to find an integer $n \geq 1$ for which $Ш(E)[n]$ is trivial, then it suffices to compute the Selmer group $\mathrm{Sel}_n(E)$ to obtain generators of $E(\mathbb{Q})$. However, the Tate–Shafarevich group is not well-understood and its finiteness is one of the main open problems in the theory of elliptic curves.

Conjecture 2.4 (Tate–Shafarevich)**.** *The Tate–Shafarevich group of E is finite.*

Note that the finiteness of the Tate–Shafarevich group implies that is is always possible to find n for which $Ш(E)[n]$ is trivial, leading to an algorithm for the computation of $E(\mathbb{Q})$.
There is a geometric interpretation of the Selmer and Tate–Shafarevich groups which consists in identifying the elements of $H^1(\mathbb{Q}, E)$ and $H^1(\mathbb{Q}_p, E)$ with equivalence classes of certain projective curves called homogeneous spaces. Under this identification, an element of the first cohomology group $H^1(\mathbb{Q}, E)$ (respectively $H^1(\mathbb{Q}_p, E)$) is trivial if and only if the corresponding curve possesses a $\mathbb{Q}$-rational (respectively $\mathbb{Q}_p$-rational) point. Elements of the Selmer group then correspond to curves with a local (i.e. $\mathbb{Q}_p$-rational) point everywhere, and the Tate–Shafarevich group is the subgroup of elements with no global (i.e. $\mathbb{Q}$-rational) point. This explains why the Selmer group is easily computable and the Tate–Shafarevich group is not, as the search for local points can be reduced to computations over finite fields while determining the existence of global solutions to an equation is much more difficult. It also allows to interpret the Tate–Shafarevich group as a measure of the failure of the Hasse principle.
In practice, upper bounds on the rank usually come in the form of bounds for the size of the p-Selmer group for some prime p.

Definition. The **p-Selmer rank** of E is the integer $s_p(E) = \dim_{\mathbb{F}_p}(\mathrm{Sel}_p(E))$.

The short exact sequence (2.4.1) implies the equality

$$s_p(E) = \mathrm{rank}(E(\mathbb{Q})) + \dim_{\mathbb{F}_p}(E(\mathbb{Q})[p]) + \dim_{\mathbb{F}_p}(Ш(E)[p]),$$

so assuming the Tate–Shafarevich Conjecture, the p-Selmer rank of E equals the rank of E for all but finitely many primes p.

It is also useful to consider all powers of a given prime p at once. One then obtains the p^∞-Selmer group $\mathrm{Sel}_{p^\infty}(E)$, defined by the obvious adaptation of the definition above, which fits into the short exact sequence

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

Definition. The **p^∞-Selmer rank** of E, denoted by $s_{p^\infty}(E)$, is the rank of E plus the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in $Ш(E)[p^\infty]$.

Note that Conjecture 2.4 implies $s_{p^\infty}(E) = \mathrm{rank}(E(\mathbb{Q}))$ for every prime p.

2.5 Main results and conjectures

The rank of elliptic curves is the subject of many speculations. This section contains an overview of the main conjectures about the rank and of the interplay that exists between them, as well as a presentation of selected results pertaining to said conjectures. All elliptic curves are assumed to be defined over the rationals.
One of the first and most natural question one might ask is to determine whether the rank of elliptic curves is bounded. The general consensus has long been that this should be false and that there should exist elliptic curves with arbitrarily large rank; a belief instigated by the function field analogue where ranks are known to be unbounded from the work of Tate and Shafarevich [TŠ67]. However, a recent heuristic approach of Park, Poonen, Voight and Wood [PPVW19] goes against this belief and suggests that all but finitely many elliptic curves have rank at most 21. The largest recorded rank is due to Elkies who exhibited a curve with 28 linearly independent rational points. The Generalised Riemann Hypothesis for L-functions of elliptic curves and for Dedekind zeta functions would imply that the rank of this curve is exactly 28 [KSW19].

2.5.1 The Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve defined over the rationals. Perhaps the most important conjecture concerning the rank is due to Birch and Swinnerton-Dyer [BSD65] and relates the (algebraic) rank to the analytic rank.

Conjecture 2.5 (Birch–Swinnerton-Dyer)**.** *One has*

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_{\mathrm{an}}(E).$$

This conjecture is known to hold for elliptic curves with analytic rank equal to zero or one. It was shown by Gross and Zagier [GZ86] that the (algebraic) rank is at least the analytic rank whenever the analytic rank is at most one. Further work of Kolyvagin [Kol88], [Kol90] on this topic results in the following theorem.

Theorem 2.8 (Gross–Zagier, Kolyvagin)**.** *Let E be an elliptic curve with analytic rank at most one. One has*

$$\mathrm{rank}(E(\mathbb{Q})) = \mathrm{rank}_{\mathrm{an}}(E),$$

and the Tate–Shafarevich group of E is finite.

A recent result of Skinner [Ski20] shows that under certain technical assumptions, the converse also holds.

Theorem 2.9 (Skinner)**.** *Assume that E has multiplicative reduction at every prime. Assume further that there is one odd prime at which E has nonsplit multiplicative reduction or two odd primes at which E has split multiplicative reduction. If the rank of E is one and the Tate–Shafarevich group of E is finite, then the analytic rank of E is one.*

There exists a weaker version of Conjecture 2.5 only concerned with the parity of the ranks.

Conjecture 2.6 (Parity Conjecture)**.** *One has*

$$\mathrm{rank}(E(\mathbb{Q})) \equiv \mathrm{rank}_{\mathrm{an}}(E) \bmod 2.$$

Conjecture 2.6 is obviously implied by Conjecture 2.5 and therefore known to hold for curves with analytic rank at most one. The best result in direction of the general case is the proof of the p-parity Conjecture by Dokchitser and Dokchitser [DD10].

Theorem 2.10 (Dokchitser–Dokchitser)**.** *Let p be a prime. One has*

$$s_{p^\infty}(E) \equiv \mathrm{rank}_{\mathrm{an}}(E) \bmod 2.$$

A refined version of the Birch and Swinnerton-Dyer Conjecture predicts the precise value of the leading coefficient of the Taylor series of $L(E,s)$ at $s=1$ in terms of various quantities associated to the curve E. Let

$$\Omega_E = \int_{E(\mathbb{R})} \left| \frac{\mathrm{d}x}{y} \right|,$$

denote the real period of E.

Conjecture 2.7 (Birch–Swinnerton-Dyer)**.** *One has*

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{\mathrm{rank}(E(\mathbb{Q}))}} = \frac{2^{\mathrm{rank}(E(\mathbb{Q}))} \cdot \Omega_E \cdot \mathrm{Reg}(E) \cdot \#Ш(E) \cdot \prod_p c_p(E)}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}.$$

Despite overwhelming numerical evidence, this conjecture is only known to hold in a few special cases.

2.5.2 Counting elliptic curves

In recent years, a statistical approach has been employed to tackle problems regarding ranks, with the goal of proving results not for individual curves but rather on average in families. The main and most interesting of these families being the one comprised of all elliptic curves defined over the rationals. As this family is of course infinite, is it a necessity to first and foremost order and count the curves in some manner.
One of the most natural orderings of elliptic curves is by the size of their discriminant, that is by considering the set

$$\mathcal{E}_\Delta(X) = \{E/\mathbb{Q} : |\Delta_E| \leq X\}.$$

Unfortunately, this ordering suffers from a significant issue as no precise asymptotic estimate for the cardinality of the set $\mathcal{E}_\Delta(X)$ is known; a heuristic prediction for this number can be found in the work of Brumer and McGuinness [BM90].

Conjecture 2.8 (Brumer–McGuinness)**.** *There exists a constant $c>0$ such that one has*

$$\#\mathcal{E}_\Delta(X) \sim cX^{5/6},$$

as $X \to \infty$.

A second and also very natural way to order elliptic curves is by the size of their conductor, and the corresponding set is

$$\mathcal{E}_N(X) = \{E \text{ defined over } \mathbb{Q} : N_E \leq X\}.$$

Just as when ordering by size of the discriminant, no precise asymptotic estimate exists for the number of elements in this set; a heuristic asymptotic estimate was given by Watkins [Wat08].

Conjecture 2.9 (Watkins)**.** *There exists a constant $c>0$ such that one has*

$$\#\mathcal{E}_N(X) \sim cX^{5/6},$$

as $X \to \infty$.

A recent paper of Shankar, Shankar and Wang [SSW19] establishes such estimates for certain subfamilies of the family of all elliptic curves.

Theorem 2.11 (Shankar–Shankar–Wang). *Let $\kappa \in (0, 7/4)$. There exist two constants $c_1, c_2 > 0$ such that one has*

$$\#\{E \in \mathcal{E}_N(X) : |\Delta_E| < N_E^{\kappa}\} \sim c_2 X^{5/6},$$

as well as

$$\#\{E \in \mathcal{E}_N(X) : \Delta_E/N_E \text{ is square-free}\} \sim c_1 X^{5/6},$$

as $X \to \infty$.

It is worth mentioning that the authors expect the second estimate of Theorem 2.11 to hold for every positive value of κ.
A third and more convenient ordering of elliptic curves is by the size of the coefficients of their minimal Weierstrass equation.

Definition. The **height** of an elliptic curve E defined by a minimal Weierstrass equation is the integer

$$H(E) = \max\{4|A|^3, 27B^2\}.$$

One can then consider the set of curves ordered by height

$$\mathcal{E}_H(X) = \{E/\mathbb{Q} : H(E) \leq X\}.$$

The main benefit of this ordering is that counting curves of bounded height is straightforward via a sieving argument.

Proposition 2.12. *There exists a constant $c > 0$ such that one has*

$$\#\mathcal{E}_H(X) \sim cX^{5/6},$$

as $X \to \infty$.

For this reason, this ordering is often used in practice when studying distribution of quantities associated to elliptic curves.

2.5.3 Distribution of ranks

The main object of interest of most statistical investigations is the rank. A conjecture originating in the work of Goldfeld [Gol79] and extended using the heuristics of Katz and Sarnak [KS99] predicts its distribution.

Conjecture 2.10 (Rank Distribution). *When all elliptic curves defined over the rationals are ordered by size of their discriminant, by size of their conductor, or by height, the proportion of curves with rank zero and the proportion of curves with rank one are both one half.*

This conjecture implies in particular that the density of curves with rank at least two is zero and that the average rank of all elliptic curves defined over the rationals is one half.
Progress towards Conjecture 2.10 when the curves are ordered by height has been achieved in a series of outstanding papers by Bhargava and Shankar [BS15a], [BS15b], [BS13a], [BS13b] where the authors compute the average size of the n-Selmer group for small values of n and deduce several results about the distribution of ranks.
For $n \geq 1$, let $\sigma(n)$ denote the sum of divisors of n, that is

$$\sigma(n) = \sum_{d|n} d.$$

Theorem 2.13 (Bhargava–Shankar). *Let $n \in \{1, 2, 3, 4, 5\}$. When all elliptic curves defined over the rationals are ordered by height, the average size of the n-Selmer group is $\sigma(n)$.*

Since a bound on the size of the Selmer group implies a bound on the rank, a consequence of Theorem 2.13 is the boundedness of the average rank of elliptic curves.

Theorem 2.14 (Bhargava–Shankar). *When all elliptic curves defined over the rationals are ordered by height, the average rank is less than* 0.885.

Another consequence follows from combining Theorem 2.13 with Theorem 2.10.

Theorem 2.15 (Bhargava–Shankar)**.** *When all elliptic curves defined over the rationals are ordered by height, the proportion of curves with rank zero is greater than one fifth. Assuming Conjecture 2.4, the proportion of curves with rank one is greater than one fourth.*

A third consequence of Theorem 2.13 concerning the analytic rank comes from also considering the work of Skinner and Urban [SU14].

Theorem 2.16 (Bhargava–Shankar)**.** *When all elliptic curves defined over the rationals are ordered by height, a positive proportion of curves have analytic rank zero.*

Together with Theorem 2.8, Theorem 2.16 implies that a positive proportion of all elliptic curves satisfy Conjecture 2.5.
Although they only compute the average size of the n-Selmer group for a few values of n, Bhargava and Shankar conjecture that their result can be extended to any positive integer n.

Conjecture 2.11 (Bhargava–Shankar)**.** *When all elliptic curves defined over the rationals are ordered by height, the average size of the n-Selmer group is $\sigma(n)$.*

This conjecture is closely related to Conjecture 2.10, as shown by the next proposition.

Proposition 2.17. *Assume that Conjecture 2.11 holds for infinitely many values of n. When all elliptic curves defined over the rationals are ordered by height, the proportion of curves with rank at most one is one.*

This proposition can be further refined to give a sufficient condition for Conjecture 2.10 to hold in full, expressed in terms of other conjectures. One of these not yet mentioned concerns the signs of the functional equations.

Conjecture 2.12 (Root Number Equidistribution)**.** *When all elliptic curves defined over the rationals are ordered by size of their discriminant, by size of their conductor, or by height, the proportion of curves with root number zero and the proportion of curves with root number one are both one half.*

All the necessary conjectures to state the following proposition have now been introduced.

Proposition 2.18. *Assume that Conjecture 2.11 holds for infinitely many positive values of n and that Conjecture 2.6 and Conjecture 2.12 both hold. When all elliptic curves defined over the rationals are ordered by height, the proportion of curves with rank zero and the proportion of curves with rank one are both one half.*

2.6 Quadratic twists

It is often useful to work not on the full family of all elliptic curves defined over the rationals but rather on subfamilies of curves of a specific form. This allows to develop intuition and to formulate conjectures which can then be extended to larger families, and this process has been used extensively to gain insight about ranks of elliptic curves. One such family of great importance is the family of quadratic twists of a given elliptic curve.
Fix an elliptic curve E defined over the rationals by a Weierstrass equation

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

Definition. A **twist** of E is an elliptic curve defined over the rationals which is isomorphic to E over a finite extension of $\mathbb{Q}$. A **quadratic twist** of E is a twist of E which is isomorphic to E over a quadratic extension of $\mathbb{Q}$.

Quadratic twists of E are parametrised by square-free integers. Let d be a square-free integer; the corresponding quadratic twist of E is the elliptic curve E_d defined by the equation

$$dy^2 = x^3 + Ax + B,$$

which is isomorphic to E over the quadratic field $\mathbb{Q}(\sqrt{d})$.
Consider the family of quadratic twists E_d of E, where d runs over all square-free integers. Just as for the family of all elliptic curves, conjectures about ranks in this family are plentiful. One of the oldest and simplest of these conjectures is due to Honda [Hon60] and states that the ranks in families of quadratic twists are bounded.

Conjecture 2.13 (Honda)**.** *There exists a constant C_E depending only on E such that for all square-free integers d, one has*

$$\operatorname{rank}(E_d(\mathbb{Q})) \leq C_E.$$

Contrary to the situation of the family of all elliptic curves, there is a unique and very natural ordering for quadratic twists of a fixed curve E which simply consists in ordering twists by the size of the square-free integer d. All three orderings considered when working with the family of all elliptic curves are equivalent to this one.
Denote the set of positive square-free integers up to X by

$$\mathcal{S}(X) = \{1 \leq d \leq X : \mu(d) \neq 0\}.$$

The number of quadratic twists of the curve E ordered by size of d is easily computed as one has

$$\#\mathcal{S}(X) \sim \frac{6}{\pi^2} X,$$

as $X \to \infty$.
The distribution of the rank in a family of quadratic twists is predicted by a conjecture of Goldfeld [Gol79].

Conjecture 2.14 (Goldfeld)**.** *The proportion of quadratic twists of E with analytic rank zero and the proportion of quadratic twists of E with rank one are both one half.*

This conjecture is noticeably similar to Conjecture 2.10, the reason being that Goldfeld's Conjecture predates it and was actually the first indication that such a result should hold. It implies that in a family of quadratic twists, the curves with rank at least two have density zero and that the average rank is one half.
Although the general case is likely far from being solved, Conjecture 2.14 is known to hold for a specific choice of base curve E, the so-called congruent numbers curve, through the combined recent results of Smith [Smi17] and Kriz [Kri20].

Theorem 2.19 (Kriz)**.** *Conjecture 2.14 holds for the elliptic curve E defined by the equation*

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

2.7 Analogy with number fields

An interesting aspect of the theory of elliptic curves is the striking analogy that exists with the theory of number fields. This parallel stems from the fact that both the group of rational points of an elliptic curve and the group of units of the ring of integers of a number field are finitely generated, as a result of the Mordell–Weil Theorem (Theorem 2.3) and of the Dirichlet Unit Theorem (Theorem 1.10) respectively. The theory developed for number fields has been at the source of the formulation and proof of several key results presented above in this chapter.

2.7.1 The general case

Let E be an elliptic curve defined over the rationals and let K be a number field with ring of integers $\mathcal{O}_K$. The various objects associated to the curve E can be related to the objects associated to the field K, as illustrated in Table 2.1.
The Tate–Shafarevich group and the class group both measure the failure of a certain property, the failure of the Hasse principle in the case of the Tate–Shafarevich group and the failure of unique factorisation in the ring of integers $\mathcal{O}_K$ in the case of the class group.

elliptic curve E defined over $\mathbb{Q}$		number field K
group $E(\mathbb{Q})$	$\longleftrightarrow$	group of units $\mathcal{O}_K^\times$
Mordell–Weil Theorem	$\longleftrightarrow$	Dirichlet Unit Theorem
torsion subgroup $E(\mathbb{Q})_{\text{tors}}$	$\longleftrightarrow$	roots of unity $\mu(K)$
conductor N_E	$\longleftrightarrow$	absolute value of discriminant $\lvert\Delta_K\rvert$
regulator $\text{Reg}(E)$	$\longleftrightarrow$	regulator $\text{Reg}(K)$
L-function $L(E,s)$	$\longleftrightarrow$	Dedekind zeta function $\zeta_K(s)$
Tate–Shafarevich group $Ш(E)$	$\longleftrightarrow$	class group $C(K)$

Table 2.1: Analogy between elliptic curves and number fields

While the finiteness of the class number is well-known, that of the Tate–Shafarevich group is merely conjectural and predicted by Conjecture 2.4. Its order appears to be intimately linked with the regulator $\text{Reg}(E)$ in the formula predicted by Birch and Swinnerton-Dyer in Conjecture 2.7. This is the analogue of the Class Number Formula in Theorem 1.11 where the class number $h(K)$ appears alongside the regulator $\text{Reg}(K)$.
It is worth noting that both the Class Number Formula and the formula predicted by the Birch and Swinnerton-Dyer Conjecture can be regarded as cases of the more general conjectures of Bloch and Kato [BK90] about special values of L-functions.

2.7.2 Quadratic twists and real quadratic fields

The comparison can be pushed further by considering only rank one quadratic twists of a given elliptic curve. Under this analogy, these correspond to real quadratic fields which were discussed in Section 1.5 which form a one parameter family of fields whose unit groups all have rank one.
Let E be an elliptic curve defined over the rationals by the minimal Weierstrass equation

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

and define the quantity $\eta_d(A,B)$ through

$$\log \eta_d(A,B) = \begin{cases} \min\{\hat{h}_{E_d}(P) : P \in E_d(\mathbb{Q}) \smallsetminus E_d(\mathbb{Q})_{\text{tors}}\}, & \text{rank}(E(\mathbb{Q})) \geq 1, \\ \infty, & \text{rank}(E(\mathbb{Q})) = 0. \end{cases} \tag{2.7.1}$$

If d is a square-free integer for which $\text{rank}(E_d(\mathbb{Q})) = 1$, then the group $E_d(\mathbb{Q})$ is generated (up to torsion) by a single point whose height is minimal amongst nontorsion points of $E_d(\mathbb{Q})$; this generator is the analogue of the fundamental unit of a real quadratic field. The elliptic regulator is then given solely in terms of the height of this generator as

$$\text{Reg}(E_d) = 2 \log \eta_d(A,B).$$

This expression should be compared with the one for $\text{Reg}(K)$ in (1.5.1), further cementing the idea that $\eta_d(A,B)$ is a direct analogue of ϵ_d defined in (1.1.2).
A very natural continuation is to attempt to transpose the results and conjectures stated in Chapter 1 to the context of elliptic curves. This was done by Le Boudec [LB16] for two particular results, with conclusions as follows.
First, it is known from the work of Iwaniec [Iwa90] and of Murty and Murty [MM91] that the average size of $L'(E_d,1)$ as d runs over square-free integers is about $\log d$. Meanwhile, the formula of the Birch and Swinnerton-Dyer Conjecture predicts that $L'(E_d,1)$ is of size roughly $d^{-1/2} \#Ш(E_d) \log \eta_d(A,B)$. It is therefore reasonable to expect that there exists a constant $c_E > 0$ depending on E such that one has

$$\sum_{\substack{d \in \mathcal{S}(X) \\ \text{rank}(E_d(\mathbb{Q}))=1}} \#Ш(E_d) \log \eta_d(A,B) \sim c_E X^{3/2} \log X, \tag{2.7.2}$$

as $X \to \infty$. This gives a conjectural analogue of Theorem 1.8, and thus also of the estimate of Siegel in (1.2.5).

Second is an analogue of Conjectures 1.3 and 1.4. One can expect that for every $\varepsilon > 0$ and for almost all square-free integers d for which $\operatorname{rank}(E_d(\mathbb{Q})) = 1$, it holds that

$$\eta_d(A, B) \geq \exp(d^{1/2-\varepsilon}). \tag{2.7.3}$$

Recall that the Conjecture 2.14 predicts that the set of square-free d for which E_d has rank at least two has density zero, and as the lower bound (2.7.3) is trivially satisfied for rank zero twists, one can expect it to hold for almost all square-free integers d. Here, Le Boudec [LB16] has shown that one has $\eta_d(A, B) > d^{1/4-\varepsilon}$ for almost all d. In comparison, the trivial lower bound for $\eta_d(A, B)$ (which should be compared with the lower bound in (1.2.7)) is of the form $\eta_d(A, B) \gg d^{1/8}$. This lower bound is sharp as it is attained for all square-free integers $d = z(x^3 + Axz^2 + Bz^3)$ with $x, z \geq 1$ and it follows from the work of Greaves [Gre92] that there are about $X^{1/2}$ such integers up to X. Finally, it is necessary to mention the work of Delaunay [Del01], [Del05], [Del07] who formulated predictions similar to the heuristics of Cohen and Lenstra from Conjecture 1.5 in the context of elliptic curves. These articles contain several conjectural results about the Tate–Shafarevich group with which the conjectural formulas (2.7.2) and (2.7.3) agree.

Chapter 3

The number of quadratic twists with a rational point of almost minimal height

3.1 Introduction

Fix a polynomial $F(x) \in \mathbb{Z}[x]$ of the form

$$F(x) = x^3 + Ax + B, \tag{3.1.1}$$

with discriminant

$$\Delta = -(4A^3 + 27B^2) \neq 0,$$

and let E be the elliptic curve defined over $\mathbb{Q}$ by the Weierstrass equation

$$E : y^2 = F(x).$$

Let $\mathcal{S}(X)$ denote the set of positive square-free integers up to X, and for $d \in \mathcal{S}(X)$, denote by E_d the quadratic twist of E defined over $\mathbb{Q}$ by the equation

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

We are interested in the quantity $\eta_d(A, B)$ defined in (2.7.1), which is roughlythe elliptic regulator $\mathrm{Reg}(E_d)$ whenever E_d has rank one, making it a sensible analogue of the quantity defined in (1.1.2). One has the sharp lower bound (see for instance [LB16, Section 2.2])

$$\eta_d(A, B) \gg d^{1/8}, \tag{3.1.2}$$

and following the work of Le Boudec [LB16], we are interested in the counting function

$$\mathcal{N}_\alpha(A, B; X) = \#\left\{d \in \mathcal{S}(X) : \eta_d(A, B) \leq d^{1/8+\alpha}\right\},$$

for a fixed $\alpha > 0$. This counting function mirrors the one considered by Hooley defined in (1.3.1), with (3.1.2) playing the role of the lower bound in (1.2.7).
Let $\lambda_{A,B}$ be the number of irreducible factors of $F(x)$ in $\mathbb{Z}[x]$. The following conjecture is the direct analogue of Conjecture 1.1 and was communicated to the author by Le Boudec in private conversations.

Conjecture 3.1. *Let $\alpha > 0$. There exists a constant $c_{A,B}(\alpha) > 0$ such that one has*

$$\mathcal{N}_\alpha(A, B; X) \sim c_{A,B}(\alpha) X^{1/2} (\log X)^{\lambda_{A,B}},$$

as $X \to \infty$.

Our main result establishes this prediction for sufficiently small values of α, similarly to how Hooley's Theorem 1.6 establishes Conjecture 1.1 for α small enough.

Theorem 3.1. *Let $\alpha \in (0, 1/120)$. There exists a constant $c_{A,B}(\alpha) > 0$ such that one has*

$$\mathcal{N}_\alpha(A, B; X) \sim c_{A,B}(\alpha) X^{1/2} (\log X)^{\lambda_{A,B}},$$

as $X \to \infty$.

Organisation of the chapter

We begin in Section 3.2 by establishing auxiliary results to be used later on. In Section 3.3, we follow the lines of Hooley's work as we investigate a modified counting function of lesser arithmetic significance, for which we prove an asymptotic formula. Finally, in Section 3.4, we deduce Theorem 3.1 from our work in Section 3.3 by relating the quantity $\mathcal{N}_\alpha(A, B; X)$ to the modified counting function through the Cauchy–Schwarz inequality. This results in an error term corresponding to the contribution of the curves having two rational points of small height that are linearly independent modulo 2-torsion. We show that this contribution is negligible using a theorem of Salberger [Sal08, Theorem 0.1] based on the determinant method (and which improved upon the work of Heath-Brown [HB02, Theorem 10]), as well as an explicit computation of lines on a quartic surface.

3.2 Preliminaries

For improved readability, we omit the dependency on A and B in the notation for new quantities defined from this point on.
If $f : \mathbb{Z}_{\geq 1} \to \mathbb{C}$ is an arithmetic function, we write $L(f, s)$ for the corresponding Dirichlet series

$$L(f, s) = \sum_{n \geq 1} \frac{f(n)}{n^s}.$$

We will require the following Tauberian theorem, which can be found in [CLT01, Appendix A]. Despite being a classical result, it does not seem to appear anywhere else in the literature, as noted by the authors.

Proposition 3.2. *Let $f : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 0}$ be an arithmetic function and let $S(f; X)$ be the corresponding summatory function*

$$S(f; X) = \sum_{n \leq X} f(n).$$

Assume that the Dirichlet series associated to f satisfies the following conditions

1. *$L(f, s)$ is absolutely convergent in some half-plane $\Re(s) > \sigma > 0$,*
2. *$L(f, s)$ meromorphically extends to a half-plane $\Re(s) > \sigma - \delta_0 > 0$ with a single pole at $s = \sigma$ of order m,*
3. *there exists $\kappa > 0$ such that for $\Re(s) > \sigma - \delta_0$, one has*

$$\left| L(f, s) \left(\frac{s - \sigma}{s} \right)^m \right| \leq |1 + \Im(s)|^\kappa.$$

Then, there exists a monic polynomial P of degree $m - 1$ such that for every $\delta \in (0, \delta_0)$, we have

$$S(f; X) = \frac{R}{\sigma (m-1)!} X^\sigma P(\log X) + O(X^{\sigma - \delta}),$$

as $X \to \infty$, where $R = \lim_{s \to \sigma} L(f, s)(s - \sigma)^m$.

3.2.1 Summing cubic congruences

For F the polynomial fixed in (3.1.1), we define the arithmetic function

$$\vartheta(n) = \#\left\{\rho \bmod n : F(\rho) \equiv 0 \bmod n\right\}, \tag{3.2.1}$$

and for $a \in \mathbb{Z}_{\geq 1}$, we define the summatory function

$$\Theta(a; X) = \sum_{n \leq X} \vartheta(n^a).$$

Recall that $\lambda_{A,B}$ denotes the number of irreducible factors of the polynomial F. In this section, we establish the following proposition.

Proposition 3.3. *For every $a \geq 1$, there exists $c_1(a) > 0$ such that*

$$\Theta(a; X) = c_1(a) X (\log X)^{\lambda_{A,B}-1} + O_a(X(\log X)^{\lambda_{A,B}-2}),$$

as $X \to \infty$.

This result is known to hold with a better error term in the case where F is an irreducible polynomial and $a = 1$, and can be found in an article of Lü [Lö09, Theorems 1.1 and 1.2]. The proof carries over to the case $a \geq 1$, as will be explained below.
We begin by establishing some properties of the arithmetic function ϑ, the first of which is its multiplicativity.

Lemma 3.4. *The function ϑ is multiplicative.*

Proof. Let q_1 and q_2 be two coprime integers and denote by $\bar{q}_1$ the inverse of q_1 modulo q_2 and by $\bar{q}_2$ the inverse of q_2 modulo q_1. The map

$$(\rho_1, \rho_2) \longmapsto q_1\bar{q}_1\rho_2 + q_2\bar{q}_2\rho_1 \bmod q_1q_2,$$

is a bijection from the set

$$\{(\rho_1, \rho_2) \in \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} : F(\rho_j) \equiv 0 \bmod q_j,\ j = 1, 2\},$$

to

$$\{\rho \in \mathbb{Z}/q_1q_2\mathbb{Z} : F(\rho) \equiv 0 \bmod q_1q_2\},$$

with inverse $\rho \mapsto (\rho \bmod q_1, \rho \bmod q_2)$. □

The next obvious step is to understand how the function ϑ behaves at powers of primes. It is a well-known fact (see for instance [Ste91, Corollary 2]) that for any p and $k \geq 1$, one has

$$\vartheta(p^k) \ll_p 1. \tag{3.2.2}$$

For the primes not dividing the discriminant Δ, one can be more precise.

Lemma 3.5. *Let $p \nmid \Delta$ and $k \geq 1$. One has*

$$\vartheta(p^k) = \vartheta(p).$$

Proof. By Hensel's lemma (see for instance [Neu99, II.4.6]), every simple root of the polynomial $F \bmod p$ lifts uniquely to a simple root of $F \bmod p^k$. □

We now state one more property of the function ϑ which will come into use in the next section.

Lemma 3.6. *Let $a, b \geq 1$. One has*

$$\vartheta(ab) \ll \vartheta(a)\vartheta(b).$$

Proof. If there exists p dividing a with $\vartheta(p) = 0$, then $\vartheta(p^k) = 0$ for all $k \geq 1$ as every root of $F \bmod p^k$ reduces to a root of $F \bmod p$. By multiplicativity, one then has $\vartheta(a) = \vartheta(ab) = 0$ so the result holds in this case. It remains to show that it also holds when $\vartheta(p) \geq 1$ for all p dividing ab. By Lemma 3.5 and (3.2.2), one has

$$\vartheta(ab) = \prod_{\substack{p^k \| ab \\ p \nmid \Delta}} \vartheta(p^k) \prod_{\substack{p^k \| ab \\ p \mid \Delta}} \vartheta(p^k) \ll \prod_{\substack{p \mid ab \\ p \nmid \Delta}} \vartheta(p),$$

as well as

$$\vartheta(a) = \prod_{\substack{p^k \| a \\ p \nmid \Delta}} \vartheta(p^k) \prod_{\substack{p^k \| a \\ p \mid \Delta}} \vartheta(p^k) \geq \prod_{\substack{p \mid a \\ p \nmid \Delta}} \vartheta(p).$$

Since the last inequality obviously also holds for $\vartheta(b)$, the result follows. □

With Lemma 3.5 established, one sees that the Dirichlet series associated to $\Theta(a; X)$, given by

$$L_a(s) = \sum_{n \geq 1} \frac{\vartheta(n^a)}{n^s},$$

scales from $L_1(s) = L(\vartheta, s)$ by a holomorphic factor that is bounded for $\Re(s) > 1/2$. Indeed, we have

$$L_a(s) = L_1(s) \prod_{p \mid \Delta} \left(1 + \sum_{k \geq 1} \frac{\vartheta(p^{ak})}{p^{ks}}\right) \left(1 + \sum_{k \geq 1} \frac{\vartheta(p^k)}{p^{ks}}\right)^{-1},$$

so by (3.2.2), the product over primes dividing the discriminant is as claimed. Because of this, the application of Perron's formula which stems Lü's proof can be carried out with $L_a(s)$ instead of $L_1(s)$ and the bounds in his article hold verbatim, so that his result extends to any $a \geq 1$.
To show Proposition 3.3, it remains to treat the cases $\lambda_{A,B} \in \{2, 3\}$. The next two lemmas give an explicit description of the value of the function ϑ at all but finitely many primes.

Lemma 3.7. *Assume $\lambda_{A,B} = 3$. For $p \nmid \Delta$, one has*

$$\vartheta(p) = 3.$$

Proof. This is an immediate consequence of the fact that every root of $F \bmod p$ is simple whenever p does not divide Δ. □

Lemma 3.8. *Assume $\lambda_{A,B} = 2$. There exist an integer $N \geq 1$ and a nonprincipal Dirichlet character $\chi \bmod N$ such that for $p \nmid N\Delta$, one has*

$$\vartheta(p) = 2 + \chi(p).$$

Proof. Denote by F_1 the irreducible quadratic factor of F_1 and let

$$\vartheta_1(n) = \#\{\rho \bmod n : F_1(\rho) \equiv 0 \bmod n\},$$

so that for $p \nmid \Delta$, we have $\vartheta(p) = 1 + \vartheta_1(p)$. Denote by K_1 the splitting field of F_1, by N its discriminant, and by χ the corresponding Kronecker symbol. By the Dedekind-Kummer theorem (see [Neu99, I.8.3]), the factorization of $F_1 \bmod p$ is determined by $\chi(p)$ for $p \nmid N$ and we therefore have $\vartheta_1(p) = 1 + \chi(p)$ for $p \nmid N\Delta$, thus proving the lemma. □

We now have all the necessary results to prove Proposition 3.3 for $\lambda_{A,B} \in \{2, 3\}$.

Proof of Proposition 3.3. As above, we write

$$L_a(s) = \sum_{n \geq 1} \frac{\vartheta(n^a)}{n^s}.$$

We begin by showing the result in the case $\lambda_{A,B} = 3$. By Lemma 3.7, the Euler product of $L_a(s)$ is given by

$$L_a(s) = \prod_{p|\Delta} \left(1 + \sum_{k\geq 1} \frac{\vartheta(p^{ak})}{p^{ks}}\right) \prod_{p\nmid\Delta} \left(1 + \frac{3}{p^s - 1}\right).$$

Setting

$$h_3(p;s) = 1 - \frac{3}{p^{2s}} + \frac{2}{p^{3s}},$$

we find

$$L_a(s) = \zeta(s)^3 \prod_{p|\Delta} \left(1 + \sum_{k\geq 1} \frac{\vartheta(p^{ak})}{p^{ks}}\right) \left(1 - \frac{1}{p^s}\right)^3 \prod_{p\nmid\Delta} h_3(p;s).$$

Using (3.2.2), we see that the product over the primes dividing Δ defines a bounded holomorphic function on $\Re(s) > 0$. Since the product $\prod_{p\nmid\Delta} h_3(p;s)$ is bounded and holomorphic for $\Re(s) > 1/2$, we can apply Proposition 3.2 in this region (after possibly dividing by a suitable constant so that the bound in the proposition is satisfied) to conclude the proof in this case.
We now move on to the case $\lambda_{A,B} = 2$. By Lemma 3.8, there exists N such that

$$L_a(s) = \prod_{p|N\Delta} \left(1 + \sum_{k\geq 1} \frac{\vartheta(p^{ak})}{p^{ks}}\right) \prod_{p\nmid N\Delta} \left(1 + \frac{2 + \chi(p)}{p^s - 1}\right).$$

Setting

$$h_2(p;s) = 1 - \frac{2 + \chi(p)}{p^{2s}} + \frac{1 + \chi(p)}{p^{3s}},$$

we find

$$L_a(s) = \zeta(s)^2 L(\chi, s) \prod_{p|N\Delta} \left(1 + \sum_{k\geq 1} \frac{\vartheta(p^{ak})}{p^{ks}}\right) \left(1 - \frac{1}{p^s}\right)^2 \left(1 - \frac{\chi(p)}{p^s}\right) \prod_{p\nmid N\Delta} h_2(p;s).$$

Here again, both products define functions that are holomorphic and bounded on $\Re(s) > 1/2$, and since χ is nonprincipal, $L(\chi, s)$ is also holomorphic and bounded in this region. It suffices to apply Proposition 3.2 to conclude the proof. □

3.2.2 Lemmas concerning arithmetic functions

This section contains several lemmas about arithmetic functions. We write

$$\tilde{F}(x,z) = x^3 + Axz^2 + Bz^3.$$

The first result of this section is an adaptation of the classical counting of roots modulo an integer and in an interval.

Lemma 3.9. *Let q, $z \in \mathbb{Z}$ with $(q,z) = 1$ and $t_1 < t_2$. We have*

$$\#\{t_1 < n \leq t_2 : \tilde{F}(n,z) \equiv 0 \bmod q\} = \left(\frac{t_2 - t_1}{q} + O(1)\right) \vartheta(q).$$

Proof. Splitting this set depending on the residue class of n mod q, one has

$$\#\{t_1 < n \leq t_2 : \tilde{F}(n,z) \equiv 0 \bmod q\} = \sum_{\substack{a \bmod q \\ \tilde{F}(a,z)\equiv 0 \bmod q}} \#\left\{t_1 < n \leq t_2 : n \equiv a \bmod q\right\},$$

and writing $a = cz$, this becomes

$$\#\{t_1 < n \leq t_2 : \tilde{F}(n,z) \equiv 0 \bmod q\} = \sum_{\substack{c \bmod q \\ F(c)\equiv 0 \bmod q}} \#\left\{t_1 < n \leq t_2 : n \equiv cz \bmod q\right\}.$$

The trivial estimate

$$\#\{t_1 < n \le t_2 : n \equiv cz \bmod q\} = \frac{t_2 - t_1}{q} + O(1),$$

completes the proof. □

Next, we define two arithmetic functions ϕ_1 and ϕ_2 by

$$\phi_1(n) = \prod_{p|n} \left(1 + \frac{1}{p}\right)^{-1}, \qquad \phi_2(n) = \prod_{p|n} \left(1 + \frac{1}{p+1}\right)^{-1}, \tag{3.2.3}$$

and prove some results involving them. We write φ for the Euler totient function and let

$$\sigma_x(n) = \sum_{d|n} d^x.$$

For brevity, we also write $(a_1, \dots, a_n) = \gcd(a_1, \dots, a_n)$.

Lemma 3.10. *Let $\ell, q \ge 1$ with $(\ell, q) = 1$, $\delta > 0$ and $X \ge 1$. We have*

$$\sum_{\substack{n \le X \\ (n,q)=1}} \frac{\varphi(\ell n)}{\ell n} = \frac{6}{\pi^2}\phi_1(\ell q)X + O_\delta\left(\frac{\sigma_{-\delta}(q)}{\phi_1(\ell q)}X^\delta\right).$$

Proof. Denote by $S(X)$ the sum to estimate. We have

$$S(X) = \sum_{\substack{n \le X \\ (n,q)=1}} \sum_{d|\ell n} \frac{\mu(d)}{d}.$$

Using Möbius inversion to get rid of the coprimality condition, we find

$$S(X) = \sum_{d \le \ell X} \frac{\mu(d)}{d} \sum_{g|q} \mu(g) \#\left\{m \le X/g : \ell g m \equiv 0 \bmod d\right\}.$$

The congruence condition can be replaced by $m \equiv 0 \bmod d/(\ell g, d)$, so that

$$S(X) = \sum_{d \le \ell X} \frac{\mu(d)}{d} \sum_{g|q} \mu(g) \left\lfloor \frac{X(\ell g, d)}{gd} \right\rfloor.$$

For any fixed $\delta > 0$ and any $N \ge 1$ we have the estimate $\lfloor N \rfloor = N + O(N^\delta)$. Since $(\ell, q) = 1$, we get

$$S(X) = X \sum_{d \le \ell X} \frac{\mu(d)(\ell, d)}{d^2} \sum_{g|q} \frac{\mu(g)(g, d)}{g} + O(E(X)),$$

where

$$E(X) = X^\delta \sum_{d \le \ell X} |\mu(d)| \frac{(\ell, d)^\delta}{d^{1+\delta}} \sum_{g|q} \frac{(g, d)^\delta}{g^\delta}.$$

To compute the main term, we use that

$$\sum_{g|q} \frac{\mu(g)(g, d)}{g} = \prod_{p|q} \left(1 - \frac{(p, d)}{p}\right).$$

The product vanishes whenever d is not coprime to q, hence

$$S(X) = X \prod_{p|q} \left(1 - \frac{1}{p}\right) \sum_{\substack{d \le \ell X \\ (d,q)=1}} \frac{\mu(d)(\ell, d)}{d^2} + O(E(X)).$$

We have

$$\sum_{\substack{d\leq \ell X\\(d,q)=1}}\frac{\mu(d)(\ell,d)}{d^2}=\prod_{p\nmid q}\left(1-\frac{(p,\ell)}{p^2}\right)+O(X^{-1}),$$

and we split this last product depending on whether p divides ℓ or not, giving

$$\begin{aligned}\prod_{p\nmid q}\left(1-\frac{(p,\ell)}{p^2}\right)&=\frac{1}{\zeta(2)}\prod_{p\mid \ell q}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p\mid \ell}\left(1-\frac{1}{p}\right)\\&=\frac{1}{\zeta(2)}\phi_1(\ell)\prod_{p\mid q}\left(1-\frac{1}{p^2}\right)^{-1},\end{aligned}$$

which produces the desired main term for $S(X)$. To estimate $E(X)$, note that

$$\sum_{g\mid q}\frac{(g,d)^\delta}{g^\delta}\leq (q,d)^\delta\sigma_{-\delta}(q),$$

from which we deduce that

$$E(X)\leq X^\delta\sigma_{-\delta}(q)\sum_{d\geq 1}\frac{|\mu(d)|(\ell q,d)^\delta}{d^{1+\delta}}\leq X^\delta\frac{\sigma_{-\delta}(q)}{\phi_1(\ell q)}\prod_p\left(1+\frac{1}{p^{1+\delta}}\right),$$

which concludes the proof. □

Lemma 3.11. *Let $q\geq 1$ and $X\geq 1$. We have*

$$\sum_{\substack{n\leq X\\(n,q)=1}}|\mu(n)|\phi_1(n)=c_2\phi_2(q)X+O_\epsilon(X^{1/2+\epsilon}),$$

with

$$c_2=\prod_p\left(1-\frac{2}{p(p+1)}\right).$$

Proof. Consider the Dirichlet series

$$f_1(s)=\prod_{p\nmid q}\left(1+\frac{\phi_1(p)}{p^s}\right).$$

Writing

$$g_1(s)=\prod_p\left(1+\frac{\phi_1(p)-1}{p^s}-\frac{\phi_1(p)}{p^{2s}}\right),\qquad g_2(s)=\prod_{p\mid q}\left(1+\frac{\phi_1(p)}{p^s}\right)^{-1},$$

a simple computation shows the identity $f_1(s)=\zeta(s)g_1(s)g_2(s)$. Both g_1 and g_2 are holomorphic and bounded for $\Re(s)>1/2$ and in this region, one has

$$\left|1+\frac{\phi_1(p)}{p^s}\right|^{-1}\leq\left(1+\frac{\phi_1(p)}{p^{1/2}}\right)^{-1}=1-\frac{1}{p^{1/2}+p^{-1/2}+1}<1,$$

so $|g_2(s)|<1$. Applying Proposition 3.2, it suffices to see that $g_1(1)=c_2$ and $g_2(1)=\phi_2(q)$ to conclude. □

Lemma 3.12. *Let $\delta>0$. One has*

$$\sum_{n\leq X}\frac{\sigma_{-\delta}(n)\vartheta(n^2)}{\phi_1(n)}\ll_\delta X(\log X)^{\lambda_{A,B}-1},$$

as $X\to\infty$.

Proof. For $\Re(s) > 1$, consider the Dirichlet series given by the product

$$f_2(s) = \prod_p \left(1 + \frac{1}{\phi_1(p)} \sum_{k\geq 1} \frac{\sigma_{-\delta}(p^k)\vartheta(p^{2k})}{p^{ks}}\right).$$

It is uniformly convergent on any compact in this half-plane. Setting

$$g_3(s) = \prod_{p|\Delta} \left(1 + \frac{1}{\phi_1(p)} \sum_{k\geq 1} \frac{\sigma_{-\delta}(p^k)\vartheta(p^{2k})}{p^{ks}}\right) \left(1 + \frac{\vartheta(p)}{\phi_1(p)} \sum_{k\geq 1} \frac{\sigma_{-\delta}(p^k)}{p^{ks}}\right)^{-1},$$

we find by Lemma 3.5 that

$$f_2(s) = g_3(s) \prod_p \left(1 + \frac{\vartheta(p)}{\phi_1(p)} \sum_{k\geq 1} \frac{\sigma_{-\delta}(p^k)}{p^{ks}}\right).$$

One easily shows the bounds

$$\sum_{k\geq 1} \frac{\sigma_{-\delta}(p^k)}{p^{ks}} = \frac{1}{p^s - 1} + O\left(\frac{1}{p^{\Re(s)+\delta}}\right), \qquad \frac{1}{\phi_1(p)} = 1 + O\left(\frac{1}{p}\right),$$

which lead to

$$1 + \frac{\vartheta(p)}{\phi_1(p)} \sum_{k\geq 1} \frac{\sigma_{-\delta}(p^k)}{p^{ks}} = 1 + \frac{\vartheta(p)}{p^s - 1} + O\left(\frac{1}{p^{\Re(s)+\delta}}\right).$$

We can then write

$$f_2(s) = g_3(s)g_4(s) \prod_p \left(1 + \frac{\vartheta(p)}{p^s - 1}\right),$$

where $g_4(s)$ is a function satisfying

$$g_4(s) = \prod_p \left(1 + O\left(\frac{1}{p^{\Re(s)+\delta}}\right)\right).$$

We can now relate $f_2(s)$ and $L(\vartheta, s)$ by defining

$$g_\vartheta(s) = \prod_{p|\Delta} \left(1 + \sum_{k\geq 1} \frac{\vartheta(p^k)}{p^{ks}}\right)^{-1} \left(1 + \frac{\vartheta(p)}{p^s - 1}\right). \tag{3.2.4}$$

Using Lemmas 3.4 and 3.5, we obtain

$$f_2(s) = g_3(s)g_4(s)g_\vartheta(s)L(\vartheta, s).$$

All three functions g_3, g_4 and g_ϑ are holomorphic for $\Re(s) > \max\{0, 1 - \delta\}$, so Proposition 3.2 applies as it did for $L(\vartheta, s)$ in the proof of Proposition 3.3. This gives the result. □

Finally, for $n \geq 1$, we define the arithmetic function

$$w(n) = \sum_{m\geq 1} \frac{\mu(m)\phi_1(mn)\phi_2(mn)\vartheta(m^2n^2)}{m^2}, \tag{3.2.5}$$

and show an asymptotic formula for its summatory function.

Lemma 3.13. *For $n \geq 1$, one has*

$$w(n) = \prod_{p\nmid n} \left(1 - \frac{\vartheta(p^2)}{p(p+2)}\right) \prod_{p^k||n} \left(\vartheta(p^{2k}) - \frac{\vartheta(p^{2k+2})}{p^2}\right) \left(1 + \frac{2}{p}\right)^{-1}.$$

Proof. Define a multiplicative arithmetic function $\tilde{w}$ via

$$\tilde{w}(p^k) = \frac{p}{p+2}\left(\vartheta(p^{2k}) - \frac{\vartheta(p^{2k+2})}{p^2}\right).$$

Fix a prime p dividing n and write $k = v_p(n)$, $n_p = np^{-k}$. We expand $w(n)$ into

$$w(n) = \phi_1(p^k)\phi_2(p^k)\vartheta(p^{2k}) \sum_{\substack{m\geq 1\\ p\nmid m}} \frac{\mu(m)\phi_1(n_p m)\phi_2(n_p m)\vartheta(n_p^2 m^2)}{m^2} + \sum_{\substack{m\geq 1\\ p\mid m}} \frac{\mu(m)\phi_1(n_p p^k m)\phi_2(n_p p^k m)\vartheta(n_p^2 p^{2k} m^2)}{m^2}.$$

Since m is square-free, it is exactly divisible by p in the second sum. Using the multiplicativity of ϑ, ϕ_1 and ϕ_2, we take that factor p out to obtain

$$w(n) = \left(\phi_1(p^k)\phi_2(p^k)\vartheta(p^{2k}) - \frac{\phi_1(p^{k+1})\phi_2(p^{k+1})\vartheta(p^{2k+2})}{p^2}\right) \times \sum_{\substack{m\geq 1\\ p\nmid m}} \frac{\mu(m)\phi_1(n_p m)\phi_2(n_p m)\vartheta(n_p^2 m^2)}{m^2}.$$

Since ϕ_1 and ϕ_2 are constant on prime powers, this yields

$$w(n) = \tilde{w}(p^k) \sum_{\substack{m\geq 1\\ p\nmid m}} \frac{\mu(m)\phi_1(n_p m)\phi_2(n_p m)\vartheta(n_p^2 m^2)}{m^2}.$$

Repeating this process on the remaining sum so as to go through all prime factors of n, we end up with

$$w(n) = \tilde{w}(n) \sum_{\substack{m\geq 1\\ (m,n)=1}} \frac{\mu(m)\phi_1(m)\phi_2(m)\vartheta(m^2)}{m^2}.$$

The function inside the sum is multiplicative and expanding it as a product, we find

$$w(n) = \tilde{w}(n) \prod_{p\nmid n}\left(1 - \frac{\vartheta(p^2)}{p(p+2)}\right),$$

which shows the asserted equality. □

Lemma 3.14. *There exists $c_3 > 0$ such that one has*

$$\sum_{n\leq X} w(n) = c_3 X(\log X)^{\lambda_{A,B}-1} + O(X(\log X)^{\lambda_{A,B}-2}),$$

as $X \to \infty$.

Proof. Using Lemma 3.13, we can write

$$w(n) = w_0 w_1(n),$$

where w_1 is a multiplicative function defined as

$$w_1(n) = \prod_{p^k\| n}\left(\vartheta(p^{2k}) - \frac{\vartheta(p^{2k+2})}{p^2}\right)\left(1+\frac{2}{p}\right)^{-1}\left(1 - \frac{\vartheta(p^2)}{p(p+2)}\right)^{-1},$$

and w_0 is the constant

$$w_0 = \prod_p \left(1 - \frac{\vartheta(p^2)}{p(p+2)}\right).$$

It is enough to estimate the sum $\sum_{n\leq X} w_1(n)$, which we do by looking at $L(w_1, s)$. For a prime p not dividing Δ, we have $w_1(p^k) = \vartheta(p)(1 + O(p^{-1}))$, and thus, we can write

$$L(w_1, s) = g_{w,1}(s) \prod_p \left(1 + \frac{\vartheta(p)}{p^s - 1}\left(1 + O(p^{-1})\right)\right),$$

with

$$g_{w,1}(s) = \prod_{p|\Delta} \left(1 + \sum_{k\geq 1} \frac{w_1(p^k)}{p^{ks}}\right) \left(1 + \frac{\vartheta(p)}{p^s - 1}\left(1 + O(p^{-1})\right)\right)^{-1}.$$

From the definition of w_1, it is easy to see that we have $w_1(p^k) \ll_p 1$. Hence, the function $g_{w,1}(s)$ is holomorphic for $\Re(s) > 0$. There exists a function

$$g_{w,2}(s) = \prod_p \left(1 + O(p^{-(\Re(s)+1)})\right),$$

which is holomorphic for $\Re(s) > 0$, and such that

$$L(w_1, s) = g_{w,1}(s) g_{w,2}(s) \prod_p \left(1 + \frac{\vartheta(p)}{p^s - 1}\right).$$

The product appearing in this expression is related to the Riemann zeta function. Using definition (3.2.4) of $g_\vartheta(s)$, we indeed see that

$$L(w_1, s) = g_{w,1}(s) g_{w,2}(s) g_\vartheta(s) L(\vartheta, s).$$

We apply Proposition 3.2 to $L(w_1, s)$ using the computation of $L(\vartheta, s)$ from Proposition 3.3 to conclude. □

3.3 A modified counting function

In this section, we investigate for $X \geq 1$ the modified counting function

$$\mathcal{N}^*_\alpha(X) = \sum_{d\in\mathcal{S}(X)} \#\left\{P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\text{tors}} : \exp \hat{h}_{E_d}(P) \leq d^{1/8+\alpha}\right\},$$

which is known to satisfy

$$X^{1/2-\epsilon} \ll_\epsilon \mathcal{N}^*_\alpha(X) \ll X^{1/2+4\alpha},$$

for any $\alpha > 0$ and $\epsilon > 0$ as X goes to infinity. The upper bound can be found in [LB16] while the lower bound comes from the family constructed by Gouvêa and Mazur [GM91]. The ϵ can be removed, as seen in [LB18].
This section is dedicated to establishing the more precise estimate from the following proposition.

Proposition 3.15. *Let $\alpha \in (0, 1/56)$. There exists $c_4(\alpha) > 0$ such that one has*

$$\mathcal{N}^*_\alpha(X) = c_4(\alpha) X^{1/2} (\log X)^{\lambda_{A,B}} + O(X^{1/2} (\log X)^{\lambda_{A,B}-1}),$$

as $X \to \infty$.

For the remainder of this section, we assume $\alpha < 1/56$.

3.3.1 Framing the quantity $\mathcal{N}_\alpha^*(X)$

We begin by recalling the definitions of the height functions in use (see [Sil09, VIII] for a more complete description). We denote the set of primitive vectors in $\mathbb{Z}^n$ by

$$\mathbb{Z}^n_{\text{prim}} = \{(a_1, \dots, a_n) \in \mathbb{Z}^n : \gcd(a_1, \dots, a_n) = 1\}.$$

The classical (logarithmic) height function $h : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{Z}$ is defined for $(x, z) \in \mathbb{Z}^2_{\text{prim}}$ by

$$h(x : z) = \log \max\{|x|, |z|\},$$

and the Weil height of a point $(x : y : z) \in \mathbb{P}^2(\mathbb{Q})$ is defined by

$$h_x(x : y : z) = \begin{cases} h(x : z), & (x : y : z) \neq (0 : 1 : 0), \\ 0, & (x : y : z) = (0 : 1 : 0). \end{cases}$$

Finally, the canonical height on the group $E(\mathbb{Q})$ is defined by the limit

$$\hat{h}_E(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h(2^n P).$$

By the basic properties of the canonical height (see for instance [Sil09, VIII.9.3]), there exist two constants h_1 and h_2 depending only on A and B and with $h_1 < 0 < h_2$ such that for every point $P \in E(\mathbb{Q})$, we have

$$h_1 \leq \hat{h}_E(P) - \frac{1}{2} h_x(P) \leq h_2.$$

Because E_d and E are isomorphic over $\bar{\mathbb{Q}}$ via the map

$$\begin{array}{rccc} \iota : & E_d(\bar{\mathbb{Q}}) & \longrightarrow & E(\bar{\mathbb{Q}}) \\ & (x : y : z) & \longmapsto & (x : d^{1/2} y : z), \end{array}$$

and because of the invariance under $\bar{\mathbb{Q}}$-isomorphism of the canonical height, we have

$$\hat{h}_{E_d}(P) = \hat{h}_E(\iota(P)),$$

for every P. Moreover, it is immediate that for $P \in E_d(\mathbb{Q})$ the equality $h_x(P) = h_x(\iota(P))$ holds, which means that for any $P \in E_d(\mathbb{Q})$ we have

$$h_1 \leq \hat{h}_{E_d}(P) - \frac{1}{2} h_x(P) \leq h_2. \tag{3.3.1}$$

A point $P = (x : y : z)$ in $E_d(\mathbb{Q})$ is a torsion point if and only if $\hat{h}_{E_d}(P) = 0$. By (3.3.1), this means that both $|x|$ and $|z|$ are bounded. From the equation of the curve, this also implies that dy^2 is bounded and therefore so is d, provided that $y \neq 0$. We have thus shown the estimate

$$\sum_{d \in \mathcal{S}(X)} \#\left\{P \in E_d(\mathbb{Q})_{\text{tors}} \setminus E_d(\mathbb{Q})[2]\right\} \ll 1.$$

This motivates the definition of a new quantity

$$\mathcal{N}_\alpha^\dagger(X) = \sum_{d \in \mathcal{S}(X)} \#\left\{P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})[2] : \exp \hat{h}_{E_d}(P) \leq d^{1/8+\alpha}\right\},$$

which is related to $\mathcal{N}_\alpha^*(X)$ through

$$\mathcal{N}_\alpha^*(X) = \mathcal{N}_\alpha^\dagger(X) + O(1). \tag{3.3.2}$$

For $j \in \{1, 2\}$, we define the quantities

$$\mathcal{N}_{\alpha,j}(X) = \sum_{d \in \mathcal{S}(X)} \#\left\{P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})[2] : \mathrm{e}^{h_j} (\exp h_x(P))^{1/2} \leq d^{1/8+\alpha}\right\},$$

with h_1 and h_2 the constants defined above. Observe that we have the inequalities

$$\mathcal{N}_{\alpha,2}(X) \leq \mathcal{N}_\alpha^\dagger(X) \leq \mathcal{N}_{\alpha,1}(X). \tag{3.3.3}$$

As a consequence of (3.3.2) and (3.3.3), Proposition 3.15 will follow from the next proposition.

Proposition 3.16. *There exists $c_5(\alpha) > 0$ such that for $j \in \{1,2\}$, we have*

$$\mathcal{N}_{\alpha,j}(X) = c_5(\alpha) X^{1/2} (\log X)^{\lambda_{A,B}} + O_j(X^{1/2}(\log X)^{\lambda_{A,B}-1}),$$

as $X \to \infty$.

The remainder of this section is dedicated to proving this proposition.

3.3.2 Asymptotic behavior of $\mathcal{N}_{\alpha,j}(X)$

Fix $j \in \{1,2\}$. We begin by setting $C_j = \mathrm{e}^{-2h_j}$, so that

$$\mathcal{N}_{\alpha,j}(X) = \sum_{d \in \mathcal{S}(X)} \#\left\{ (x,y,z) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0} \times \mathbb{Z}_{\geq 1} : \begin{array}{r} |x|, z \leq C_j d^{1/4+2\alpha} \\ (x,y,z) = 1 \\ dy^2 z = \tilde{F}(x,z) \end{array} \right\}.$$

The triples (x,y,z) counted here all come in pairs as the conditions are independent of the sign of y. We will thus restrict our attention to $y \geq 1$. We call upon a result describing the coordinates of rational points on the twisted curve E_d (see for instance [LB16, Lemma 1]).

Lemma 3.17. *Let $d \geq 1$ square-free and let $(x_0, y, z_0) \in \mathbb{Z} \times \mathbb{Z}^2_{\geq 1}$ satisfying $(x_0, y, z_0) = 1$ and $dy^2 z_0 = \tilde{F}(x_0, z_0)$. There is a unique way to write*

$$d = d_0 d_1, \qquad x_0 = d_1 x z, \qquad z_0 = d_1^2 z^3,$$

with $(d_0, d_1, z, x) \in \mathbb{Z}^3_{\geq 1} \times \mathbb{Z}$ satisfying $(xy, d_1 z) = 1$ and

$$d_0 y^2 = \tilde{F}(x, d_1 z^2).$$

Applying Lemma 3.17, we obtain the new expression

$$\mathcal{N}_{\alpha,j}(X) = 2\# \left\{ (d_0, d_1, y, z, x) \in \mathbb{Z}^4_{\geq 1} \times \mathbb{Z} : \begin{array}{r} d_0 d_1 \in \mathcal{S}(X) \\ |x|, d_1 z^2 \leq C_j (d_0 d_1)^{1/4+2\alpha} \\ (xy, d_1 z) = 1 \\ d_0 y^2 = \tilde{F}(x, d_1 z^2) \end{array} \right\}.$$

We now derive an explicit description of the range of the product yz. Setting

$$C_0 = 1 + |A| + |B|,$$

the equation of the curve implies $d_0 y^2 \leq C_0 \max\{|x|, d_1 z^2\}^3$, from which we obtain the inequality

$$\max\{|x|, d_1 z^2\} (d_1 z^2)^{-1/4} \geq \max\{|x|, d_1 z^2\}^{3/4} \geq C_0^{-1/4} d_0^{1/4} y^{1/2}.$$

From this, we extract

$$\max\{|x|, d_1 z^2\} \geq C_0^{-1/4} (yz)^{1/2} (d_0 d_1)^{1/4},$$

and defining $D_j = C_0^{1/2} C_j^2$, this implies that $yz \leq D_j (d_0 d_1)^{4\alpha}$. This recovers the bound $\eta_d(A,B) \gg d^{1/8}$ stated in the introduction. Taking this restriction into account, $\mathcal{N}_{\alpha,j}(X)$ can be written as

$$\mathcal{N}_{\alpha,j}(X) = 2\# \left\{ (d_0, d_1, y, z, x) \in \mathbb{Z}^4_{\geq 1} \times \mathbb{Z} : \begin{array}{r} d_0 d_1 \in \mathcal{S}(X) \\ |x|, d_1 z^2 \leq C_j (d_0 d_1)^{1/4+2\alpha} \\ yz \leq D_j (d_0 d_1)^{4\alpha} \\ (xy, d_1 z) = 1 \\ d_0 y^2 = \tilde{F}(x, d_1 z^2) \end{array} \right\}.$$

Note that d_0 and d_1 are necessarily coprime here because the equation of the curve implies that $(d_0, d_1) \mid x^3$, while $(x, d_1) = 1$. We get rid of the square-free condition on d_0 by means of Möbius inversion, writing $d_0 = \ell^2 d_2$. The previous expression becomes

$$\mathcal{N}_{\alpha,j}(X) = 2 \sum_{\ell \leq X^{1/2}} \mu(\ell) \# \left\{ (d_2, d_1, y, z, x) \in \mathbb{Z}^4_{\geq 1} \times \mathbb{Z} : \begin{array}{r} \ell^2 d_1 d_2 \leq X,\ \mu(d_1) \neq 0 \\ |x|, d_1 z^2 \leq C_j (\ell^2 d_1 d_2)^{1/4+2\alpha} \\ yz \leq D_j (\ell^2 d_1 d_2)^{4\alpha} \\ (\ell xy, d_1 z) = 1 \\ \ell^2 y^2 d_2 = \tilde{F}(x, d_1 z^2) \end{array} \right\}.$$

The equation of the curve in this last expression brings to light the constraint

$$\ell y \leq K_j X^{3/8+3\alpha},$$

where $K_j = (C_0 C_j^3)^{1/2}$, and shows that the variable d_2 is completely determined by the other five. We define the range of the variable x

$$\mathcal{X}_j(g,y,z,d_1;\alpha;X) = \left\{ x \in \mathbb{R} : \begin{array}{c} d_1 y^{-2}\tilde{F}(gx,d_1z^2) \leq X \\ |gx|, d_1z^2 \leq C_j(d_1y^{-2}\tilde{F}(gx,d_1z^2))^{1/4+2\alpha} \\ yz \leq D_j(d_1y^{-2}\tilde{F}(gx,d_1z^2))^{4\alpha} \end{array} \right\},$$

and with this notation, we have

$$\mathcal{N}_{\alpha,j}(X) = 2\sum_{\ell \leq X^{1/2}} \mu(\ell) \# \left\{ (d_1,y,z,x) \in \mathbb{Z}_{\geq 1}^3 \times \mathbb{Z} : \begin{array}{c} x \in \mathcal{X}_j(1,y,z,d_1;\alpha;X) \\ \ell y \leq K_j X^{3/8+3\alpha} \\ (\ell xy, d_1 z) = 1,\ \mu(d_1) \neq 0 \\ \tilde{F}(x,d_1z^2) \equiv 0 \bmod \ell^2 y^2 \end{array} \right\}.$$

Next, we set

$$\mathcal{A}_j(y,z,\ell;\alpha;X) = \left\{ (d_1,x) \in \mathbb{Z}_{\geq 1} \times \mathbb{Z} : \begin{array}{c} x \in \mathcal{X}_j(1,y,z,d_1;\alpha;X) \\ (\ell xy, d_1 z) = 1,\ \mu(d_1) \neq 0 \\ \tilde{F}(x,d_1z^2) \equiv 0 \bmod \ell^2 y^2 \end{array} \right\},$$

so that the cardinality to estimate now reads

$$\mathcal{N}_{\alpha,j}(X) = 2\sum_{\ell \leq X^{3/8+3\alpha}} \mu(\ell) \sum_{\substack{yz \leq D_j X^{4\alpha} \\ \ell y \leq K_j X^{3/8+3\alpha}}}\sum \#\mathcal{A}_j(y,z,\ell;\alpha;X).$$

For a parameter $\theta \in (0, 3/8+3\alpha)$, we define the quantity $\mathcal{N}_{\alpha,j}^{(\theta)}(X)$, corresponding to the contribution of the terms with $\ell y > X^\theta$, by

$$\mathcal{N}_{\alpha,j}^{(\theta)}(X) = \sum_{\ell \leq X^{3/8+3\alpha}} \mu(\ell) \sum_{\substack{yz \leq D_j X^{4\alpha} \\ X^\theta < \ell y \leq K_j X^{3/8+3\alpha}}}\sum \#\mathcal{A}_j(y,z,\ell;\alpha;X).$$

To estimate this quantity, we will require the following statement, which is an immediate consequence of a result of Heath-Brown [HB84, Lemma 3].

Lemma 3.18. *Let $(m_1,m_2,q) \in \mathbb{Z}^3_{\mathrm{prim}}$ with $q \neq 0$ and let $X_1, X_2 > 0$. We have*

$$\# \left\{ (x_1,x_2) \in \mathbb{Z}^2_{\mathrm{prim}} : \begin{array}{c} |x_1| \leq X_1,\ |x_2| \leq X_2 \\ x_1m_1 + x_2m_2 \equiv 0 \bmod q \end{array} \right\} \ll \frac{X_1X_2}{q} + 1.$$

We can now show the desired estimate.

Lemma 3.19. *One has*

$$\mathcal{N}_{\alpha,j}^{(\theta)}(X) \ll_\epsilon X^{1/2+8\alpha-\theta+\epsilon} + X^{3/8+7\alpha+\epsilon}.$$

Proof. Relaxing the conditions on d_1 and x, we find

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) \ll \# \left\{ (d_1,x) \in \mathbb{Z}_{\geq 1} \times \mathbb{Z} : \begin{array}{c} |x|, d_1 \ll X^{1/4+2\alpha} \\ (\ell xy, d_1 z) = 1 \\ \tilde{F}(x,d_1z^2) \equiv 0 \bmod \ell^2 y^2 \end{array} \right\}.$$

Splitting the right-hand side depending on the congruence class of x mod ℓ^2y^2, we find

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) \ll \sum_{\substack{\rho \bmod \ell^2y^2 \\ \tilde{F}(\rho,z^2) \equiv 0 \bmod \ell^2y^2}} \# \left\{ (d_1,x) \in \mathbb{Z}_{\geq 1} \times \mathbb{Z} : \begin{array}{c} |x|, d_1 \ll X^{1/4+2\alpha} \\ (\ell xy, d_1 z) = 1 \\ x \equiv \rho d_1 \bmod \ell^2 y^2 \end{array} \right\},$$

and the coprimality condition $(\ell y, z) = 1$ allows for a change of variables leading to

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) \ll \sum_{\substack{\rho \bmod \ell^2y^2 \\ F(\rho)\equiv 0 \bmod \ell^2y^2}} \#\left\{(d_1,x)\in\mathbb{Z}_{\geq 1}\times\mathbb{Z} : \begin{array}{c} |x|, d_1 \ll X^{1/4+2\alpha} \\ (\ell xy, d_1 z) = 1 \\ x \equiv \rho d_1 z^2 \bmod \ell^2y^2 \end{array}\right\}.$$

Recall the definition of ϑ in (3.2.1). We apply Lemma 3.18 to find the estimate

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) \ll \left(\frac{X^{1/2+4\alpha}}{\ell^2y^2}+1\right)\vartheta(\ell^2y^2).$$

Using the easy estimate $\vartheta(n) \ll_\epsilon n^\epsilon$ and carrying out the summation over z, one obtains

$$\mathcal{N}^{(\theta)}_{\alpha,j}(X) \ll_\epsilon X^{1/2+8\alpha+\epsilon}\sum_{\ell y > X^\theta}\sum\frac{1}{\ell^2y^3} + X^{4\alpha+\epsilon}\sum_{\ell y \leq X^{3/8+3\alpha}}\sum\frac{1}{y},$$

which shows the result. □

Going back to $\mathcal{N}_{\alpha,j}(X)$, we restrict our attention to the small values of ℓy. Indeed, we have $\alpha < 1/56$ so Lemma 3.19 allows us to write

$$\mathcal{N}_{\alpha,j}(X) = 2\sum_{\ell y\leq X^\theta}\sum\mu(\ell)\sum_{yz\leq D_jX^{4\alpha}}\#\mathcal{A}_j(y,z,\ell;\alpha;X) + O_\epsilon(X^{7/8+11\alpha-2\theta+\epsilon}) + O(X^{1/2}).$$

We now turn to the cardinality of $\mathcal{A}_j(y,z,\ell;\alpha;X)$ in this range. It can be written as

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) = \sum_{\substack{d_1\leq C_jX^{1/4+2\alpha}\\(\ell y,d_1z)=1}}|\mu(d_1)|\#\left\{x\in\mathbb{Z} : \begin{array}{c} x\in\mathcal{X}_j(1,y,z,d_1;\alpha;X) \\ (x,d_1z)=1 \\ \tilde{F}(x,d_1z^2)\equiv 0 \bmod \ell^2y^2\end{array}\right\},$$

and getting rid of the coprimality condition on x, we find

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) = \sum_{\substack{d_1\leq C_jX^{1/4+2\alpha}\\(\ell y,d_1z)=1}}|\mu(d_1)|\sum_{g|d_1z}\mu(g)\#\left\{x\in\mathbb{Z} : \begin{array}{c} x\in\mathcal{X}_j(g,y,z,d_1;\alpha;X) \\ \tilde{F}(gx,d_1z^2)\equiv 0 \bmod \ell^2y^2\end{array}\right\}.$$

Note that the congruence relation in this last expression can be replaced by

$$\tilde{F}(x,d_1z^2g^{-1})\equiv 0 \bmod \ell^2y^2.$$

Moreover, since, by definition, $\mathcal{X}_j(g,y,z,d_1;\alpha;X)$ is a union of a finite number of intervals, Lemma 3.9 gives

$$\#\mathcal{A}_j(y,z,\ell;\alpha;X) = \frac{\vartheta(\ell^2y^2)}{\ell^2y^2}\sum_{\substack{d_1\leq C_jX^{1/4+2\alpha}\\(\ell y,d_1z)=1}}|\mu(d_1)|\sum_{g|d_1z}\mu(g)\operatorname{vol}(\mathcal{X}_j(g,y,z,d_1;\alpha;X)) + O_\epsilon(X^{1/4+2\alpha+\epsilon}),$$

where $\operatorname{vol}(\mathcal{X})$ denotes the Lebesgue measure of $\mathcal{X}$. We can now define the main term

$$\mathcal{M}_{\alpha,j}(X) = \sum_{\ell y\leq X^\theta}\sum\frac{\mu(\ell)\vartheta(\ell^2y^2)}{\ell^2y^2}\sum_{yz\leq D_jX^{4\alpha}}\sum_{\substack{d_1\leq XC_j^{1/4+2\alpha}\\(\ell y,d_1z)=1}}|\mu(d_1)|\sum_{g|d_1z}\mu(g)\operatorname{vol}(\mathcal{X}_j(g,y,z,d_1;\alpha;X)), \tag{3.3.4}$$

so as to have

$$\mathcal{N}_{\alpha,j}(X) = 2\mathcal{M}_{\alpha,j}(X) + O(X^{1/2}) + O_\epsilon(X^{1/2+8\alpha-\theta+\epsilon}) + O_\epsilon(X^{1/4+6\alpha+\theta+\epsilon}).$$

Since we assume $\alpha < 1/56$, we may choose θ in the range

$$8\alpha < \theta < \frac{1}{4} - 6\alpha, \tag{3.3.5}$$

making all three error terms less than $X^{1/2}$ and leaving us with

$$\mathcal{N}_{\alpha,j}(X) = 2\mathcal{M}_{\alpha,j}(X) + O(X^{1/2}). \tag{3.3.6}$$

3.3.3 Asymptotic behavior of $\mathcal{M}_{\alpha,j}(X)$

To compute the expression defined in (3.3.4), we start by defining the function

$$G(t,u,v) = \max\left\{ v\tilde{F}(t,u^2v), \frac{|t|}{(v\tilde{F}(t,u^2v))^{1/4+2\alpha}}, \frac{u^2v}{(v\tilde{F}(t,u^2v))^{1/4+2\alpha}}, \frac{u}{C_0^{1/2}(v\tilde{F}(t,u^2v))^{4\alpha}} \right\},$$

as well as the quantities

$$\mathfrak{X}_j = C_j X^{1/4+2\alpha}, \qquad \mathfrak{Z}_j = \frac{C_j^2 X^{4\alpha}}{y}, \qquad \mathfrak{D}_j = \frac{y^2 X^{1/4-6\alpha}}{C_j^3}.$$

These satisfy $\mathfrak{D}_j\mathfrak{Z}_j^2 = \mathfrak{X}_j$ and $\mathfrak{D}_j\mathfrak{X}_j^3 = y^2X$, so if we let $(t,u,v) = (gx/\mathfrak{X}_j, z/\mathfrak{Z}_j, d_1/\mathfrak{D}_j)$, we obtain

$$v\tilde{F}(t,u^2v) = \frac{d_1\tilde{F}(gx,d_1z^2)}{y^2X}.$$

In particular, the condition $x \in \mathcal{X}_j(g,y,z,d_1;\alpha;X)$ is equivalent to

$$0 < G\left(\frac{gx}{\mathfrak{X}_j}, \frac{z}{\mathfrak{Z}_j}, \frac{d_1}{\mathfrak{D}_j}\right) \le 1,$$

and the measure of the set $\mathcal{X}_j(g,y,z,d_1;\alpha;X)$ can therefore be written as an integral

$$\mathrm{vol}(\mathcal{X}_j(g,y,z,d_1;\alpha;X)) = \int_{0<G(gt/\mathfrak{X}_j,z/\mathfrak{Z}_j,d_1/\mathfrak{D}_j)\le 1} \mathrm{d}t.$$

Taking g out of this integral, we define

$$A_{\alpha,j}^{(1)}(y,z,d_1) = \int_{0<G(t/\mathfrak{X}_j,z/\mathfrak{Z}_j,d_1/\mathfrak{D}_j)\le 1} \mathrm{d}t,$$

so that after a change of variables and after carrying out the summation over g, $\mathcal{M}_{\alpha,j}(X)$ becomes

$$\mathcal{M}_{\alpha,j}(X) = \sum_{\ell y \le X^\theta}\sum \frac{\mu(\ell)\vartheta(\ell^2y^2)}{\ell^2y^2} \sum_{\substack{d_1 \le C_jX^{1/4+2\alpha} \\ (d_1,\ell y)=1}} |\mu(d_1)| \sum_{\substack{yz \le D_jX^{4\alpha} \\ (z,\ell y)=1}} \frac{\varphi(d_1z)}{d_1z} A_{\alpha,j}^{(1)}(y,z,d_1).$$

The next step is to compare the sum over z with the corresponding integral, which can be done as $A_{\alpha,j}^{(1)}(y,z,d_1)$ is a piecewise C^1 function in the z and d_1 variables. Recall the definitions of ϕ_1 and ϕ_2 in (3.2.3). By means of Abel summation and making use of Lemma 3.10 to estimate the sum, we obtain

$$\sum_{\substack{z \le D_jX^{4\alpha}/y \\ (z,\ell y)=1}} \frac{\varphi(d_1z)}{d_1z} A_{\alpha,j}^{(1)}(y,z,d_1) = \frac{6}{\pi^2}\phi_1(d_1)\phi_1(\ell y)\int_{u\ge 1} A_{\alpha,j}^{(1)}(y,u,d_1)\,\mathrm{d}u$$
$$+ O\left(\frac{\sigma_{-1/2}(\ell y)}{\phi_1(\ell y)\phi_1(d_1)}\left(\frac{X^{4\alpha}}{y}\right)^{1/2} \max_{z\le D_jX^{4\alpha}/y} A_{\alpha,j}^{(1)}(y,z,d_1)\right),$$

We can now define

$$A^{(2)}_{\alpha,j}(y,d_1)=\int_{u\geq 1}A^{(1)}_{\alpha,j}(y,u,d_1)\,\mathrm{d}u,$$

and rewrite $\mathcal{M}_{\alpha,j}(X)$ as

$$\mathcal{M}_{\alpha,j}(X)=\frac{6}{\pi^2}\sum_{\substack{\ell y\leq X^{\theta}\\ y\leq D_jX^{4\alpha}}}\sum\frac{\mu(\ell)\phi_1(\ell y)\vartheta(\ell^2y^2)}{\ell^2y^2}\sum_{\substack{d_1\leq C_jX^{1/4+2\alpha}\\ (d_1,\ell y)=1}}|\mu(d_1)|\phi_1(d_1)A^{(2)}_{\alpha,j}(y,d_1)$$
$$+O(E^{(1)}_{\alpha,j}(X)),$$

where

$$E^{(1)}_{\alpha,j}(X)=X^{2\alpha}\sum_{\substack{\ell y\leq X^{\theta}\\ y\ll X^{4\alpha}}}\sum\frac{\sigma_{-1/2}(\ell y)\vartheta(\ell^2y^2)}{\phi_1(\ell y)\ell^2y^{5/2}}\sum_{d_1\ll X^{1/4+2\alpha}}\frac{1}{\phi_1(d_1)}\max_{z\leq D_jX^{4\alpha}/y}A^{(1)}_{\alpha,j}(y,z,d_1).$$

Next, we proceed as previously and compare the sum over d_1 in $\mathcal{M}_{\alpha,j}(X)$ with the corresponding integral using Lemma 3.11 to find

$$\sum_{\substack{d_1\leq C_jX^{1/4+2\alpha}\\ (d_1,\ell y)=1}}|\mu(d_1)|\phi_1(d_1)A^{(2)}_{\alpha,j}(y,d_1)=c_2\phi_2(\ell y)\int_{v\geq 1}A^{(2)}_{\alpha,j}(y,v)\,\mathrm{d}v$$
$$+O_{\epsilon}\left(X^{1/8+\alpha+\epsilon}\max_{d_1\leq C_jX^{1/4+2\alpha}}A^{(2)}_{\alpha,j}(y,d_1)\right).$$

Setting

$$A^{(3)}_{\alpha,j}(y)=\int_{v\geq 1}A^{(2)}_{\alpha,j}(y,v)\,\mathrm{d}v,$$

we arrive at the following expression

$$\mathcal{M}_{\alpha,j}(X)=\frac{6c_2}{\pi^2}\sum_{\substack{\ell y\leq X^{\theta}\\ y\leq D_jX^{4\alpha}}}\sum\frac{\mu(\ell)\phi_1(\ell y)\phi_2(\ell y)\vartheta(\ell^2y^2)}{\ell^2y^2}A^{(3)}_{\alpha,j}(y)$$
$$+O(E^{(1)}_{\alpha,j}(X))+O(E^{(2)}_{\alpha,j}(X)),$$

where

$$E^{(2)}_{\alpha,j}(X)\ll_{\epsilon}X^{1/8+\alpha+\epsilon}\sum_{\ell y\leq X^{\theta}}\sum\frac{\vartheta(\ell^2y^2)}{\ell^2y^2}\max_{d_1\leq C_jX^{1/4+2\alpha}}A^{(2)}_{\alpha,j}(y,d_1).$$

At this point, we extend the range of integration in $A^{(3)}_{\alpha,j}(y)$ by defining

$$A^{(4)}_{\alpha,j}(y)=\int_{v>0}\int_{u>0}A^{(1)}_{\alpha,j}(y,u,v)\,\mathrm{d}u\,\mathrm{d}v,$$

and since $A^{(1)}_{\alpha,j}(y,u,v)\ll\mathfrak{X}_j$ for every $u,v>0$, the difference between the two integrals satisfies

$$A^{(4)}_{\alpha,j}(y)-A^{(3)}_{\alpha,j}(y)\ll\mathfrak{X}_j\mathfrak{D}_j+\mathfrak{X}_j\mathfrak{Z}_j+\mathfrak{X}_j\ll X^{1/2-4\alpha}y^2+\frac{X^{1/4+6\alpha}}{y}+X^{1/4+2\alpha}.$$

Since $y\geq 1$ and we are assuming that $\alpha<1/40$, the term $X^{1/2-4\alpha}y^2$ is dominating here. Replacing $A^{(3)}_{\alpha,j}(y)$ by $A^{(4)}_{\alpha,j}(y)$ in the last expression for $\mathcal{M}_{\alpha,j}(X)$ results in the error term

$$X^{1/2-4\alpha}\sum_{\substack{\ell y\leq X^{\theta}\\ y\ll X^{4\alpha}}}\sum\frac{\vartheta(\ell^2y^2)}{\ell^2}\ll X^{1/2}(\log X)^{\lambda_{A,B}-1},$$

so we have

$$\mathcal{M}_{\alpha,j}(X) = \frac{6c_2}{\pi^2} \sum_{\substack{\ell y \le X^\theta \\ y \le D_j X^{4\alpha}}}\sum \frac{\mu(\ell)\phi_1(\ell y)\phi_2(\ell y)\vartheta(\ell^2 y^2)}{\ell^2 y^2} A^{(4)}_{\alpha,j}(y) + O(E^{(1)}_{\alpha,j}(X)) + O(E^{(2)}_{\alpha,j}(X)) + O(X^{1/2}(\log X)^{\lambda_{A,B}-1}).$$

We now compute the size of both error terms $E^{(1)}_{\alpha,j}(X)$ and $E^{(2)}_{\alpha,j}(X)$.

Lemma 3.20. *We have*

$$E^{(1)}_{\alpha,j}(X) \ll X^{1/2}(\log X)^{\lambda_{A,B}-1},$$

as $X \to \infty$.

Proof. We compare the sum over d_1 with the corresponding integral and make use of the fact that $\phi_1(d_1)^{-1}$ is constant on average. Indeed, as an easy application of Proposition 3.2, one has that there exists a constant $c_6 > 0$ such that

$$\sum_{n \le N} \phi_1(n)^{-1} = c_6 N + O_\epsilon(N^\epsilon),$$

which leads to the estimate

$$\sum_{d_1 \ll X^{1/4+2\alpha}} \frac{1}{\phi_1(d_1)} \max_{z \le D_j X^{4\alpha}/y} A^{(1)}_{\alpha,j}(y,z,d_1) \ll \int_{v \ge 1} A^{(1)}_{\alpha,j}(y,z_m,v)\,\mathrm{d}v,$$

where z_m denotes the point where the maximum is attained. The size of the sum over d_1 is therefore at most $\mathfrak{X}_j\mathfrak{D}_j \ll X^{1/2-4\alpha}y^2$ and we obtain

$$E^{(1)}_{\alpha,j}(X) \ll X^{1/2-2\alpha} \sum_{y \ll X^{4\alpha}} \frac{\sigma_{-1/2}(y)\vartheta(y^2)}{\phi_1(y)y^{1/2}} \sum_{\ell \le X^\theta/y} \frac{\sigma_{-1/2}(\ell)\vartheta(\ell^2)}{\phi_1(\ell)\ell^2}.$$

Both sums can be computed using Lemma 3.12 and Abel summation to show the lemma. □

Lemma 3.21. *We have*

$$E^{(2)}_{\alpha,j}(X) \ll_\epsilon X^{3/8+7\alpha+\epsilon},$$

as $X \to \infty$.

Proof. It suffices to note that $A^{(2)}_{\alpha,j}(y,d) \ll \mathfrak{X}_j\mathfrak{Z}_j \ll X^{1/4+6\alpha}$ since the sum over ℓ and y is bounded by a constant by Lemma 3.6 and Proposition 3.3. □

In light of Lemmas 3.20 and 3.21 and since we assume $\alpha < 1/56$, we can now write

$$\mathcal{M}_{\alpha,j}(X) = \frac{6c_2}{\pi^2} \sum_{\substack{\ell y \le X^\theta \\ y \le D_j X^{4\alpha}}}\sum \frac{\mu(\ell)\phi_1(\ell y)\phi_2(\ell y)\vartheta(\ell^2 y^2)}{\ell^2 y^2} A^{(4)}_{\alpha,j}(y) + O(X^{1/2}(\log X)^{\lambda_{A,B}-1}).$$

Define

$$\Omega(\alpha) = \iiint_{\substack{u,v>0 \\ 0<G(t,u,v)\le 1}} \mathrm{d}t\,\mathrm{d}u\,\mathrm{d}v,$$

and remark that this expression relates to $A^{(4)}_{\alpha,j}(y)$ through

$$A^{(4)}_{\alpha,j}(y) = \Omega(\alpha)\mathfrak{X}_j\mathfrak{Z}_j\mathfrak{D}_j = \Omega(\alpha)X^{1/2}y,$$

and incorporating this in the last expression for $\mathcal{M}_{\alpha,j}(X)$ gives

$$\mathcal{M}_{\alpha,j}(X) = \frac{6c_2}{\pi^2}\Omega(\alpha)X^{1/2} \sum_{\substack{\ell y \le X^\theta \\ y \le D_j X^{4\alpha}}}\sum \frac{\mu(\ell)\phi_1(\ell y)\phi_2(\ell y)\vartheta(\ell^2 y^2)}{\ell^2 y} + O(X^{1/2}(\log X)^{\lambda_{A,B}-1}).$$

Recalling definition of the arithmetic function w in (3.2.5), the sum over ℓ can be written as

$$\sum_{\ell \leq X^{\theta}/y} \frac{\mu(\ell)\phi_1(\ell y)\phi_2(\ell y)\vartheta(\ell^2 y^2)}{\ell^2} = w(y) + O_\epsilon(X^{-\theta(1-\epsilon)} y^{1-\epsilon}\vartheta(y^2)).$$

We sum the error term over y using Abel summation and Proposition 3.3 and find

$$\frac{1}{X^{\theta(1-\epsilon)}} \sum_{y \ll X^{4\alpha}} \frac{\vartheta(y^2)}{y^\epsilon} \ll X^{(4\alpha-\theta)(1-\epsilon)}$$

for any choice of ϵ small enough. Recall that θ is in the range (3.3.5) so this term is actually $O(1)$ and we are left with

$$\mathcal{M}_{\alpha,j}(X) = \frac{6c_2}{\pi^2}\Omega(\alpha)X^{1/2} \sum_{y \leq D_j X^{4\alpha}} \frac{w(y)}{y} + O(X^{1/2}(\log X)^{\lambda_{A,B}-1}).$$

Making use of Lemma 3.14 to compute the sum over y, we find

$$\sum_{y \leq D_j X^{4\alpha}} \frac{w(y)}{y} = c_3 \frac{(4\alpha)^{\lambda_{A,B}}}{\lambda_{A,B}} (\log X)^{\lambda_{A,B}} + O((\log X)^{\lambda_{A,B}-1}),$$

and hence

$$\mathcal{M}_{\alpha,j}(X) = \frac{6c_2c_3 4^{\lambda_{A,B}}}{\pi^2\lambda_{A,B}}\Omega(\alpha)\alpha^{\lambda_{A,B}}X^{1/2}(\log X)^{\lambda_{A,B}} + O_\epsilon(X^{1/2}(\log X)^{\lambda_{A,B}-1}).$$

Plugging this estimate into (3.3.6) concludes the proof of Proposition 3.16 and with it, the proof of Proposition 3.15.

3.4 Proof of Theorem 3.1

In this section, we derive the asymptotic behavior of $\mathcal{N}_\alpha(A, B; X)$ from that of $\mathcal{N}^*_\alpha(X)$. Theorem 3.1 is a consequence of the following proposition.

Proposition 3.22. *Let $\alpha \in (0, 1/120)$ and $T_2 = \#E(\mathbb{Q})[2]$. We have*

$$\mathcal{N}^*_\alpha(X) \sim 2T_2\mathcal{N}_\alpha(A, B; X),$$

as $X \to \infty$.

To prove Proposition 3.22, we begin by noting that whenever the group $E_d(\mathbb{Q})$ contains a nontorsion point P of small height, we have the inclusion

$$\{\pm P + Q : Q \in E_d(\mathbb{Q})[2]\} \subset E_d(\mathbb{Q}),$$

and all these points are nontorsion and have small height. From this observation and the fact that there is a group isomorphism $E_d(\mathbb{Q})[2] \simeq E(\mathbb{Q})[2]$ comes the inequality

$$2T_2\mathcal{N}_\alpha(A, B; X) \leq \mathcal{N}^*_\alpha(X).$$

We need to prove that the reverse inequality holds asymptotically as X grows to infinity. We let

$$\mathrm{SP}(d) = \#\left\{P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\mathrm{tors}} : \exp \hat{h}_{E_d}(P) \leq d^{1/8+\alpha}\right\},$$

so that

$$\mathcal{N}^*_\alpha(X) = \sum_{d \in \mathcal{S}(X)} \mathrm{SP}(d).$$

Applying the Cauchy–Schwarz inequality, we obtain

$$\mathcal{N}^*_\alpha(X)^2 \leq \mathcal{N}_\alpha(A, B; X) \sum_{d \in \mathcal{S}(X)} \mathrm{SP}(d)^2. \tag{3.4.1}$$

The square appearing here can be expanded as

$$\mathrm{SP}(d)^2 = \#\left\{(P_1,P_2)\in (E_d(\mathbb{Q})\setminus E_d(\mathbb{Q})_{\mathrm{tors}})^2 : \exp\hat{h}_{E_d}(P_1), \exp\hat{h}_{E_d}(P_2)\le d^{1/8+\alpha}\right\},$$

from which we extract a diagonal term corresponding to $P_2\equiv \pm P_1 \bmod E_d(\mathbb{Q})[2]$. When $\mathrm{SP}(d)\neq 0$, this becomes

$$\mathrm{SP}(d)^2 = 2T_2\mathrm{SP}(d) + \#\left\{(P_1,P_2)\in E_d(\mathbb{Q})^2 : \begin{array}{c}\exp\hat{h}_{E_d}(P_1), \exp\hat{h}_{E_d}(P_2)\le d^{1/8+\alpha}\\ P_1,P_2\notin E_d(\mathbb{Q})_{\mathrm{tors}}\\ P_1\not\equiv \pm P_2 \bmod E_d(\mathbb{Q})[2]\end{array}\right\},$$

which, when plugged into (3.4.1), gives

$$\mathcal{N}_\alpha^*(X)^2 \le \mathcal{N}_\alpha(A,B;X)\left(2T_2\mathcal{N}_\alpha^*(X)+\mathcal{Q}_\alpha(X)\right),$$

with

$$\mathcal{Q}_\alpha(X) = \sum_{d\in\mathcal{S}(X)} \#\left\{(P_1,P_2)\in E_d(\mathbb{Q})^2 : \begin{array}{c}\exp\hat{h}_{E_d}(P_1), \exp\hat{h}_{E_d}(P_2)\le d^{1/8+\alpha}\\ P_1,P_2\notin E_d(\mathbb{Q})_{\mathrm{tors}}\\ P_1\not\equiv \pm P_2 \bmod E_d(\mathbb{Q})[2]\end{array}\right\}.$$

To prove Proposition 3.22, it is now enough to show that one has

$$\mathcal{Q}_\alpha(X) = o(\mathcal{N}_\alpha^*(X)), \tag{3.4.2}$$

as $X\to\infty$.

3.4.1 Estimating $\mathcal{Q}_\alpha(X)$

To estimate $\mathcal{Q}_\alpha(X)$, we broaden the set in which the points P_1 and P_2 can be taken to only exclude the 2-torsion. This will not cause any trouble since, as we already noted in Section 3.3.1, there are only finitely many values d with $E_d(\mathbb{Q})_{\mathrm{tors}}\neq E_d(\mathbb{Q})[2]$. Calling upon the inequalities in (3.3.1) to relax the constraint on the height, we obtain

$$\mathcal{Q}_\alpha(X) \ll \sum_{d\in\mathcal{S}(X)} \#\left\{(P_1,P_2)\in E_d(\mathbb{Q})^2 : \begin{array}{c}\exp h_x(P_1),\, \exp h_x(P_2)\ll d^{1/4+2\alpha}\\ P_1,P_2\notin E_d(\mathbb{Q})[2]\\ P_1\not\equiv \pm P_2 \bmod E_d(\mathbb{Q})[2]\end{array}\right\}. \tag{3.4.3}$$

To compute an upper bound for this quantity, we express the points on E_d in terms of integer coordinates. The following lemma is a reformulation of Lemma 3.17 which turns out to be more convenient in the current situation.

Lemma 3.23. *Let $d\ge 1$ square-free and $P\in E_d(\mathbb{Q})\setminus E_d(\mathbb{Q})[2]$. There exists a unique 5-tuple $(x,y,z,t,\ell)\in\mathbb{Z}\times\mathbb{Z}_{\neq 0}\times\mathbb{Z}_{\ge 1}^3$ satisfying*

$$z^2|t, \qquad d = t\ell z^{-2}, \qquad (xy,t)=1, \qquad \ell y^2 = \tilde{F}(x,t),$$

such that $P=(xt:yz:t^2)$.

Proof. Using homogeneous coordinates, write $P=(x_0:y:z_0)$ with $(x_0,y,z_0)\in\mathbb{Z}\times\mathbb{Z}_{\neq 0}\times\mathbb{Z}_{\ge 1}$ satisfying $(x_0,y,z_0)=1$ and $dy^2z_0=\tilde{F}(x,z)$. Assume first that $y\ge 1$. By Lemma 3.17, there exist a unique $(\ell,d_1,z,x)\in\mathbb{Z}_{\ge 1}^3\times\mathbb{Z}$ with $(xy,d_1z)=1$ and $\ell y^2=\tilde{F}(x,d_1z^2)$ such that $d=\ell d_1$, $x_0=d_1xz$ and $z_0=d_1^2z^3$. Setting $t=d_1z^2$ gives $x_0=tx/z$ and $z_0=t^2/z$ so $P=(xt:yz:t^2)$. If $y\le -1$, we apply the same process to the inverse $-P=(x_0:-y:z_0)$ and find $-P=(xt:-yz:t^2)$. Taking again the inverse, we obtain the result. □

Using Lemma 3.23, we write two points $P_1,P_2\in E_d(\mathbb{Q})$ as

$$P_1=(x_1t_1:y_1z_1:t_1^2), \qquad P_2=(x_2t_2:y_2z_2:t_2^2),$$

and we express the conditions

$$\exp h_x(P_j)\ll d^{1/4+2\alpha}, \qquad P_j\notin E_d(\mathbb{Q})[2], \qquad P_1\not\equiv\pm P_2 \bmod E_d(\mathbb{Q})[2], \tag{3.4.4}$$

in terms of these coordinates. The height restriction is the same as in Section 3.3.2 and is therefore implied by the two bounds

$$x_j, t_j \ll X^{1/4+2\alpha}, \qquad y_j z_j \ll X^{4\alpha}.$$

Next, the condition $P_j \notin E_d(\mathbb{Q})[2]$ depends only on the x-coordinate of the point and we write it as $x(P_j) \notin x(E_d(\mathbb{Q})[2])$. Since P_j is a rational point and $x(E_d[2]) = x(E[2])$, this is equivalent to $(x_j : t_j) \notin x(E[2])$. Finally, we reformulate the congruence condition, which we write

$$P_2 \notin \{\pm P_1 + Q : Q \in E_d(\mathbb{Q})[2]\}.$$

As both P_1 and P_2 are rational points, projecting onto the x-coordinate gives the equivalent condition

$$x(P_2) \notin x(\{P_1 + Q : Q \in E_d[2]\}). \tag{3.4.5}$$

We give an explicit description of the set of translations of P_1 by the 2-torsions points. Denote by q_2, q_3 and q_4 the roots of the polynomial $F(x)$. One easily verifies that these satisfy the relations

$$q_2 + q_3 + q_4 = 0, \qquad A = q_2q_3 + q_2q_4 + q_3q_4, \qquad B = -q_2q_3q_4. \tag{3.4.6}$$

We set

$$Q_1 = O, \qquad Q_j = (q_j : 0 : 1),$$

so that the 2-torsion subgroup of E and its projection onto the x-coordinate are

$$E[2] = \{Q_1, Q_2, Q_3, Q_4\}, \qquad x(E[2]) = \{(1:0), (q_2:1), (q_3:1), (q_4:1)\}.$$

The addition formula (see [Sil09, III.2.3]) on E_d for $P_2 \neq \pm P_1$ and $P_1, P_2 \neq O$ reads

$$x(P_1 + P_2) = \left(d \left(\frac{y_2z_2/t_2^2 - y_1z_1/t_1^2}{x_2/t_2 - x_1/t_1} \right)^2 - \frac{x_1}{t_1} - \frac{x_2}{t_2} : 1 \right).$$

For $k \in \{2, 3, 4\}$, we compute

$$\begin{aligned} x(P_1 + Q_k) &= \left(\frac{t_1\tilde{F}(x_1, t_1)}{(y_1z_1)^2} \left(\frac{y_1z_1/t_1^2}{x_1/t_1 - q_k} \right)^2 - \frac{x_1}{t_1} - q_k : 1 \right) \\ &= \left(\frac{F(x_1, t_1)}{(x_1 - q_kt_1)^2} - (x_1 + q_kt_1) : t_1 \right). \end{aligned}$$

Expanding $F(x, t) = \prod_j (x - q_jt)$ and introducing k_1, k_2 so that $\{k, k_1, k_2\} = \{2, 3, 4\}$, this becomes

$$\begin{aligned} x(P_1 + Q_k) &= ((x_1 - q_{k_1}t_1)(x_1 - q_{k_2}t_1) - (x_1^2 - q_k^2t_1^2) : t_1(x_1 - q_kt_1)) \\ &= ((q_k^2 + q_{k_1}q_{k_2})t_1 - (q_{k_1} + q_{k_2})x_1 : x_1 - q_kt_1) \end{aligned}$$

Finally, we apply (3.4.6) and arrive at

$$x(P_1 + Q_k) = (q_kx_1 + (2q_k^2 + A)t_1 : x_1 - q_kt_1). \tag{3.4.7}$$

Let

$$\Sigma((x_1 : t_1)) = \{(x_1 : t_1)\} \sqcup \{(q_kx_1 + (2q_k^2 + A)t_1 : x_1 - q_kt_1) : 2 \leq k \leq 4\}.$$

By construction, the condition $(x_2 : t_2) \in \Sigma((x_1 : t_1))$ defines an equivalence condition, which we denote by

$$(x_1 : t_1) \sim_{E[2]} (x_2 : t_2).$$

We now have the desired reformulation, as (3.4.5) is equivalent to $(x_1 : t_1) \not\sim_{E[2]} (x_2 : t_2)$.

With the three conditions in (3.4.4) expressed in terms of the coordinates of Lemma 3.23, we are now able to write (3.4.3) as

$$\mathcal{Q}_\alpha(X) \ll \sum_{\ell \ll X} \sum_{\substack{y_1 z_1 \ll X^{4\alpha} \\ y_2 z_2 \ll X^{4\alpha}}} \sum \# \left\{ (x_1, x_2, t_1, t_2) \in \mathbb{Z}^4 : \begin{array}{c} x_1, x_2, t_1, t_2 \ll X^{1/4+2\alpha} \\ (x_1 y_1, t_1) = (x_2 y_2, t_2) = 1 \\ \ell y_1^2 = \tilde{F}(x_1, t_1) \\ \ell (y_2 z_2)^2 t_1 = z_1^2 t_2 \tilde{F}(x_2, t_2) \\ (x_1 : t_1),\ (x_2 : t_2) \notin x(E[2]) \\ (x_1 : t_1) \not\sim_{E[2]} (x_2 : t_2) \end{array} \right\}.$$

Here, just as in Section 3.3.2, we assume $y_1, y_2 \geq 1$ at the cost of a factor 2 which gets absorbed in the constant. Let

$$V_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) = \left\{ (x_1, x_2, t_1, t_2) \in \mathbb{Z}^4_{\text{prim}} : (y_2 z_2)^2 t_1 \tilde{F}(x_1, t_1) = (y_1 z_1)^2 t_2 \tilde{F}(x_2, t_2) \right\}, \tag{3.4.8}$$

where $\boldsymbol{y} = (y_1, y_2)$ and $\boldsymbol{z} = (z_1, z_2)$. Carrying out the summation over ℓ, we can now write

$$\mathcal{Q}_\alpha(X) \ll \sum_{\substack{y_1 z_1 \ll X^{4\alpha} \\ y_2 z_2 \ll X^{4\alpha}}} \sum \# \left\{ (x_1, x_2, t_1, t_2) \in V_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) : \begin{array}{c} x_1, x_2, t_1, t_2 \ll X^{1/4+2\alpha} \\ (x_1 : t_1),\ (x_2 : t_2) \notin x(E[2]) \\ (x_1 : t_1) \not\sim_{E[2]} (x_2 : t_2) \end{array} \right\}.$$

We let $L_{\boldsymbol{y},\boldsymbol{z}}$ denote the closed subset of $V_{\boldsymbol{y},\boldsymbol{z}}$ defined as the union of the lines contained in the surface, and set

$$\mathcal{Q}_\alpha^{\text{lines}}(X) = \sum_{\substack{y_1 z_1 \ll X^{4\alpha} \\ y_2 z_2 \ll X^{4\alpha}}} \sum \# \left\{ (x_1, x_2, t_1, t_2) \in L_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) : \begin{array}{c} x_1, x_2, t_1, t_2 \ll X^{1/4+2\alpha} \\ (x_1 : t_1),\ (x_2 : t_2) \notin x(E[2]) \\ (x_1 : t_1) \not\sim_{E[2]} (x_2 : t_2) \end{array} \right\}. \tag{3.4.9}$$

By a theorem of Salberger [Sal08, Theorem 0.1], the number of rational points in a box of height at most H on the surface $V_{\boldsymbol{y},\boldsymbol{z}}$ not lying on any line satisfies the bound

$$\# \left\{ (x_1, x_2, t_1, t_2) \in V_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) \setminus L_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) : x_1, x_2, t_1, t_2 \ll H \right\} \ll_\epsilon H^{13/8+\epsilon},$$

for any $\epsilon > 0$, as $H \to \infty$. Applying this, we find

$$\# \left\{ (x_1, x_2, t_1, t_2) \in V_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) \setminus L_{\boldsymbol{y},\boldsymbol{z}}(\mathbb{Q}) : x_1, x_2, t_1, t_2 \ll X^{1/4+2\alpha} \right\} \ll_\epsilon X^{13/32+13\alpha/4+\epsilon},$$

which leads to the estimate

$$\mathcal{Q}_\alpha(X) = \mathcal{Q}_\alpha^{\text{lines}}(X) + O_\epsilon(X^{13/32+45\alpha/4+\epsilon}). \tag{3.4.10}$$

3.4.2 Lines on the quartic surface

We now give an explicit description of the rational lines on the surface $V_{\boldsymbol{y},\boldsymbol{z}}$ and compute $\mathcal{Q}_\alpha^{\text{lines}}(X)$. For a variety V and a subset $S \subset V$, define

$$\text{Isom}(V; S) = \{\psi : V \to V \text{ isomorphism} : \psi(S) = S\}.$$

Let

$$n_E = \begin{cases} 2, & AB \neq 0, \\ 4, & B = 0, \\ 6, & A = 0. \end{cases}$$

The group $\text{Isom}(E; E[2])$ is easily understood. One has [Sil09, III.10.3, X.5.1]

$$\text{Isom}(E; E[2]) = \{\tau_Q \circ m_\zeta : (Q, \zeta) \in E[2] \times \boldsymbol{\mu}_{n_E}\},$$

with the maps given by

$$\tau_Q(P) = P + Q, \qquad m_\zeta(x : y : z) = (\zeta^2 x : \zeta^3 y : z).$$

Projection onto the x-coordinate induces an injective group homomorphism

$$x^* : \mathrm{Isom}(E; E[2])/\langle m_{-1}\rangle \longrightarrow \mathrm{Isom}(\mathbb{P}^1; x(E[2])). \tag{3.4.11}$$

We show that it is actually an isomorphism. To each $\sigma \in \mathrm{Isom}(\mathbb{P}^1; x(E[2]))$, we associate a matrix γ_σ through the isomorphism

$$\mathrm{Isom}(\mathbb{P}^1(\bar{\mathbb{Q}})) \simeq \mathrm{PGL}_2(\bar{\mathbb{Q}}),$$

which acts by linear transformation. Every element of $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ acts on $x(E[2])$ as a permutation of the indices $\{1, 2, 3, 4\}$, and one easily checks that the only matrix fixing $x(E[2])$ pointwise is the identity. This gives an injective group homomorphism

$$\mathrm{Isom}(\mathbb{P}^1; x(E[2])) \longrightarrow \mathfrak{S}_4,$$

and we identify $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ with its image. Let

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\}.$$

The group $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ is described in the following lemma.

Lemma 3.24. *Let $\{i, j, k\} = \{2, 3, 4\}$. One has*

$$\mathrm{Isom}(\mathbb{P}^1; x(E[2])) = \begin{cases} V_4, & AB \neq 0, \\ \langle V_4, (ij)\rangle, & B = 0 \text{ (due to } q_k = 0), \\ \langle V_4, (ijk)\rangle, & A = 0. \end{cases}$$

The corresponding matrices are

$$\gamma_{(1k)(ij)} = \begin{pmatrix} q_k & 2q_k^2 + A \\ 1 & -q_k \end{pmatrix},$$

and

$$\gamma_{(ij)} = \begin{pmatrix} \zeta_2 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \gamma_{(ijk)} = \begin{pmatrix} \zeta_3 & 0 \\ 0 & 1 \end{pmatrix},$$

where ζ_n is a primitive n-th root of unity.

Proof. We compute the matrices associated to permutations in $\mathfrak{S}_4$ and determine which correspond to elements of $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$. Write $\bar{Q}_n = x(Q_n)$ so that $\bar{Q}_1 = (1 : 0)$ and $\bar{Q}_n = (q_n : 1)$ for $n \in \{2, 3, 4\}$. For $\sigma \in \mathfrak{S}_4$, we denote the corresponding matrix by

$$\gamma_\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

and normalise the representative with $c = 1$ when $c \neq 0$ and $d = 1$ when $c = 0$. We can now identify the coefficients by looking at the action of γ_σ on $x(E[2])$. Let $\mathfrak{S}_4^{(n)}$ be the set of n-cycles in $\mathfrak{S}_4$ so that $\mathfrak{S}_4 = V_4 \sqcup \mathfrak{S}_4^{(2)} \sqcup \mathfrak{S}_4^{(3)} \sqcup \mathfrak{S}_4^{(4)}$. We look at each of these sets individually.

- V_4: Let $\sigma = (1k)(ij)$. The action of γ_σ exchanges $\bar{Q}_1$ and $\bar{Q}_k$ so one finds

  $$(a : c) = (q_k : 1), \qquad (aq_k + b : cq_k + d) = (1 : 0),$$

  and with our choice of representative, this gives $a = q_k$, $c = 1$ and $d = -q_k$. Since γ_σ also exchanges $\bar{Q}_i$ and $\bar{Q}_j$, we obtain $b = q_i q_j - q_i q_k - q_j q_k$ which, using (3.4.6), is simply $b = 2q_k^2 + A$. This determines the matrix γ_σ and thus, shows $V_4 \subseteq \mathrm{Isom}(\mathbb{P}^1; x(E[2]))$.

- $\mathfrak{S}_4^{(2)}$: We show

$$\mathfrak{S}_4^{(2)} \cap \mathrm{Isom}(\mathbb{P}^1; x(E[2])) = \begin{cases} \{(1k), (ij)\}, & B = 0 \text{ via } q_k = 0, \\ \emptyset, & B \neq 0. \end{cases}$$

It suffices to consider $\sigma = (1k)$ since $(ij) \in (1k)V_4$, so (ij) belongs to $\mathrm{Isom}(\mathbb{P}^1; x(E[2])$ exactly when $(1k)$ does. As above, we have $a = q_k$, $c = 1$ and $d = -q_k$. For γ_σ to fix both $\bar{Q}_i$ and $\bar{Q}_j$, we must have $b = q_i^2 - 2q_iq_k$ and $b = q_j^2 - 2q_jq_k$, which holds if and only if $q_k = 0$ and in that case, one has $b = q_i^2 = q_j^2 = -A$ by (3.4.6). This shows that $(1k)$, and thus also (ij), belongs to $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ if and only if $q_k = 0$, with corresponding matrix

$$\gamma_{(1k)} = \begin{pmatrix} 0 & -A \\ 1 & 0 \end{pmatrix}.$$

- $\mathfrak{S}_4^{(3)}$: We show

$$\mathfrak{S}_4^{(3)} \cap \mathrm{Isom}(\mathbb{P}^1; x(E[2])) = \begin{cases} \mathfrak{S}_4^{(3)}, & A = 0, \\ \emptyset, & A \neq 0. \end{cases}$$

It suffices to consider $\sigma = (1ij)$ since $\langle \sigma, V_4 \rangle = \mathfrak{S}_4^{(3)}$. From $\gamma_\sigma \bar{Q}_1 = \bar{Q}_i$ and $\gamma_\sigma \bar{Q}_j = \bar{Q}_1$, we find $a = q_i$ and $c = 1$ as well as $d = -q_j$. The action on $\bar{Q}_i$ and $\bar{Q}_k$ gives $b = q_iq_j - q_i^2 - q_j^2$ and $b = q_k(q_k - q_i - q_j)$ respectively. Applying (3.4.6), these become $b = 3q_iq_j - q_k^2$ and $b = 2q_k^2$, so one must have $q_k^2 = q_iq_j$ in order to have $\sigma \in \mathrm{Isom}(\mathbb{P}^1; x(E[2]))$. By (3.4.6), this implies $A = 0$. The corresponding matrix is

$$\gamma_{(1ij)} = \begin{pmatrix} q_i & 2q_iq_j \\ 1 & -q_j \end{pmatrix}.$$

To show the converse, note that $A = 0$ implies $\{q_2, q_3, q_4\} = \{\zeta_3^i B^{1/3} : i = 0, 1, 2\}$, where ζ_3 is a primitive cube root of unity. One then has $q_k^2 = q_iq_j$ and the matrix $\gamma_{(1ij)}$ above acts on $x(E[2])$ as $(1ij)$, so $(1ij)$ lies in $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$.

- $\mathfrak{S}_4^{(4)}$: We show

$$\mathfrak{S}_4^{(4)} \cap \mathrm{Isom}(\mathbb{P}^1; x(E[2])) = \begin{cases} \{(1ikj), (1jki)\}, & B = 0 \text{ via } q_k = 0, \\ \emptyset, & B \neq 0. \end{cases}$$

Let $\sigma = (1ikj)$. The action of γ_σ on $\bar{Q}_1$ and $\bar{Q}_j$ show $a = q_i$, $c = 1$ and $d = -q_j$, while the action on $\bar{Q}_i$ and $\bar{Q}_k$ give $b = q_iq_k - q_jq_k - q_i^2$ and $b = q_jq_k - q_iq_k - q_j^2$ respectively. Replacing $q_k = -(q_i + q_j)$ by (3.4.6), we find that one must have $q_j = -q_i$ in order for these two expressions to be equal. This implies $q_k = 0$ and $b = -q_i^2$. This shows that $(1ikj)$, and thus also $(1jki)$ by multiplication by elements of V_4, belong to $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ if and only if $q_k = 0$, while the other 4-cycle do not.

To summarise, we have seen that the group $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ is generated by V_4 and also either (ij) or (ijk) if $q_k = 0$ or $A = 0$ respectively. One can then compute the corresponding matrices $\gamma_{(ij)} = \gamma_{(1k)}\gamma_{(1k)(ij)}$ and $\gamma_{(ijk)} = \gamma_{(1ik)}\gamma_{(1k)(ij)}$, which are as claimed. □

Lemma 3.24 proves that the map x^* defined in (3.4.11) is a group isomorphism, as claimed. We also recover the formula (3.4.7) for the x-coordinate of the translation by a 2-torsion point. The explicit description of $\mathrm{Isom}(\mathbb{P}^1; x(E[2]))$ allows us to make use of the following result of Boissière and Sarti [BS07, proof of Proposition 4.1].

Proposition 3.25. *Let $F_1(x_1, t_1) = F_2(x_2, t_2)$ be the equation of a smooth surface V of degree d in $\mathbb{P}^3$ and for $j \in \{1, 2\}$, let $Z(F_j)$ denote the zeroes of F_j in $\mathbb{P}^1$. Let*

$$\mathrm{Isom}(\mathbb{P}^1; Z(F_1), Z(F_2)) = \{\psi : \mathbb{P}^1 \to \mathbb{P}^1 \text{ isomorphism} : \psi(Z(F_1)) = Z(F_2)\}.$$

The lines contained in the surface V are exactly

1. *the d^2 lines with given by $(x_1 : t_1) \in Z(F_1)$ and $(x_2 : t_2) \in Z(F_2)$,*

2. *the d lines given by $(x_2 : t_2) = \psi(x_1 : t_1)$ for each $\psi \in \mathrm{Isom}(\mathbb{P}^1; Z(F_1), Z(F_2))$.*

We apply Proposition 3.25 to the surface $V_{\boldsymbol{y},\boldsymbol{z}}$, which is of degree 4. With the notation of the proposition, we have

$$F_1(x,t) = (y_2z_2)^2 t\tilde{F}(x,t), \qquad F_2(x,t) = (y_1z_1)^2 t\tilde{F}(x,t),$$

and thus $Z(F_1) = Z(F_2) = x(E[2])$. Combining this with the isomorphism (3.4.11), we arrive at the following result.

Proposition 3.26. *The lines contained in the surface $V_{\boldsymbol{y},\boldsymbol{z}}$ are exactly*

1. *the 16 lines given by $(x_1 : t_1)$, $(x_2 : t_2) \in x(E[2])$,*
2. *the 4 lines given by $(x_2 : t_2) = x^*(\psi)(x_1 : t_1)$ for each $\psi \in \mathrm{Isom}(E; E[2])/\langle m_{-1}\rangle$.*

We are left with the task of determining which of these line are rational. We state this as a corollary.

Corollary 3.27. *The rational lines on $V_{\boldsymbol{y},\boldsymbol{z}}$ are of one of two possible types*

1. *the lines given by $(x_1 : t_1)$, $(x_2 : t_2) \in x(E(\mathbb{Q})[2])$,*
2. *the lines given by $(x_2 : t_2) = x^*(\tau_Q)(x_1 : t_1)$ with $Q \in E(\mathbb{Q})[2]$.*

Proof. It is clear that a line of the first kind in Proposition 3.26 is rational only if it is of the first type in the corollary. We need to show that a line of the second kind determined by $x^*(\tau_Q \circ m_\zeta)$ is rational only if $\zeta \in \{\pm 1\}$ and $Q \in E(\mathbb{Q})[2]$. Note that the condition $\zeta \in \{\pm 1\}$ is always satisfied when $AB \neq 0$.
We begin by considering $Q = Q_1$. This is the point at infinity so it belongs to $E(\mathbb{Q})[2]$. From the description of m_ζ at the beginning of Section 3.4.2, the corresponding lines are

$$(x_2 : t_2) = x^*(\tau_{Q_1} \circ m_\zeta)(x_1 : t_1) = (\zeta^2 x_1 : t_1).$$

We dehomogenize this expression to obtain

$$\begin{cases} x_2 = c(1,\zeta)\zeta^2 x_1, \\ t_2 = c(1,\zeta)t_1, \end{cases}$$

for some $c(1,\zeta) \in \bar{\mathbb{Q}}^\times$. Such a line is rational only if both $c(1,\zeta)$ and ζ^2 are rational so in particular, ζ must be a fourth root of unity. This shows that the only possibility when $A = 0$ is $\zeta \in \{\pm 1\}$. We are left with showing that no rational line arises from choosing $\zeta \in \{\pm i\}$ when $B = 0$. Plugging the expressions for x_2 and t_2 in the equation defining $V_{\boldsymbol{y},\boldsymbol{z}}$ in (3.4.8) and using $\zeta^2 = -1$, we find

$$(y_2z_2)^2 t_1\tilde{F}(x_1,t_1) = -c(1,\zeta)^4 (y_1z_1)^2 t_1\tilde{F}(-x_1,t_1).$$

When $B = 0$, we have $\tilde{F}(-x,t) = -\tilde{F}(x,t)$, so this implies

$$(y_2z_2)^2 = -c(1,\zeta)^4 (y_1z_1)^2,$$

from which we deduce $c(1,\zeta) \notin \mathbb{Q}$. This completes the proof when $Q = Q_1$.
We now turn to $Q = Q_k$ for $k \in \{2,3,4\}$. The computation in (3.4.7) shows that the four lines corresponding to $\tau_{Q_k} \circ m_\zeta$ are defined by

$$(x_2 : t_2) = (\zeta^2 q_k x_1 + (2q_k^2 + A)t_1 : \zeta^2 x_1 - q_k t_1).$$

After dehomogenising, this becomes

$$\begin{cases} x_2 = c(k,\zeta)(\zeta^2 q_k x_1 + (2q_k^2 + A)t_1), \\ t_2 = c(k,\zeta)(\zeta^2 x_1 - q_k t_1), \end{cases}$$

where $c(k,\zeta) \in \bar{\mathbb{Q}}^\times$. This defines a rational line only when $c(k,\zeta)$, ζ^2 and q_k are all rational, which only happens when $Q_k \in E(\mathbb{Q})[2]$ and $\zeta \in \boldsymbol{\mu}_4$. Just as in the case $Q = Q_1$, it remains is to show

that $\zeta \in \{\pm i\}$ does not produce any rational line when $B = 0$. Write $\pm q$ for the two nonzero roots of F, so $A = -q^2$. We again plug the expressions for x_2 and t_2 in the definition of $V_{\boldsymbol{y},\boldsymbol{z}}$. When $q_k = 0$, this gives

$$(y_2 z_2)^2 t_1 \tilde{F}(x_1, t_1) = -c(k,\zeta)^4 q^4 (y_1 z_1)^4 t_1 \tilde{F}(x_1, t_1),$$

and when $q_k \neq 0$, we find

$$(y_2 z_2)^2 t_1 \tilde{F}(x_1, t_1) = -4c(k,\zeta)^4 q_k^4 (y_1 z_1)^4 t_1 \tilde{F}(x_1, t_1).$$

In both cases, one has $c(k,\zeta) \notin \mathbb{Q}$ so no rational line arises this way. This shows the result when $Q \neq Q_1$ and thus, completes the proof. □

An immediate consequence of this corollary is that one has $\mathcal{Q}_\alpha^{\text{lines}}(X) = 0$, since the two conditions in the definition (3.4.9) are exactly the opposite of the two possibilities in Corollary 3.27. From (3.4.10), we now obtain

$$\mathcal{Q}_\alpha(X) \ll_\epsilon X^{13/32+13\alpha/4+\epsilon},$$

and since we assume $\alpha < 1/120$, the bound (3.4.2) is satisfied. This concludes the proof of Theorem 3.1.

Chapter 4

Average rank of quadratic twists with a rational point of almost minimal height

4.1 Introduction

Fix A, $B \in \mathbb{Z}$ satisfying $4A^3 + 27B^2 \neq 0$. Let E denote the elliptic curve defined over the rationals by the equation

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

and for every square-free integer d, let E_d be the quadratic twist of E defined over the rationals by the equation

$$E_d : dy^2 = x^3 + Ax + B.$$

Write $\operatorname{rank}_{\mathrm{an}} E_d(\mathbb{Q})$ for the analytic rank of E_d, that is the order of vanishing of the Hasse–Weil L-function $L(E_d, s)$ at $s = 1$, and $\operatorname{rank} E_d(\mathbb{Q})$ for the algebraic rank of E_d, which is the rank of the finitely generated abelian group $E_d(\mathbb{Q})$. Recall that the Parity Conjecture asserts that

$$\operatorname{rank}_{\mathrm{an}} E_d(\mathbb{Q}) \equiv \operatorname{rank} E_d(\mathbb{Q}) \bmod 2,$$

while the Birch and Swinnerton-Dyer Conjecture states that the two ranks are actually equal. For $X \geq 1$, denote the set of square-free integers up to X by

$$\mathcal{S}(X) = \{1 \leq d \leq X : \mu(d) \neq 0\}.$$

It has been conjectured by Goldfeld [Gol79] that the average rank of quadratic twists, when ordered by the size of d, is exactly $1/2$. More precisely, he predicted that for $\nu \in \{0, 1\}$, one has

$$\#\{d \in \mathcal{S}(X) : \operatorname{rank} E_d(\mathbb{Q}) = \nu\} \sim \frac{1}{2}\#\mathcal{S}(X). \tag{4.1.1}$$

We mention that this prediction has since been extended, following the heuristics of Katz and Sarnak [KS99], to state that amongst all elliptic curves defined over $\mathbb{Q}$, the density of rank zero curves and the density of rank one curves are both one half. This broader version of the conjecture is supported by the recent work of Bhargava and Shankar [BS15a], [BS15b], [BS13a], [BS13b].
Le Boudec [LB18] has recently investigated the analogue of Goldfeld's prediction (4.1.1) when the twists are ordered using a quantity coming from the geometry of their Mordell–Weil lattice. Recall that each twist E_d comes equipped with a canonical height function $\hat{h}_{E_d} : E_d(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ (see Section 4.2 for its definition). Following the work of Le Boudec [LB16], we consider the quantity $\eta_d(A, B)$ defined in (2.7.1). Recall that it is defined through

$$\log \eta_d(A, B) = \min\{\hat{h}_{E_d}(P) : P \in E_d(\mathbb{Q}) \setminus E_d(\mathbb{Q})_{\mathrm{tors}}\}, \tag{4.1.2}$$

if $\operatorname{rank} E_d(\mathbb{Q}) \geq 1$, and by $\eta_d(A, B) = \infty$ if $\operatorname{rank} E_d(\mathbb{Q}) = 0$. Le Boudec [LB18] showed that when the twists are ordered by the size of $\eta_d(A, B)$, then the average analytic rank is larger than one, and under the Parity Conjecture the same holds for the algebraic rank.

Remark that if $\eta_d(A,B) < \infty$, then $\operatorname{rank} E_d(\mathbb{Q}) \geq 1$ which, by the work of Kolyvagin [Kol88] and Breuil, Conrad, Diamond and Taylor [BCDT01], implies that $\operatorname{rank}_{\mathrm{an}} E_d(\mathbb{Q}) \geq 1$. Thus, given the prediction (4.1.1), one might have expected the average rank to be one.
The goal of the present work is to provide a further example of a subfamily of the family of all quadratic twists for which the average analytic rank is also greater than one. The quantity $\eta_d(A,B)$ defined in (4.1.2) satisfies the sharp lower bound (see for instance [LB16, Section 2.2])

$$\eta_d(A,B) \gg d^{1/8},$$

and we are interested in the quadratic twists for which this bound is almost attained. For $\alpha > 0$, we define the set

$$\mathcal{D}_{A,B}(\alpha; X) = \{d \in \mathcal{S}(X) : \eta_d(A,B) \leq d^{1/8+\alpha}\},$$

We note that the author [Pet20b, Theorem 1] has recently established an asymptotic formula for this quantity when $\alpha \in (0, 1/120)$. Our main result investigates the average analytic rank of the quadratic twists of E as d runs over the set $\mathcal{D}_{A,B}(\alpha; X)$.

Theorem 4.1. *Let $\alpha \in (0, 1/120)$ and assume that the polynomial $x^3 + Ax + B$ is irreducible over $\mathbb{Z}$. One has*

$$\liminf_{X\to\infty} \frac{1}{\#\mathcal{D}_{A,B}(\alpha; X)} \sum_{d\in\mathcal{D}_{A,B}(\alpha;X)} \operatorname{rank}_{\mathrm{an}} E_d(\mathbb{Q}) > 1.$$

We have decided to restrict ourselves to the case of an irreducible polynomial in order to keep the proof concise, but we expect our method to be robust enough to handle the general case.
For a prime number p, let $\mathrm{Sel}_{p^\infty}(E_d)$ be the p^∞-Selmer group of E_d. There is a short exact sequence

$$0 \longrightarrow E_d(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E_d) \longrightarrow Ш(E_d)[p^\infty] \longrightarrow 0,$$

where $Ш(E_d)$ is the Tate–Shafarevich group of E_d and $Ш(E_d)[p^\infty]$ is its p-primary part. Let $\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_d)$ be the number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in $\mathrm{Sel}_{p^\infty}(E_d)$. The above short exact sequence implies the inequality

$$\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_d) \geq \operatorname{rank} E_d(\mathbb{Q}), \tag{4.1.3}$$

while the Tate–Shafarevich Conjecture implies that these quantities are actually equal. By (4.1.3), we have $\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_d) \geq 1$ for $d \in \mathcal{D}_{A,B}(\alpha; X)$. Moreover, the p-Parity Theorem of Dokchitser and Dokchitser [DD10, Theorem 1.4] states that $\operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_d)$ and $\operatorname{rank}_{\mathrm{an}} E_d(\mathbb{Q})$ share the same parity.
During the proof of Theorem 4.1, we actually show that there exists a positive proportion of twists with analytic rank even and at least two, which implies the following corollary.

Corollary 4.2. *Under the assumptions of Theorem 4.1, one has*

$$\liminf_{X\to\infty} \frac{1}{\#\mathcal{D}_{A,B}(\alpha; X)} \sum_{d\in\mathcal{D}_{A,B}(\alpha;X)} \operatorname{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E_d) > 1.$$

In addition, we also clearly obtain the following result about the average algebraic rank.

Corollary 4.3. *Assume the Parity Conjecture. Under the assumptions of Theorem 4.1, one has*

$$\liminf_{X\to\infty} \frac{1}{\#\mathcal{D}_{A,B}(\alpha; X)} \sum_{d\in\mathcal{D}_{A,B}(\alpha;X)} \operatorname{rank} E_d(\mathbb{Q}) > 1.$$

Organisation of the chapter

The proof of Theorem 4.1 follows the strategy of Le Boudec [LB18] and is the subject of Section 4.2, where it is realised assuming the validity of Propositions 4.4 and 4.5. The purpose of Section 4.3 is to establish Proposition 4.4, using a result of Salberger [Sal08] based on the determinant method and which improves on the celebrated work of Heath-Brown [HB02]. In Section 4.4, we establish Proposition 5 by showing that a certain polynomial in three variables takes the expected amount of square-free values as its variables run over some region.

4.2 The proof of Theorem 4.1

We begin by recalling the definitions of various height functions. Let $h : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ denote the logarithmic Weil height and let $h_x : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ be defined by

$$h_x(x : y : z) = h(x : z)$$

if $(x : y : z) \neq (0 : 1 : 0)$, and $h_x(0 : 1 : 0) = 0$. The canonical height $\hat{h}_{E_d}$ on E_d is defined for $P \in E_d(\mathbb{Q})$ by

$$\hat{h}_{E_d}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{4^n} h_x(2^n P).$$

One can show (see for instance [LB16, Lemma 3]) the existence of two constants c_1 and c_2 depending only on A and B such that for every $P \in E_d(\mathbb{Q})$, one has

$$c_1 < \hat{h}_{E_d}(P) - \frac{1}{2} h_x(P) < c_2. \tag{4.2.1}$$

Write

$$F(x, z) = x^3 + Axz^2 + Bz^3, \tag{4.2.2}$$

and recall that, under the assumptions of Theorem 4.1, this polynomial is irreducible over the integers. We introduce the polynomial

$$Q(u, v, w) = vF(u, vw^2). \tag{4.2.3}$$

For $(u, v, w) \in \mathbb{Z}^3_{\geq 1}$ satisfying $Q(u, v, w) \geq 1$ and $\mu(Q(u, v, w)) \neq 0$, the point P with coordinates $(uvw : 1 : v^2w^3)$ lies in $E_{Q(u,v,w)}(\mathbb{Q})$. The square-free assumption on $Q(u, v, w)$ ensures that $\gcd(u, vw) = 1$, which implies $h_x(P) = \log \max\{u, vw^2\}$. Thus, if $\max\{u, vw^2\} \geq \mathrm{e}^{-2c_1}$, the first inequality in (4.2.1) implies $\hat{h}_{E_d}(P) \neq 0$, so P is not a torsion point. In this case, we have

$$\log \eta_d(A, B) \leq \hat{h}_{E_d}(P) < \frac{1}{2} h_x(P) + c_2,$$

which leads to

$$\eta_d(A, B) < \mathrm{e}^{c_2} \max\{u, vw^2\}^{1/2}.$$

We introduce the region

$$\mathcal{R}_Q(\alpha) = \{(u, v, w) \in \mathbb{R}^3_{\geq 1} : \mathrm{e}^{-2c_1} \leq \max\{u, vw^2\} \leq \mathrm{e}^{-2c_2} Q(u, v, w)^{1/4+2\alpha}\}, \tag{4.2.4}$$

and define the number of representations

$$r_Q(\alpha; d) = \#\{(u, v, w) \in \mathbb{Z}^3 \cap \mathcal{R}_Q(\alpha) : Q(u, v, w) = d\}.$$

By the above discussion, if d is square-free, the condition $r_Q(\alpha; d) \geq 1$ ensures $\eta_d(A, B) \leq d^{1/8+\alpha}$. In other words, the set

$$\mathcal{Q}(\alpha; X) = \{d \in \mathcal{S}(X) : r_Q(\alpha; d) \geq 1\} \tag{4.2.5}$$

is a subset of $\mathcal{D}_{A,B}(\alpha; X)$.
Let $\omega(E_d)$ denote the sign of the functional equation of $L(E_d, s)$. As mentioned in Section 4.1, the analytic rank of E_d is at least one for $d \in \mathcal{D}_{A,B}(\alpha; X)$, so that $\mathrm{rank}_{\mathrm{an}}\, E_d(\mathbb{Q})$ is at least 2 and even if and only if $\omega(E_d) = 1$. For $\nu \in \{-1, 1\}$, we define

$$\Omega_\nu(\alpha; X) = \frac{\#\{d \in \mathcal{D}_{A,B}(\alpha; X) : \omega(E_d) = \nu\}}{\#\mathcal{D}_{A,B}(\alpha; X)}.$$

To prove Theorem 4.1, we establish that for $\alpha \in (0, 1/120)$ and $\nu \in \{-1, 1\}$, one has

$$\liminf_{X\to\infty} \Omega_\nu(\alpha; X) > 0. \tag{4.2.6}$$

Letting d range over the set $\mathcal{Q}(\alpha; X)$ defined in (4.2.5) instead of $\mathcal{D}_{A,B}(\alpha; X)$ provides the lower bound

$$\Omega_\nu(\alpha; X) \geq \frac{\#\{d \in \mathcal{Q}(\alpha; X) : \omega(E_d) = \nu\}}{\#\mathcal{D}_{A,B}(\alpha; X)}. \tag{4.2.7}$$

We introduce the second moment

$$R_Q^{(2)}(\alpha; X) = \sum_{d \leq X} r_Q(\alpha; d)^2,$$

as well as the modified first moment

$$S_{Q,\nu}(\alpha; X) = \sum_{\substack{d \in \mathcal{S}(X) \\ \omega(E_d) = \nu}} r_Q(\alpha; d).$$

The Cauchy–Schwarz inequality, combined with the lower bound (4.2.7), yields

$$\Omega_\nu(\alpha; X) \geq \frac{S_{Q,\nu}(\alpha; X)^2}{\#\mathcal{D}_{A,B}(\alpha; X) R_Q^{(2)}(\alpha; X)}. \tag{4.2.8}$$

The cardinality of the set $\mathcal{D}_{A,B}(\alpha; X)$ is the subject of a recent article by the author, where it is shown [Pet20b, Theorem 1] that for $\alpha < 1/120$, there exists a positive constant $c(\alpha)$ such that one has

$$\#\mathcal{D}_{A,B}(\alpha; X) \sim c(\alpha) X^{1/2} \log X. \tag{4.2.9}$$

In Section 4.3, we establish the following upper bound for the second moment.

Proposition 4.4. *Let $\alpha \in (0, 1/120)$. One has*

$$R_Q^{(2)}(\alpha; X) \ll X^{1/2} \log X.$$

In Section 4.4, we prove the following lower bound for the modified first moment.

Proposition 4.5. *Let $\alpha \in (0, 1/56)$ and $\nu \in \{-1, 1\}$. One has*

$$S_{Q,\nu}(\alpha; X) \gg X^{1/2} \log X.$$

In both Propositions 4.4 and 4.5, as well as all throughout the remainder of this article, the implied constants can depend on α.
Putting together the inequality (4.2.8), the estimate (4.2.9) and Propositions 4.4 and 4.5, we obtain (4.2.6), which completes the proof of Theorem 4.1.

4.3 The second moment estimate

In this section, we establish Proposition 4.4. We begin with an easy preliminary lemma concerning the range of the triples in $\mathcal{R}_Q(\alpha)$.

Lemma 4.6. *Let $\alpha \in (0, 1/24)$. For $(u, v, w) \in \mathbb{Z}^3 \cap \mathcal{R}_Q(\alpha)$ satisfying $Q(u, v, w) \leq X$, one has $w \ll X^{4\alpha}$.*

Proof. From the definition of $\mathcal{R}_Q(\alpha)$ in (4.2.4), one has

$$\max\{u, vw^2\} \ll Q(u, v, w)^{1/4+2\alpha} \ll (v \max\{u, vw^2\}^3)^{1/4+2\alpha},$$

so that $\max\{u, vw^2\}^{1-24\alpha} \ll v^{1+8\alpha}$. This implies $w \ll v^{16\alpha/(1-24\alpha)}$, and it suffices to note that one has $vw^2 \ll X^{1/4+2\alpha}$ to complete the proof. □

We now turn to the computation of $R_Q^{(2)}(\alpha; X)$. Consider the diagonal term

$$m_Q(\alpha; d) = \#\left\{((u_1, v_1, w_1), (u_2, v_2, w_2)) \in \mathbb{Z}^3 \times \mathbb{Z}^3 : \begin{array}{c}(u_1, v_1, w_1), (u_2, v_2, w_2) \in \mathcal{R}_Q(\alpha)\\ Q(u_1, v_1, w_1) = Q(u_2, v_2, w_2) = d\\ (u_1 : v_1 w_1^2) = (u_2 : v_2 w_2^2)\end{array}\right\},$$

where the extra condition is an equality in $\mathbb{P}^1(\mathbb{Q})$, and let

$$a_Q(\alpha; d) = r_Q(\alpha; d)^2 - m_Q(\alpha; d). \tag{4.3.1}$$

Let

$$M_Q(\alpha; X) = \sum_{d \le X} m_Q(\alpha; d), \qquad A_Q(\alpha; X) = \sum_{d \le X} a_Q(\alpha; d). \tag{4.3.2}$$

We now provide upper bounds for these two quantities, in the form of two lemmas.

Lemma 4.7. *Let $\alpha \in (0, 1/24)$. One has*

$$M_Q(\alpha; X) \ll X^{1/2} \log X.$$

Proof. For a fixed value of $d \ge 1$, let $((u_1, v_1, w_1), (u_2, v_2, w_2))$ be a pair counted in $m_Q(\alpha; d)$. Write $u = \gcd(u_1, u_2)$, $u_1 = ux$ and $u_2 = uy$, where x and y are coprime positive integers. The projective condition defining $m_Q(\alpha; d)$ dehomogenises to

$$xu_2 = yu_1, \qquad xv_2 w_2^2 = yv_1 w_1^2.$$

From these expressions, we obtain

$$Q(u_2, v_2, w_2) = \frac{y^4 w_1^2}{x^4 w_2^2} Q(u_1, v_1, w_1),$$

and since $Q(u_1, v_1, w_1) = d \ge 1$, the equation $Q(u_1, v_1, w_1) = Q(u_2, v_2, w_2)$ appearing in the definition of $m_Q(\alpha; d)$ becomes $w_2 x^2 = w_1 y^2$. Together with the second dehomogenised relation, this shows $v_1 x^3 = v_2 y^3$. From the coprimality of x and y, it follows that x^2 divides w_1 and that x^3 divides v_2. Writing $w_1 = wx^2$ and $v_2 = vx^3$ for some positive integers v and w, we obtain $w_2 = wy^2$ and $v_1 = vy^3$ and therefore, we have

$$((u_1, v_1, w_1), (u_2, v_2, w_2)) = ((ux, vy^3, wx^2), (uy, vx^3, wy^2)),$$

for some unique 5-tuple (u, v, w, x, y) of positive integers. This brings about the new expression

$$m_Q(\alpha; d) = \#\left\{(u, v, w, x, y) \in \mathbb{Z}_{\ge 1}^5 : \begin{array}{c}(ux, vy^3, wx^2), (uy, vx^3, wy^2) \in \mathcal{R}_Q(\alpha)\\ Q(ux, vy^3, wx^2) = d\end{array}\right\},$$

and Lemma 4.6 implies $wx^2, wy^2 \ll X^{4\alpha}$. Summing over d, we reach the upper bound

$$M_Q(\alpha; X) \ll \sum_{wx^2, wy^2 \ll X^{4\alpha}} \sum\sum \#\left\{(u, v) \in \mathbb{Z}_{\ge 1}^2 : \begin{array}{l}1 \le Q(ux, vy^3, wx^2) \le X\\ ux, uy, vw^2x^3y^4, vw^2x^4y^3 \ll X^{1/4+2\alpha}\end{array}\right\}. \tag{4.3.3}$$

An elementary application of the classical lattice-point counting method of Davenport [Dav51] shows

$$\#\left\{(u, v) \in \mathbb{Z}_{\ge 1}^2 : \begin{array}{l}1 \le Q(ux, vy^3, wx^2) \le X\\ ux, uy, vx^3, vy^3 \ll X^{1/4+2\alpha}\end{array}\right\} \ll \iint_{0 < Q(ux, vy^3, wx^2) \le X} \mathrm{d}u\, \mathrm{d}v + \frac{X^{1/4+2\alpha}}{\min\{x, y\}}.$$

The change of variables $(u, v) \mapsto (uvX^{1/4} w^{1/2} (xy)^3, vX^{1/4} w^{-3/2})$ yields

$$\iint_{0 < Q(ux, vy^3, wx^2) \le X} \mathrm{d}u\, \mathrm{d}v = \frac{X^{1/2}(xy)^3}{w} \iint_{0 < (xy)^{12} v^4 F(u, 1) \le 1} v\, \mathrm{d}u\, \mathrm{d}v.$$

The integral over v has size $F(u,1)^{-1/2}(xy)^{-6}$ and, since $F(u,1)$ has three distinct roots, integrating over u gives a constant. Summing over x, y and w in (4.3.3), we obtain

$$\begin{aligned} M_Q(\alpha;X) &\ll \sum\sum\sum_{wx^2,wy^2\ll X^{4\alpha}} \left\{ \frac{X^{1/2}}{w(xy)^3} + \frac{X^{1/4+2\alpha}}{\min\{x,y\}} \right\} \\ &\ll X^{1/2}\log X + X^{1/4+6\alpha}\log X, \end{aligned}$$

which concludes the proof since $\alpha < 1/24$. □

Lemma 4.8. *Let $\alpha \in (0, 1/120)$. One has*

$$A_Q(\alpha;X) \ll X^{1/2}.$$

Proof. Using Lemma 4.6 and carrying out the summation over d, we find in particular that

$$A_Q(\alpha;X) \ll \sum\sum_{w_1,w_2\ll X^{4\alpha}} \#\left\{ (u_1,u_2,v_1,v_2)\in\mathbb{Z}^4 : \begin{array}{c} 1\le u_1,u_2,v_1,v_2 \ll X^{1/4+2\alpha} \\ Q(u_1,v_1,w_1)=Q(u_2,v_2,w_2) \\ (u_1:v_1w_1^2)\neq(u_2:v_2w_2^2) \end{array} \right\}.$$

For fixed w_1 and w_2, write $\mathbf{w}=(w_1,w_2)$ and let $V_{\mathbf{w}}$ be the projective surface in $\mathbb{P}^3$ defined by the equation

$$Q(u_1,v_1,w_1) = Q(u_2,v_2,w_2).$$

Let H denote the usual exponential Weil height on $\mathbb{P}^3(\mathbb{Q})$ and set

$$a_{Q,\mathbf{w}}(k;\alpha;X) = \#\left\{ (u_3:u_4:v_3:v_4)\in V_{\mathbf{w}}(\mathbb{Q}) : \begin{array}{c} H(u_3:u_4:v_3:v_4)\ll X^{1/4+2\alpha}/k \\ (u_3:v_3w_1^2)\neq(u_4:v_4w_2^2) \end{array} \right\}.$$

Summing over $k=\gcd(u_1,u_2,v_1,v_2)$, we find

$$A_Q(\alpha;X) \ll \sum\sum_{w_1,w_2\ll X^{4\alpha}} \sum_{k\ll X^{1/4+2\alpha}} a_{Q,\mathbf{w}}(k;\alpha;X).$$

Let $L_{\mathbf{w}}$ denote the Zariski closed subset of $V_{\mathbf{w}}$ defined as the union of the lines contained in $V_{\mathbf{w}}$. Since the polynomial $F(x,z)$ is assumed to be irreducible, meaning that the curve E and all its twists E_d have trivial 2-torsion, a recent result by the author [Pet20b, Corollary 4.6] states that if a point $(u_3:u_4:v_3:v_4)\in V_{\mathbf{w}}(\mathbb{Q})$ lies in $L_{\mathbf{w}}(\mathbb{Q})$, then $(u_3:v_3w_1^2)=(u_4:v_4w_2^2)$ in $\mathbb{P}^1(\mathbb{Q})$. Such points are excluded here and a result of Salberger [Sal08, Theorem 0.1] therefore shows that for any $\epsilon>0$, we have

$$a_{Q,\mathbf{w}}(k;\alpha;X) \ll_\epsilon \left(\frac{X^{1/4+2\alpha}}{k}\right)^{13/8+\epsilon}.$$

It follows that

$$A_Q(\alpha;X) \ll_\epsilon X^{13/32+45\alpha/4+\epsilon},$$

and the assumption $\alpha<1/120$ concludes the proof. □

We finally note that combining the equality (4.3.1) with the definitions in (4.3.2) and with Lemmas 4.7 and 4.8, we immediately complete the proof of Proposition 4.4.

4.4 The square-free sieve

This section is dedicated to establishing Proposition 4.5. Let N_E denote the conductor of E. For $a\in(\mathbb{Z}/4N_E\mathbb{Z})^\times$, we define

$$S_Q(a;\alpha;X) = \sum_{\substack{d\in\mathcal{S}(X)\\ d\equiv a \bmod 4N_E}} r_Q(\alpha;d).$$

We will show the following lower bound.

Proposition 4.9. *Let $\alpha \in (0, 1/56)$ and $a \in (\mathbb{Z}/4N_E\mathbb{Z})^\times$. One has*

$$S_Q(a; \alpha; X) \gg X^{1/2} \log X.$$

For $d \geq 1$ and square-free, let D be the discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$ and let χ_d be the associated quadratic character. When $\gcd(D, N_E) = 1$, the sign of the functional equation of $L(E_d, s)$ is determined by (see for instance [Sil01, Section 4.3])

$$\omega(E_d) = \chi_d(-N_E)\omega(E).$$

Because of this, there exists $a \in (\mathbb{Z}/4N_E\mathbb{Z})^\times$ such that

$$S_{Q,\nu}(\alpha; X) \geq S_Q(a; \alpha; X),$$

and thus, Proposition 4.5 is an immediate consequence of Proposition 4.9. The remainder of Section 4.4 is dedicated to the proof of Proposition 4.9.
We point out that a square-free sieve argument has already been employed by Gouvêa and Mazur [GM91], and at the same time but independently by Greaves [Gre92], to show that integral binary forms, under certain assumptions, represent the expected number of square-free integers. This is similar to the statement of Proposition 4.9, the difference being that in our case the variables range over the region defined in (4.2.4) instead of over a box as they do in both aforementioned articles. For this reason, the sieving process must be carried out in full here.

4.4.1 Preliminary results

This section presents several results required later on. Recall the definition (4.2.2) of the binary cubic form $F(x, z)$ and let $\Delta_F = -(4A^3 + 27B^2)$ denote the discriminant of the polynomial $F(x, 1)$. Define the arithmetic function

$$\rho(n) = \#\{u \bmod n : F(u, 1) \equiv 0 \bmod n\}. \tag{4.4.1}$$

This function is multiplicative and satisfies the upper bound [Ste91, Corollary 2]

$$\rho(p^k) \leq 2p^{v_p(\Delta_F)/2} + 1, \tag{4.4.2}$$

for any prime p and any $k \geq 1$. Moreover, it follows from Hensel's lemma that for $p \nmid \Delta_F$ and $k \geq 1$, one has

$$\rho(p^k) = \rho(p). \tag{4.4.3}$$

Together, (4.4.2) and (4.4.3) imply $\rho(n^k) \ll_k \rho(n)$. By way of an estimate for the summatory function of $\rho(n)$ (e.g. [Fom98, Equation 4]), this demonstrates the upper bound

$$\sum_{n \leq X} \rho(n^k) \ll X. \tag{4.4.4}$$

Finally, we give an elementary lemma about a sum of a certain arithmetic function involving $\varphi^*(n) = \varphi(n)/n$.

Lemma 4.10. *Let $a, q, m \in \mathbb{Z}_{\geq 1}$ with $\gcd(a, q) = 1$. One has*

$$\sum_{\substack{n \leq X \\ \gcd(n,m)=1 \\ n \equiv a \bmod q}} \mu(n)^2 \varphi^*(n) = \frac{C_0(q)C_1(m; q)}{q} X + O(X^{1/2}),$$

with

$$C_0(q) = \prod_{p \nmid q} \left(1 - \frac{2}{p^2} + \frac{1}{p^3}\right), \qquad C_1(m; q) = \prod_{\substack{p \mid m \\ p \nmid q}} \left(1 + \frac{1}{p} - \frac{1}{p^2}\right)^{-1}.$$

Proof. Write

$$f(n) = \begin{cases} \mu(n)^2\varphi^*(n), & \text{if } \gcd(n,m)=1, \\ 0, & \text{otherwise,} \end{cases}$$

and denote the quantity of interest by

$$A(X) = \sum_{\substack{n\leq X \\ n\equiv a \bmod q}} f(n).$$

This sum can be expressed as

$$\begin{aligned} A(X) &= \sum_{\substack{n\leq X \\ n\equiv a \bmod q}} \sum_{d\mid n} (f*\mu)(d) \\ &= \frac{X}{q} \sum_{\substack{d\geq 1 \\ \gcd(d,q)=1}} \frac{(f*\mu)(d)}{d} + O\left(\sum_{d\leq X} |(f*\mu)(d)|\right) + O\left(\frac{X}{q}\sum_{d>X}\frac{|(f*\mu)(d)|}{d}\right). \end{aligned}$$

Remark that for $k \geq 1$, one has

$$(f*\mu)(p^k) = \begin{cases} 0, & p\nmid m \text{ and } k\geq 3 \text{ or } p\mid m \text{ and } k\geq 2, \\ -1/p, & p\nmid m \text{ and } k=1, \\ -(1-1/p), & p\nmid m \text{ and } k=2, \\ -1, & p\mid m \text{ and } k=1, \end{cases}$$

so the main term is as claimed. Remark that the computation of $(f*\mu)(p^k)$ shows, by multiplicativity, that one has

$$|(f*\mu)(d)| \leq |(f*\mu)(d')|,$$

for all $d \geq 1$, where

$$d' = \prod_{p\nmid m} p^{v_p(d)}.$$

One can therefore assume $m = 1$ when estimating the error terms, which we now do.
Let $d \geq 1$ cube-free and write $d = d_1 d_2^2$ with d_1 and d_2 square-free and coprime. One has

$$|(f*\mu)(d_1)| = 1/d_1, \qquad |(f*\mu)(d_2^2)| \leq 1,$$

and so, the sums appearing in the error terms are bounded as

$$\sum_{d\leq X} |(f*\mu)(d)| \leq \sum_{d_1 d_2^2 \leq X} \sum \frac{1}{d_1} \ll X^{1/2},$$

and

$$\sum_{d>X} \frac{|(f*\mu)(d)|}{d} \leq \sum_{d_1 d_2^2 > X} \sum \frac{1}{d_1^2 d_2^2} \ll X^{-1/2}.$$

This concludes the proof. □

4.4.2 Setup for the square-free sieve

In order to prove Proposition 4.9, it is enough to show that the estimate holds for the quantity

$$N(\alpha; X) = \#\left\{(u,v,w)\in\mathbb{Z}^3\cap\mathcal{R}_Q(\alpha) : \begin{matrix} Q(u,v,w)\in\mathcal{S}(X) \\ (u,v,w)\equiv(u_0,v_0,w_0) \bmod 4N_E \end{matrix}\right\},$$

where u_0, v_0 and w_0 are residues classes modulo $4N_E$ for which $Q(u_0,v_0,w_0)$ is invertible.

We start by reducing the region $\mathcal{R}_Q(\alpha)$ defined in (4.2.4). Impose $u \geq c_3 vw^2$ for some $c_3 \geq 1$, so the maximum in the definition of $\mathcal{R}_Q(\alpha)$ is simply u, and let $c_4 = 1 + |A| + |B|$. For c_3 large enough, one has

$$\frac{1}{2}u^3 \leq F(u, vw^2) \leq c_4 u^3.$$

These bounds allow us to strengthen the conditions $Q(u,v,w) \leq X$ and $u \leq \mathrm{e}^{-2c_2} Q(u,v,w)^{1/4+2\alpha}$ to $c_4 u^3 v \leq X$ and $u \leq c_5 (u^3 v)^{1/4+2\alpha}$ respectively, where $c_5 = \mathrm{e}^{-2c_2} 2^{-(1/4+2\alpha)}$. This results in the inequality

$$N(\alpha; X) \geq \# \left\{ (u,v,w) \in \mathbb{Z}^3_{\geq 1} : \begin{array}{c} c_3 vw^2 \leq u,\ c_4 u^3 v \leq X \\ u \leq c_5 (u^3 v)^{1/4+2\alpha} \\ \mu(Q(u,v,w)) \neq 0 \\ (u,v,w) \equiv (u_0, v_0, w_0) \bmod 4N_E \end{array} \right\}.$$

Proceeding as in the proof of Lemma 4.6, we extract the additional condition $w \leq c_6 X^{4\alpha}$ from the right-hand side, with $c_6 = c_3^{-(1/2+12\alpha)} c_4^{-4\alpha} c_5^{2/(1-24\alpha)}$. Using the simple estimate

$$\# \left\{ (u,v,w) \in \mathbb{Z}^3_{\geq 1} : \begin{array}{c} vw^2 \ll u^3 v \leq X,\ w \ll X^{4\alpha} \\ u > c_5 (u^3 v)^{1/4+2\alpha} \end{array} \right\} \ll X^{1/2},$$

we deduce the lower bound

$$N(\alpha; X) \geq \sum_{\substack{w \leq c_6 X^{4\alpha} \\ w \equiv w_0 \bmod 4N_E}} \# \left\{ (u,v) \in \mathbb{Z}^2_{\geq 1} : \begin{array}{c} c_3 vw^2 \leq u,\ c_4 u^3 v \leq X \\ \mu(Q(u,v,w)) \neq 0 \\ (u,v) \equiv (u_0, v_0) \bmod 4N_E \end{array} \right\} + O(X^{1/2}).$$

Next, we reduce the range of u and v. Let

$$U_w = \left(\frac{c_3 X w^2}{c_4} \right)^{1/4}. \tag{4.4.5}$$

Restricting our attention to $u \leq U_w$, the condition $c_4 u^3 v \leq X$ becomes redundant and we are left with lattice points (u,v) lying in a triangle with vertices $(1,1)$, $(U_w, 1)$ and $(U_w, U_w/c_3 w^2)$. For $w \equiv w_0 \bmod 4N_E$, we define

$$N_w(X) = \# \left\{ (u,v) \in \mathbb{Z}^2_{\geq 1} : \begin{array}{c} c_3 vw^2 \leq u \leq U_w \\ \mu(Q(u,v,w)) \neq 0 \\ (u,v) \equiv (u_0, v_0) \bmod 4N_E \end{array} \right\}, \tag{4.4.6}$$

and we then obtain the lower bound

$$N(\alpha; X) \geq \sum_{\substack{w \leq c_6 X^{4\alpha} \\ w \equiv w_0 \bmod 4N_E}} N_w(X) + O(X^{1/2}). \tag{4.4.7}$$

From the definition of Q in (4.2.3), it ensues that the condition $\mu(Q(u,v,w)) \neq 0$ appearing in (4.4.6) can be reformulated as

$$\mu(v)\mu(F(u, vw^2)) \neq 0, \qquad \gcd(u, vw) = 1.$$

We remove the square-free condition on $F(u, vw^2)$ by summing over the integers $\ell \geq 1$ whose square divides $F(u, vw^2)$. The inequalities $vw^2 \leq c_3 vw^2 \leq u \leq U_w$ imply $F(u, vw^2) \leq c_4 U_w^3$, which restricts the range of ℓ to $\ell^2 \leq c_4 U_w^3$. Let

$$N_{w,\ell}(X) = \# \left\{ (u,v) \in \mathbb{Z}^2_{\geq 1} : \begin{array}{c} c_3 vw^2 \leq u \leq U_w \\ \mu(v) \neq 0,\ \gcd(u, vw) = 1 \\ F(u, vw^2) \equiv 0 \bmod \ell^2 \\ (u,v) \equiv (u_0, v_0) \bmod 4N_E \end{array} \right\}. \tag{4.4.8}$$

We show that $N_{w,\ell}(X) = 0$ whenever $\gcd(\ell, 4N_E w) > 1$. It is immediate that any common factor of ℓ and w divides u and therefore has to be equal to one. The congruence conditions in (4.4.8) imply

$$F(u, vw^2) \equiv 0 \bmod \gcd(\ell, 4N_E), \qquad (u,v) \equiv (u_0, v_0) \bmod \gcd(\ell, 4N_E),$$

and since we also have $w \equiv w_0 \bmod \gcd(\ell, 4N_E)$, we obtain $F(u_0, v_0 w_0^2) \equiv 0 \bmod \gcd(\ell, 4N_E)$. This leads to a contradiction unless $\gcd(\ell, 4N_E) = 1$, as u_0, v_0 and w_0 are chosen, at the beginning of Section 4.4.2, so that $Q(u_0, v_0, w_0) = v_0 F(u_0, v_0 w_0^2)$ is invertible modulo $4N_E$.
Taking these restrictions into account, an application of the inclusion-exclusion principle now yields

$$N_w(X) \geq \sum_{\substack{\ell^2 \leq c_4 U_w^3 \\ \gcd(\ell, 4N_E w)=1}} \mu(\ell) N_{w,\ell}(X). \tag{4.4.9}$$

We also note that all v counted in (4.4.8) are coprime to ℓ so summing over residue classes, it becomes

$$N_{w,\ell}(X) = \sum_{\substack{a,b \bmod \ell^2 \\ F(a,bw^2)\equiv 0 \bmod \ell^2 \\ \gcd(b,\ell)=1}} \sum \# \left\{ (u,v) \in \mathbb{Z}^2_{\geq 1} : \begin{array}{c} c_3 v w^2 \leq u \leq U_w \\ \mu(v) \neq 0,\ \gcd(u, vw) = 1 \\ (u,v) \equiv (a,b) \bmod \ell^2 \\ (u,v) \equiv (u_0, v_0) \bmod 4N_E \end{array} \right\}.$$

Shifting a by a factor bw^2 simplifies the congruence condition and we arrive at

$$N_{w,\ell}(X) = \sum_{\substack{a \bmod \ell^2 \\ F(a,1)\equiv 0 \bmod \ell^2}} \# \left\{ (u,v) \in \mathbb{Z}^2_{\geq 1} : \begin{array}{c} c_3 v w^2 \leq u \leq U_w \\ \mu(v) \neq 0,\ \gcd(u, vw) = 1 \\ u \equiv a v w^2 \bmod \ell^2 \\ (u,v) \equiv (u_0, v_0) \bmod 4N_E \end{array} \right\}. \tag{4.4.10}$$

4.4.3 Reducing the range of ℓ

In this section, we show that the range of ℓ in (4.4.9) can be reduced at a negligible cost. Recall the definition of $\rho(n)$ in (4.4.1). We begin with a simple upper bound on the size of $N_{w,\ell}(X)$.

Lemma 4.11. *One has*

$$N_{w,\ell}(X) \ll \left(\frac{X^{1/2}}{w\ell^2} + 1 \right) \rho(\ell^2).$$

Proof. Abandoning some of the conditions in (4.4.10) and extending the range of u and v yields

$$N_{w,\ell}(X) \ll \sum_{\substack{a \bmod \ell^2 \\ F(a,1)\equiv 0 \bmod \ell^2}} \# \left\{ (u,v) \in \mathbb{Z}^2 : \begin{array}{c} 1 \leq u, c_3 v w^2 \leq U_w \\ \gcd(u,v) = 1 \\ u \equiv a v w^2 \bmod \ell^2 \end{array} \right\}.$$

A result of Heath-Brown [HB84, Lemma 3] shows the estimate

$$\# \left\{ (u,v) \in \mathbb{Z}^2 : \begin{array}{c} 1 \leq u, c_3 v w^2 \leq U_w \\ \gcd(u,v) = 1 \\ u \equiv a v w^2 \bmod \ell^2 \end{array} \right\} \ll \frac{U_w^2}{w^2 \ell^2} + 1,$$

which, combined with the definition of U_w in (4.4.5), concludes the proof. □

An immediate consequence is the following result.

Lemma 4.12. *Let $\theta > 0$. One has*

$$\sum_{X^\theta < \ell \ll U_w^{3/2}} \mu(\ell) N_{w,\ell}(X) \ll \frac{X^{1/2-\theta}}{w} + X^{3/8} w^{3/4}.$$

Proof. Applying Lemma 4.11, we find

$$\sum_{X^\theta < \ell \ll U_w^{3/2}} \mu(\ell) N_{w,\ell}(X) \ll \frac{X^{1/2}}{w} \sum_{\ell > X^\theta} \frac{\rho(\ell^2)}{\ell^2} + \sum_{\ell \leq U_w^{3/2}} \rho(\ell^2).$$

Using (4.4.4) and, for the first sum, Abel summation, we obtain

$$\sum_{\ell > X^\theta} \frac{\rho(\ell^2)}{\ell^2} \ll \frac{1}{X^\theta}, \qquad \sum_{\ell \ll U_w^{3/2}} \rho(\ell^2) \ll X^{3/8} w^{3/4},$$

which completes the proof. □

Going back to (4.4.9), Lemma 4.12 shows that for any $\theta > 0$, we have

$$N_w(X) \geq \sum_{\substack{\ell < X^\theta \\ \gcd(\ell, 4N_E w)=1}} \mu(\ell) N_{w,\ell}(X) + O\left(\frac{X^{1/2-\theta}}{w}\right) + O(X^{3/8} w^{3/4}). \tag{4.4.11}$$

4.4.4 Estimating $N_{w,\ell}(X)$

This section is dedicated to establishing a precise estimate for the quantity $N_{w,\ell}(X)$ defined in (4.4.8) when $\gcd(\ell, 4N_E w) = 1$. Removing the coprimality condition on u in (4.4.10), we find

$$N_{w,\ell}(X) = \sum_{\substack{a \bmod \ell^2 \\ F(a,1) \equiv 0 \bmod \ell^2}} \sum_{\substack{c_3 v w^2 \leq U_w \\ \gcd(v,\ell)=1 \\ v \equiv v_0 \bmod 4N_E}} \mu(v)^2 \sum_{f \mid vw} \mu(f) \# \left\{ u_1 \in \mathbb{Z}_{\geq 1} : \begin{array}{r} c_3 v w^2 \leq f u_1 \leq U_w \\ f u_1 \equiv a v w^2 \bmod \ell^2 \\ f u_1 \equiv u_0 \bmod 4N_E \end{array} \right\}.$$

As ℓ and $4N_E$ are coprime, the two congruence conditions here reduce to a single condition on $fu_1 \bmod 4N_E\ell^2$. Moreover, vw is coprime to ℓ so the same holds for f, and we show that f is also coprime to $4N_E$. Note that it is enough to prove that $f_0 = \gcd(f, w)$ is coprime to $4N_E$ because $v_0 \bmod 4N_E$ is invertible so we already know that $\gcd(v, 4N_E) = 1$. Writing $f = f_0 f_1$, $w = f_0 w_1$ and combining

$$f u_1 \equiv u_0 \bmod 4N_E, \qquad w \equiv w_0 \bmod 4N_E,$$

with the definition (4.2.3) of Q, we obtain

$$\begin{aligned} Q(u_0, v_0, w_0) &\equiv v_0 F(f_0 f_1 u_1, v_0 f_0^2 w_1^2) \bmod 4N_E \\ &\equiv f_0^3 v_0 F(f_1 u_1, v_0 f_0 w_1^2) \bmod 4N_E. \end{aligned}$$

Here again, we use the fact that $Q(u_0, v_0, w_0)$ is invertible modulo $4N_E$ as per our choice of u_0, v_0 and w_0 at the start of Section 4.4.2. It follows that $\gcd(f_0, 4N_E) = 1$, as claimed.
The previous paragraph implies the estimate

$$\# \left\{ u_1 \in \mathbb{Z}_{\geq 1} : \begin{array}{r} c_3 v w^2 \leq f u_1 \leq U_w \\ f u_1 \equiv a v w^2 \bmod \ell^2 \\ f u_1 \equiv u_0 \bmod 4N_E \end{array} \right\} = \frac{U_w - c_3 v w^2}{4N_E \ell^2 f} + O(1),$$

and, recalling the definition of $\rho(n)$ in (4.4.1), we arrive at

$$N_{w,\ell}(X) = \rho(\ell^2) \sum_{\substack{c_3 v w^2 \leq U_w \\ \gcd(v,\ell)=1 \\ v \equiv v_0 \bmod 4N_E}} \mu(v)^2 \sum_{f \mid vw} \mu(f) \left\{ \frac{U_w - c_3 v w^2}{4N_E \ell^2 f} + O(1) \right\}.$$

We now define

$$V_{w,\ell}(X) = \sum_{\substack{c_3 v w^2 \leq U_w \\ \gcd(v,\ell)=1 \\ v \equiv v_0 \bmod 4N_E}} \mu(v)^2 \varphi^*(vw)(U_w - c_3 v w^2), \tag{4.4.12}$$

and obtain

$$N_{w,\ell}(X) = \frac{\rho(\ell^2)}{4N_E \ell^2} V_{w,\ell}(X) + O_\epsilon\left(\frac{X^{1/4+\epsilon}}{w^{3/2}}\right), \tag{4.4.13}$$

when $\gcd(\ell, 4N_E w) = 1$, and zero otherwise. Here we have used the estimates $\rho(\ell^2) \ll_\epsilon \ell^\epsilon \ll X^\epsilon$ and $\varphi^*(vw) \ll_\epsilon (vw)^\epsilon \ll X^\epsilon$ to simplify the error term, and replaced U_w by its definition (4.4.5). Define the two arithmetic functions

$$f_1(n) = \prod_{p|n}{}' \left(1 + \frac{1}{p} - \frac{1}{p^2}\right)^{-1}, \qquad f_2(n) = \varphi^*(w) \prod_{p|n}{}' \left(1 - \frac{p}{p^2 + 2p - 1}\right)^{-1}, \tag{4.4.14}$$

where the prime indicates that the product is restricted to $p \nmid 4N_E$. We compute $V_{w,\ell}(X)$ in the following lemma.

Lemma 4.13. *Assume* $\gcd(\ell, 4N_E w) = 1$. *There exists a constant* $c_7 > 0$ *such that one has*

$$V_{w,\ell}(X) = \frac{c_7 f_2(w) f_1(\ell)}{w} X^{1/2} + O_\epsilon\left(\frac{X^{3/8}}{w^{1/4-\epsilon}}\right).$$

Proof. Taking $g = \gcd(v, w)$ out and writing $v = gv_1$, (4.4.12) becomes

$$V_{w,\ell}(X) = \sum_{g|w} \sum_{\substack{c_3 g v_1 w^2 \leq U_w \\ \gcd(gv_1, \ell) = 1 \\ gv_1 \equiv v_0 \bmod 4N_E}} \mu(gv_1)^2 \varphi^*(gv_1 w)(U_w - c_3 g v_1 w^2).$$

Note that g and v_1 are necessarily coprime here. Recall from the beginning of Section 4.4.2 and from the definition of Q in (4.2.3) that v_0 is invertible modulo $4N_E$, so the sum over v_1 is zero unless $\gcd(g, 4N_E) = 1$. Noting that $\varphi^*(gw) = \varphi^*(w)$ as g divides w, we reach the new expression

$$V_{w,\ell}(X) = \varphi^*(w) \sum_{g|w}{}' \mu(g)^2 \sum_{\substack{c_3 g v_1 w^2 \leq U_w \\ \gcd(v_1, g\ell) = 1 \\ v_1 \equiv v_0 \bar{g} \bmod 4N_E}} \mu(v_1)^2 \varphi^*(v_1)(U_w - c_3 g v_1 w^2).$$

Here, the prime indicates that the sum is restricted to values of g coprime to $4N_E$, and $\bar{g}$ is the inverse of g modulo $4N_E$. Applying Lemma 4.10, we find that the sum over v_1 is

$$\frac{C_0(4N_E) C_1(g\ell; 4N_E)}{8N_E c_3 g w^2} U_w^2 + O\left(\frac{U_w^{3/2}}{g^{1/2} w}\right),$$

with C_0 and C_1 as in Lemma 4.10. Let

$$c_7 = \frac{C_0(4N_E)}{8N_E (c_3 c_4)^{1/2}} > 0,$$

and remark that the arithmetic function f_1 is chosen to have $C_1(n; 4N_E) = f_1(n)$. Replacing U_w by its expression (4.4.5), the value of the sum over v_1 becomes

$$\frac{c_7 f_1(g\ell)}{gw} X^{1/2} + O\left(\frac{X^{3/8}}{g^{1/2} w^{1/4}}\right).$$

Recall that ℓ and w are coprime and that g divides w so by multiplicativity, $f_1(g\ell) = f_1(g) f_1(\ell)$. Summing over g, we arrive at

$$V_{w,\ell}(X) = \frac{c_7 \varphi^*(w) f_1(\ell)}{w} X^{1/2} \sum_{g|w}{}' \frac{\mu(g)^2 f_1(g)}{g} + O_\epsilon\left(\frac{X^{3/8}}{w^{1/4-\epsilon}}\right).$$

The sum over g satisfies

$$\sum_{g|w}{}' \frac{\mu(g)^2 f_1(g)}{g} = \prod_{p|w}{}' \left(1 + \frac{f_1(p)}{p}\right) = \prod_{p|w}{}' \left(1 + \frac{p}{p^2 + p - 1}\right) = \frac{f_2(w)}{\varphi^*(w)},$$

which completes the proof. □

Write $c_8 = c_7/4N_E$. When $\gcd(\ell, 4N_E w) = 1$, the equation (4.4.13) and Lemma 4.13 merge into

$$N_{w,\ell}(X) = \frac{c_8 f_2(w)\rho(\ell^2)f_1(\ell)}{w\ell^2}X^{1/2} + O(X^{3/8}). \tag{4.4.15}$$

Here, the error term slightly worse than the one actually provided by the lemma. This is only to improve readability and has no consequence whatsoever, as the limitation on the range of α will be determined by a different error term.

4.4.5 Estimating $N(\alpha; X)$

We now have all the necessary estimates to compute a lower bound for $N_w(X)$, and thus also for $N(\alpha; X)$ using (4.4.7). Combining (4.4.11) and (4.4.15) gives, for any $\theta > 0$, the inequality

(4.4.16)
$$N_w(X) \geq \frac{c_8 f_2(w)}{w}X^{1/2} \sideset{}{'}\sum_{\substack{\ell < X^\theta \\ \gcd(\ell,w)=1}} \frac{\mu(\ell)\rho(\ell^2)f_1(\ell)}{\ell^2} + O\left(\frac{X^{1/2-\theta}}{w}\right) + O(X^{3/8+\theta}) + O(X^{3/8}w^{3/4}).$$

As previously, the prime indicates that the summation is restricted to indices coprime to $4N_E$. Let

$$L(w) = \sideset{}{'}\sum_{\substack{\ell \geq 1 \\ \gcd(\ell,w)=1}} \frac{\mu(\ell)\rho(\ell^2)f_1(\ell)}{\ell^2}. \tag{4.4.17}$$

As simple computation shows that $L(w)$ is finite and satisfies

$$\sideset{}{'}\sum_{\substack{\ell \leq X^\theta \\ \gcd(\ell,w)=1}} \frac{\mu(\ell)\rho(\ell^2)f_1(\ell)}{\ell^2} = L(w) + O_\epsilon\left(\frac{1}{X^{\theta-\epsilon}}\right). \tag{4.4.18}$$

We show that $L(w)$ does not vanish.

Lemma 4.14. *There exists a constant $c_9 > 0$ satisfying $L(w) \geq c_9$ for all $w \geq 1$.*

Proof. Expanding (4.4.17) as an Euler product gives

$$L(w) = \prod_{p\nmid w}{}' \left(1 - \frac{\rho(p^2)f_1(p)}{p^2}\right) = \prod_{p\nmid w}{}' \left(1 - \frac{\rho(p^2)}{p^2+p-1}\right),$$

with the second equality following from the definition of $f_1(p)$ in (4.4.14). Recall that Δ_F denotes the discriminant of the polynomial $F(x, 1)$, as defined at the beginning of Section 4.4.1. We further separate this product as

$$L(w) = \prod_{p\nmid \Delta_F}{}' \left(1 - \frac{\rho(p^2)}{p^2+p-1}\right) \prod_{p\mid \Delta_F}{}' \left(1 - \frac{\rho(p^2)}{p^2+p-1}\right) \prod_{p\mid w}{}' \left(1 - \frac{\rho(p^2)}{p^2+p-1}\right)^{-1}.$$

The product over the primes dividing w consists only of terms at least one, and the product over the prime divisors of Δ_F is a positive constant. Combined with (4.4.3), this shows

$$L(w) \gg \prod_{p\nmid \Delta_F}{}' \left(1 - \frac{\rho(p)}{p^2+p-1}\right).$$

Since $\rho(p) \leq 3$ for $p \nmid \Delta_F$, the right-hand side does not vanish and the proof is complete. □

Gathering (4.4.16), (4.4.18) and Lemma 4.14, we obtain

$$N_w(X) \geq \frac{c_8 c_9 f_2(w)}{w}X^{1/2} + O_\epsilon\left(\frac{f_2(w)}{w}X^{1/2-\theta+\epsilon}\right) + O(X^{3/8+\theta}) + O\left(\frac{X^{1/2-\theta}}{w}\right) + O(X^{3/8}w^{3/4}).$$

For any choice of $\theta \in (0, 1/8 - 4\alpha)$, we return to (4.4.7) and sum this inequality over w. From the definition of $f_2(n)$ in (4.4.14), it is immediate that $\varphi^*(w) \leq f_2(w) \ll_\epsilon w^\epsilon$, and we obtain

$$N(\alpha; X) \geq c_8 c_9 X^{1/2} \sum_{\substack{w \leq c_6 X^{4\alpha} \\ w \equiv w_0 \bmod 4N_E}} \frac{\varphi^*(w)}{w} + O(X^{1/2}),$$

since we assume $\alpha < 1/56$. An elementary computation shows that the sum over w is asymptotically a constant times $\log X$ and thus, we obtain the lower bound $N(\alpha; X) \gg X^{1/2} \log X$. As remarked at the beginning of Section 4.4.2, this completes the proof of Proposition 4.9.

Bibliography

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[BK90] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[BM90] A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382.

[Bou15] J. Bourgain, *A remark on solutions of the Pell equation*, Int. Math. Res. Not. IMRN (2015), no. 10, 2841–2855.

[BS07] S. Boissière and A. Sarti, *Counting lines on surfaces*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **6** (2007), no. 1, 39–52.

[BS13a] M. Bhargava and A. Shankar, *The average number of elements in the 4-Selmer groups of elliptic curves is 7*, arXiv:1312.7333.

[BS13b] ———, *The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1*, arXiv:1312.7859.

[BS15a] ———, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242.

[BS15b] ———, *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*, Ann. of Math. (2) **181** (2015), no. 2, 587–621.

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79–108.

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

[CLT01] A. Chambert-Loir and Y. Tschinkel, *Fonctions zêta des hauteurs des espaces fibrés*, Rational points on algebraic varieties, Progr. Math., vol. 199, Birkhäuser, Basel, 2001, pp. 71–115.

[Dat93] B. A. Datskovsky, *A mean-value theorem for class numbers of quadratic extensions*, A tribute to Emil Grosswald: number theory and related analysis, Contemp. Math., vol. 143, Amer. Math. Soc., Providence, RI, 1993, pp. 179–242.

[Dav51] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. **26** (1951), 179–183.

[DD10] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596.

[Del01] C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$, Experiment. Math. **10** (2001), no. 2, 191–196.

[Del05] ———, *Moments of the orders of Tate-Shafarevich groups*, Int. J. Number Theory **1** (2005), no. 2, 243–264.

[Del07] ———, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, pp. 323–340.

[FJ13] É. Fouvry and F. Jouve, *A positive density of fundamental discriminants with large regulator*, Pacific J. Math. **262** (2013), no. 1, 81–107.

[Fom98] O. M. Fomenko, *On the mean value of solutions of certain congruences*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **254** (1998), no. Anal. Teor. Chisel i Teor. Funkts. 15, 192–206, 248.

[Fou16] É. Fouvry, *On the size of the fundamental solution of the Pell equation*, J. Reine Angew. Math. **717** (2016), 1–33.

[Gau66] C. F. Gauss, *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn.-London, 1966.

[GM91] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23.

[Gol79] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), Lecture Notes in Math., vol. 751, Springer, Berlin, 1979, pp. 108–118.

[Gre92] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. Oxford Ser. (2) **43** (1992), no. 169, 45–65.

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Has36a] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung*, J. Reine Angew. Math. **175** (1936), 55–62.

[Has36b] ———, *Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionstheorem*, J. Reine Angew. Math. **175** (1936), 69–88.

[Has36c] ———, *Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung*, J. Reine Angew. Math. **175** (1936), 193–208.

[HB84] D. R. Heath-Brown, *Diophantine approximation with square-free numbers*, Math. Z. **187** (1984), no. 3, 335–344.

[HB02] ———, *The density of rational points on curves and surfaces*, Ann. of Math. (2) **155** (2002), no. 2, 553–595.

[Hon60] T. Honda, *Isogenies, rational points and section points of group varieties*, Jpn. J. Math. **30** (1960), 84–101.

[Hoo84] C. Hooley, *On the Pellian equation and the class number of indefinite binary quadratic forms*, J. Reine Angew. Math. **353** (1984), 98–131.

[Hua82] L. K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin-New York, 1982, Translated from the Chinese by Peter Shiu.

[Iwa90] H. Iwaniec, *On the order of vanishing of modular L-functions at the critical point*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 2, 365–376.

[JW09] M. J. Jacobson, Jr. and H. C. Williams, *Solving the Pell equation*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009.

[Kol88] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and Ш$(E, \mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.

[Kol90] ———, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[Kri20] D. Kriz, *Supersingular main conjectures, Sylvester's conjecture and Goldfeld's conjecture*, arXiv:2002.04767.

[KS99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

[KSW19] Z. Klagsbrun, T. Sherman, and J. Weigandt, *The Elkies curve has rank 28 subject only to GRH*, Math. Comp. **88** (2019), no. 316, 837–846.

[LÖ9] G. Lü, *Number of solutions of certain congruences*, Acta Arith. **140** (2009), no. 4, 317–328.

[Lan78] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin-New York, 1978.

[Lan83] ———, *Conjectured Diophantine estimates on elliptic curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 155–171.

[LB16] P. Le Boudec, *Height of rational points on quadratic twists of a given elliptic curve*, Bull. Lond. Math. Soc. **48** (2016), no. 1, 99–108.

[LB18] ———, *Average rank in families of quadratic twists: a geometric point of view*, Math. Ann. **371** (2018), no. 1-2, 695–705.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978), With an appendix by Mazur and M. Rapoport.

[Maz78] ———, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.

[Mil06] J. S. Milne, *Elliptic curves*, BookSurge Publishers, Charleston, SC, 2006.

[MM91] M. R. Murty and V. K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), no. 3, 447–475.

[Mor22] L. Mordell, *On the rational solutions of the indeterminate equation of the third and fourth degree*, Proc. Camb. Phil. Soc. **21** (1922), 179–192.

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Pet20a] J. Petit, *Average rank of quadratic twists with a rational point of almost minimal height*, arXiv:2011.13195.

[Pet20b] ———, *On the number of quadratic twists with a rational point of almost minimal height*, Int. Math. Res. Not. IMRN, to appear, arXiv:2004.02500.

[PPVW19] J. Park, B. Poonen, J. Voight, and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903.

[Rau09] N. Raulf, *Asymptotics of class numbers for progressions and for fundamental discriminants*, Forum Math. **21** (2009), no. 2, 221–257.

[Reu12] T. Reuss, *Pairs of k-free Numbers, consecutive square-full Numbers*, arXiv:1212.3150.

[Sal08] P. Salberger, *Rational points of bounded height on projective surfaces*, Math. Z. **258** (2008), no. 4, 805–826.

[Sar82] P. C. Sarnak, *Class numbers of indefinite binary quadratic forms*, J. Number Theory **15** (1982), no. 2, 229–247.

[Sar85] ———, *Class numbers of indefinite binary quadratic forms. II*, J. Number Theory **21** (1985), no. 3, 333–346.

[Sie35] C. L. Siegel, *Über die classenzahl quadratischer zahlkörper*, Acta Arithmetica **1** (1935), no. 1, 83–86.

[Sie44] ———, *The average measure of quadratic forms with given determinant and signature*, Ann. of Math. (2) **45** (1944), 667–685.

[Sil01] A. Silverberg, *Open questions in arithmetic algebraic geometry*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 83–142.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[Ski20] C. Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, Ann. of Math. (2) **191** (2020), no. 2, 329–354.

[Smi17] A. Smith, 2^∞*-Selmer groups,* 2^∞*-class groups, and Goldfeld's conjecture*, arXiv:1702.02325.

[SSW19] A. N. Shankar, A. Shankar, and X. Wang, *Families of elliptic curves ordered by conductor*, arXiv:1904.13063.

[Ste91] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. **4** (1991), no. 4, 793–835.

[SU14] C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.

[TŠ67] D. T. Těĭt and I. R. Šafarevič, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), 770–773.

[Wat08] M. Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125.

[Wei29] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315.

[Wei49] ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Xi18] P. Xi, *Counting fundamental solutions to the Pell equation with prescribed size*, Compos. Math. **154** (2018), no. 11, 2379–2402.

[Yam71] Y. Yamamoto, *Real quadratic number fields with large fundamental units*, Osaka Math. J. **8** (1971), 261–270.

[Zag81] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer-Verlag, Berlin-New York, 1981, Eine Einführung in die höhere Zahlentheorie. [An introduction to higher number theory], Hochschultext. [University Text].