HAL open science

Root numbers and the parity problem

Harald Andres Helfgott

To cite this version:

Harald Andres Helfgott. Root numbers and the parity problem. Mathematics [math]. Princeton University, 2003. English. NNT : . tel-00010129

HAL Id: tel-00010129

https://theses.hal.science/tel-00010129v1

Submitted on 14 Sep 2005

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Root Numbers and the Parity Problem

Harald A. Helfgott

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the
Department of Mathematics

June, 2003

© Copyright by Harald A. Helfgott, 2003.

All Rights Reserved

Abstract

Let $\mathcal{E}$ be a one-parameter family of elliptic curves over a number field K. It is natural to expect the average root number of the curves in the family to be zero. All known counterexamples to this folk conjecture occur for families obeying a certain degeneracy condition. We prove that the average root number is zero for a large class of families of elliptic curves of fairly general type. Furthermore, we show that any non-degenerate family $\mathcal{E}$ has average root number 0, provided that two classical arithmetical conjectures hold for two homogeneous polynomials with integral coefficients constructed explicitly in terms of $\mathcal{E}$.

The first such conjecture – commonly associated with Chowla – asserts the equidistribution of the parity of the number of primes dividing the integers represented by a polynomial. More precisely: given a homogeneous polynomial $f \in \mathbb{Z}[x, y]$, it is believed that $\mu(f(x, y))$ averages to zero. This conjecture can be said to represent the parity problem in its pure form, while covering the same notional ground as the Bunyakovsky-Schinzel and Hardy-Littlewood conjectures taken together.

For $\deg f = 1$ and $\deg f = 2$, Chowla's conjecture is essentially equivalent to the prime number theorem. For $\deg f > 2$, the conjecture has been unproven up to now; the traditional approaches by means of analysis and sieve theory fail. We prove the conjecture for $\deg f = 3$.

There remains to state the second arithmetical conjecture referred to previously. It is believed that any non-constant homogeneous polynomial $f \in \mathbb{Z}[x, y]$ yields to a square-free sieve. We sharpen the existing bounds on the known cases by a sieve refinement and a new approach combining height functions, sphere packings and sieve methods.

Acknowledgements

ὣς ἄρα φωνήσας πόρε φάρμακον ἀργεϊφόντης
ἐκ γαίης ἐρύσας, καί μοι φύσιν αὐτοῦ ἔδειξε.
ῥίζῃ μὲν μέλαν ἔσκε, γάλακτι δὲ εἴκελον ἄνθος:
μῶλυ δέ μιν καλέουσι θεοί: χαλεπὸν δέ τ' ὀρύσσειν
ἀνδράσι γε θνητοῖσι, θεοὶ δέ τε πάντα δύνανται.

Homer, *Odyssey*, 10.302–10.306

As my own words do not suffice to express my gratitude to my advisor, Henryk Iwaniec, the reader is referred to the passage above. The present work, however, is dedicated to those who authored the author, namely, Michel Helfgott and Edith Seier. To them, then, for love and geometry.

I am indebted to Gergely Harcos for his careful reading of early versions of the manuscript and for having prodded me to put my thesis in its present form. The second reader of the thesis, Peter Sarnak, has been helpful throughout my stay at Princeton. Thanks are due as well to Keith Conrad, Jordan Ellenberg, Chris Hall and Emmanuel Kowalski for their useful advice and to Keith Ramsay for our discussions on his unpublished work. This listing is not meant to be exhaustive.

Contents

Abstract iii

Acknowledgements iv

1 Introduction **1**

1.1 Root numbers of elliptic curves 1

1.2 Families of elliptic curves and questions of distribution 4

1.3 Issues and definitions 7

1.4 The square-free sieve 8

1.5 Previous results 10

1.6 A conjecture of Chowla's. The parity problem 11

1.7 Results 13

1.8 Families of curves over number fields 17

1.9 Guide to the text 20

2 The distribution of root numbers in families of elliptic curves **21**

2.1 Outline 21

2.2 Notation and preliminaries 21

2.3 Pliable Functions 26

2.3.1 Definition and basic properties 27

2.3.2 Pliability of local root numbers 34

2.3.3 Pliable functions and reciprocity 41
2.3.4 Averages and pliable functions 46
2.4 Using the square-free sieve 63
2.4.1 Conditional results 63
2.4.2 Miscellanea 65
2.5 The global root number and its distribution 71
2.5.1 Background and definitions 71
2.5.2 From the root number to Liouville's function 75
2.5.3 Averages and correlations 88
2.6 Examples 98
2.6.1 Specimens and how to find them 98
2.6.2 Pathologies 102

3 The parity problem **104**
3.1 Outline 104
3.2 Preliminaries 105
3.2.1 The Liouville function 105
3.2.2 Ideal numbers and Grössencharakters 106
3.2.3 Quadratic forms 109
3.2.4 Truth and convention 110
3.2.5 Approximation of intervals 110
3.2.6 Lattices, convex sets and sectors 110
3.2.7 Classical bounds and their immediate consequences 112
3.2.8 Bilinear bounds 114
3.2.9 Anti-sieving 121
3.3 The average of λ on integers represented by a quadratic form 122
3.4 The average of λ on the product of three linear factors 144
3.5 The average of λ on the product of a linear and a quadratic factor . . 149

3.6 The average of λ on irreducible cubics 159
3.6.1 Sketch 160
3.6.2 Axioms 172
3.6.3 Technical lemmas 175
3.6.4 Bounds and manipulations 177
3.6.5 Background and references for axioms 182
3.6.6 The bilinear condition 184
3.7 Final remarks and conclusions 190

4 The square-free sieve 192
4.1 Notation 194
4.2 Sieving 195
4.2.1 An abstract square-free sieve 195
4.2.2 Solutions and lattices 198
4.2.3 Square-full numbers 201
4.2.4 A concrete square-free sieve 207
4.3 A global approach to the square-free sieve 217
4.3.1 Elliptic curves, heights and lattices 217
4.3.2 Twists of cubics and quartics 221
4.3.3 Divisor functions and their averages 225
4.3.4 The square-free sieve for homogeneous quartics 230
4.3.5 Homogeneous cubics 233
4.3.6 Homogeneous quintics 234
4.3.7 Quasiorthogonality, kissing numbers and cubics 236
4.4 Square-free integers 242

A Addenda on the root number 247
A.1 Known instances of conjectures $\mathfrak{A}_i$ and $\mathfrak{B}_i$ over the rationals 247

A.2 Reducing hypotheses on number fields to their rational analogues . . . 249

A.3 Ultrametric analysis, field extensions and pliability 256

A.4 The root number in general 263

B Addenda on the parity problem **269**

B.1 The average of $\lambda(x^2 + y^4)$ 269

B.1.1 Notation and identities 269

B.1.2 Axioms 272

B.1.3 Estimates 273

Chapter 1

Introduction

Por qué los árboles esconden
el esplendor de sus raíces?

Neruda, *El libro de las preguntas*

1.1 Root numbers of elliptic curves

Let E be an elliptic curve over $\mathbb{Q}$. The reduction E mod p can

1. be an elliptic curve over $\mathbb{Z}/p$,
2. have a node, or
3. have a cusp.

We call the reduction *good* in the first case, *multiplicative* in the second case and *additive* in the third case. If the reduction is not good, then, as might be expected, we call it *bad*. If the reduction at p is multiplicative, we call it *split* if the slopes at the node lie in $\mathbb{Z}/p$, and *non-split* if they do not. Additive reduction becomes either good or multiplicative in some finite extension of $\mathbb{Q}$. Thus every E must fall into one of two categories: either it has good reduction over a finite extension of $\mathbb{Q}$, possibly $\mathbb{Q}$ itself, or it has multiplicative reduction over a finite extension of $\mathbb{Q}$, possibly $\mathbb{Q}$

itself. We speak accordingly of *potential good reduction* and *potential multiplicative reduction.*

The L-function of E is defined to be

$$L(E,s) = \prod_{p \text{ good}} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \text{ bad}} (1 - a_p p^{-s})^{-1},$$

where a_p is $p+1$ minus the number of points in E mod p. As can be seen, $L(E,s)$ encodes the local behaviour of E. It follows from the modularity theorem ([Wi], [TW], [BCDT]) that $L(E,s)$ has analytic continuation to all of $\mathbb{C}$ and satisfies the following functional equation:

$$\mathcal{N}_E^{(2-s)/2}(2\pi)^{s-2}\Gamma(2-s)L(E,2-s) = W(E)\mathcal{N}_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

where $W(E)$, called the *root number* of E, equals 1 or -1, and $\mathcal{N}_E$ is the conductor of E. The function $L(E,s)$ corresponds to a modular form f_E of weight 2 and level $\mathcal{N}_E$. The canonical involution $W_{\mathcal{N}}$ acting on modular forms of level $\mathcal{N}$ has f_E as an eigenvector with eigenvalue $W(E)$.

The set $E(\mathbb{Q})$ of points on E with rational coordinates is an abelian group under the standard operation $+$ (see e.g. [Si], III.1). A classical theorem of Mordell's states that $E(\mathbb{Q})$ is finitely generated. We define the *algebraic rank* of E to be the rank of $E(\mathbb{Q})$. We denote the algebraic rank of E by $\mathrm{rank}(E)$. The Birch-Swinnerton-Dyer conjecture asserts that $\mathrm{rank}(E)$ equals the order of vanishing $\mathrm{ord}_{s=1} L(E,s)$ of $L(E,s)$ at $s=1$. Since $W(E)$ is one if the order of vanishing is even and minus one if it is odd, the root number gives us the parity of the algebraic rank, conditionally on the conjecture. This fact makes the root number even more interesting than it already is on its own. Assuming the Birch-Swinnerton-Dyer conjecture for curves of algebraic rank zero, it suffices to prove that the root number of an elliptic curve is minus one to show that the rank is positive. If, on the other hand, we prove that $W(E) = 1$ and

find by other means that there are infinitely points on E, we have that the rank is "high", that is, at least two. (Rank 2 is considered high as it may already be atypical in certain contexts.)

It is a classical result ([De] – cf. [Ro], [Ta]) that the root number can be expressed as a product of local factors,

$$W(E) = \prod_v W_v(E),$$

where each $W_v(E)$ can be expressed in terms of a canonical representation $\sigma'_{E,v}$ of the Weil-Deligne group of $\mathbb{Q}_v$:

$$W_v(E) = \frac{\epsilon(\sigma'_{E,v}, \psi, dx)}{|\epsilon(\sigma'_{E,v}, \psi, dx)|},$$

where ψ is any nontrivial unitary character of $\mathbb{Q}_p$ and dx is any Haar measure on $\mathbb{Q}_p$. This expression has been made explicit in terms of the coefficients of E ([Ro3], [Con], [Ha]). Thus many questions about the distribution of $W(E) = (-1)^{\mathrm{ord}_{s=1} L(E,s)}$ have become somewhat more approachable than the corresponding questions about the distribution of $\mathrm{ord}_{s=1} L(E, s)$.

The natural expectation is that $W(E)$ be 1 as often as -1 when E varies within a family of elliptic curves that is in some sense typical or naturally defined. This is consistent with what is currently known about average ranks and seems to have become a folk conjecture (see for example [Si2], section 5). As we will see below, families in which this is known not to hold are in some sense degenerate.

1.2 Families of elliptic curves and questions of distribution

By a *family* $\mathcal{E}$ of elliptic curves over $\mathbb{Q}$ on one variable we mean an elliptic surface over $\mathbb{Q}$, or, equivalently, an elliptic curve over $\mathbb{Q}(t)$. In the latter formulation, a family is given by two rational functions $c_4, c_6 \in \mathbb{Q}(t)$ such that $\Delta = (c_4^3 - c_6^2)/1728$ is not identically zero, and its fiber $\mathcal{E}(t)$ at a point $t \in \mathbb{Q}$ is the curve given by the equation

$$y^2 = x^3 - \frac{c_4(t)}{48}x - \frac{c_6(t)}{864}.$$

For finitely many $t \in \mathbb{Q}$, the curve $\mathcal{E}(t)$ will be singular. In such a case we set $W(\mathcal{E}(t)) = 1$.

Every primitive irreducible polynomial $Q \in \mathbb{Z}[t]$ determines a valuation (or *place*) of $\mathbb{Q}(t)$. An additional valuation is given by $\deg(\text{den}) - \deg(\text{num})$, that is, the map taking an element of $\mathbb{Q}(t)$ to the degree of its denominator minus the degree of its numerator. Given a valuation v of $\mathbb{Q}(t)$ and an elliptic curve $\mathcal{E}$ over $\mathbb{Q}(t)$, we can examine the reduction $\mathcal{E} \bmod v$ and give it a type in exactly the same way we have described for reductions $E \bmod p$: the curve $\mathcal{E}$ will be said to have *good* reduction if its reduction at v is an elliptic curve over the residue field, resp. *multiplicative* reduction if the reduction at v has a node, *additive* if it has a cusp, *split multiplicative* if it has a node and the slopes at the node are in the residue field, *non-split multiplicative* if it is has a node but the slopes at the node are not in the residue field, *potentially good* if $\mathcal{E}$ has good reduction at the place lying over v in some finite extension of $\mathbb{Q}(t)$, *potentially multiplicative* if $\mathcal{E}$ has multiplicative reduction at the place lying over v in some finite extension of $\mathbb{Q}(t)$. The type of reduction of $\mathcal{E}$ at a given place v can be determined by the usual valuative criteria (see e.g. [Si], 179–183).

Define

$$M_{\mathcal{E}}(x,y) = \prod_{\mathcal{E} \text{ has mult. red. at } v} P_v(x,y), \tag{1.2.1}$$

where $P_v = x$ if v is the place $\deg(\text{den}) - \deg(\text{num})$, $P_v = x^{\deg Q} Q\left(\frac{y}{x}\right)$ if v is a valuation given by a primitive irreducible polynomial $Q \in \mathbb{Z}[t]$.

Given a function $f : \mathbb{Z} \to \mathbb{C}$ and an arithmetic progression $a + m\mathbb{Z}$, we define

$$\operatorname{av}_{a+m\mathbb{Z}} f = \lim_{N\to\infty} \frac{1}{N/m} \sum_{\substack{1\le n\le N \\ n\equiv a \bmod m}} f(n).$$

If $\operatorname{av}_{a+m\mathbb{Z}} f = 0$ for all $a \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, we say that f *averages to zero over the integers.* Given a function $f : \mathbb{Z}^2 \to \mathbb{C}$, a lattice coset $L \subset \mathbb{Z}^2$ and a sector $S \subset \mathbb{R}^2$ (see section 2.2), we define

$$\operatorname{av}_{S\cap L} f = \lim_{N\to\infty} \frac{1}{\#(S \cap L \cap [-N,N]^2)} \sum_{(x,y)\in S\cap L\cap[-N,N]^2} f(x,y).$$

We say that f *averages to zero over* $\mathbb{Z}^2$ if $\operatorname{av}_{S\cap L} f = 0$ for all choices of S and L. Given a function $f : \mathbb{Q} \to \mathbb{Z}$, a lattice coset $L \subset \mathbb{Z}^2$ and a sector $S \subset \mathbb{R}^2$, we define

$$\operatorname{av}_{\mathbb{Q},S\cap L} f = \lim_{N\to\infty} \frac{\sum_{(x,y)\in S\cap L\cap[-N,N]^2,\, \gcd(x,y)=1} f(y/x)}{\#\{(x,y) \in S \cap L \cap [-N,N]^2 : \gcd(x,y) = 1\}}.$$

We say that f *averages to zero over the rationals* if $\operatorname{av}_{\mathbb{Q},S\cap L} f = 0$ for all choices of S and L. We are making our definition of zero average strict enough for it to be invariant under fractional linear transformations. Moreover, by letting S be arbitrary, we allow sampling to be restricted to any open interval in $\mathbb{Q}$. Thus our results will not be imputable to peculiarities in averaging order or to superficial cancellation.

In the literature, a family $\mathcal{E}(t)$ for which

$$j(\mathcal{E}(t)) = \frac{c_4(\mathcal{E}(t))^3}{\Delta(\mathcal{E}(t))}$$

is constant is sometimes called a *constant family.* When examples were found ([Ro3], [Riz1]) of constant families of elliptic curves in which the root number did not average to zero, it seemed plausible that such behaviour might be a degeneracy peculiar to constant families. It was thus somewhat of a surprise when non-constant families of non-zero average root number were found to exist.

All non-constant families considered in [Man] and [Riz2] had $M_{\mathcal{E}}(x, y)$ equal to a constant, or, what is the same, $M_{\mathcal{E}}(x, y) = 1$; in other words, they had no places of multiplicative reduction as elliptic curves over $\mathbb{Q}(t)$. Families with non-constant $M_{\mathcal{E}}$ were hardly touched upon, as they were felt to present severe number-theoretical difficulties (see, e. g., [Man], p. 34, third paragraph). The subject of the present work is precisely such families.

We will see how families with non-constant $M_{\mathcal{E}}$ are not only heuristically different from families with constant $M_{\mathcal{E}}$ but also quite different in their behaviour. As we will prove – in some cases conditionally on two standard conjectures in analytic number theory, and in the other cases unconditionally – $W(\mathcal{E}(t))$ averages to zero over the integers and over the rationals for any family of elliptic curves $\mathcal{E}$ with non-constant $M_{\mathcal{E}}$. All autocovariances of $W(\mathcal{E}(t))$ other than the variance are zero as well. In other words, for any family $\mathcal{E}$ with at least one place of multiplicative reduction over $\mathbb{Q}(t)$, the function $t \mapsto W(\mathcal{E}(t))$ behaves essentially like white noise.

We may thus see the constancy of $M_{\mathcal{E}}$ as the proper criterion of degeneracy for our problem. The generic case is that of non-constant $M_{\mathcal{E}}$: for a typical pair of polynomials or rational functions $c_4(t)$, $c_6(t)$, the numerator of the discriminant $\Delta = (c_4(t)^3 - c_6(t)^2)/1728$ does in general have polynomial factors not present in $c_4(t)$ or $c_6(t)$. Any such factor will be present in $M_{\mathcal{E}}$ as well, making it non-constant.

1.3 Issues and definitions

The main analytical difficulty in case (3) lies in the parity of the number of primes dividing an integer represented by a polynomial. A precise discussion necessitates some additional definitions.

We will say that the reduction of $\mathcal{E}$ at v is *quite bad* if there is no non-zero rational function $d(t)$ for which the family

$$\mathcal{E}_d : d(t)y^2 = x^3 - \frac{c_4(t)}{48} - \frac{c_6(t)}{864}$$

has good reduction at v. If the reduction of $\mathcal{E}$ at v is bad but not quite bad, we say it is *half bad*.

We let

$$\begin{aligned} B_{\mathcal{E}}(x,y) &= \prod_{\mathcal{E} \text{ has bad red. at } v} P_v(x,y), \\ B'_{\mathcal{E}}(x,y) &= \prod_{\mathcal{E} \text{ has quite bad red. at } v} P_v(x,y), \end{aligned} \tag{1.3.1}$$

where P_v is as in (1.2.1). It follows immediately from the definitions that $M_{\mathcal{E}}(x,y)$, $B_{\mathcal{E}}(x,y)$ and $B'_{\mathcal{E}}(x,y)$ are square-free and can be constant only if identically equal to one. By saying that a polynomial P is square-free we mean that no irreducible non-constant polynomial P_i appears in the factorization $P = P_1 P_2 \cdots P_n$ more than once.

Given a function $f : \mathbb{Z} \to \{-1, 1\}$, a non-zero integer k and an arithmetic progression $a + m\mathbb{Z}$, we define

$$\gamma_{a+m\mathbb{Z},k}(f) = \lim_{N\to\infty} \frac{1}{N/m} \sum_{\substack{1\le n\le N \\ n\equiv a \bmod m}} f(n)f(n+k).$$

If $\operatorname{av}_{\mathbb{Z}} f = 0$, then $\gamma_{\mathbb{Z},k}(f)$ equals the kth autocorrelation and the kth autocovariance of the sequence $f(1), f(2), f(3), \cdots$. (Note that, since $f(n) = \pm 1$ for all n, the concepts

of autocorrelation and autocovariance coincide when $\mathrm{av}_{\mathbb{Z}} f = 0$.) We say that f is *white noise over the integers* if $\mathrm{av}_{a+m\mathbb{Z}} f = 0$ and $\mathrm{av}_{a+m\mathbb{Z},k} f = 0$ for all choices of $a + m\mathbb{Z}$ and k.

Given a function $f : \mathbb{Z} \to \{-1, 1\}$, a lattice coset $L \subset \mathbb{Z}^2$, a sector $S \subset \mathbb{R}^2$ and a non-zero rational t_0, we define

$$\gamma_{L\cap S,t}(f) = \lim_{N\to\infty} \frac{\sum_{(x,y)\in S\cap L\cap[-N,N]^2,\, \gcd(x,y)=1} f\left(\frac{y}{x}\right) f\left(\frac{y}{x}+t\right)}{\#\{(x,y) \in S \cap L \cap [-N,N]^2 : \gcd(x,y) = 1\}}.$$

We say that f *is white noise over the rationals* if $\mathrm{av}_{\mathbb{Q},L\cap S} f = 0$ and $\gamma_{L\cap S,t}(f) = 0$ for all choices of L, S and t.

We can now list all questions addressed here and in the previous literature as follows:

1. are $\{t \in \mathbb{Q} : W(\mathcal{E}(t)) = 1\}$ and $\{t \in \mathbb{Q} : W(\mathcal{E}(t)) = -1\}$ both infinite?
2. are $\{t \in \mathbb{Q} : W(\mathcal{E}(t)) = 1\}$ and $\{t \in \mathbb{Q} : W(\mathcal{E}(t)) = -1\}$ both dense in $\mathbb{Q}$?
3. does $W(\mathcal{E}(t))$ average to zero over the integers?
4. is $W(\mathcal{E}(t))$ white noise over the integers?
5. does $W(\mathcal{E}(t))$ average to zero over the rationals?
6. is $W(\mathcal{E}(t))$ white noise over the rationals?

Evidently, an affirmative answer to (2) implies one to (1). An affirmative answer to (5) implies that the answers to (1) and (2) are "yes" as well.

1.4 The square-free sieve

Starting with [GM] and [Ro3], the square-free sieve has appeared time and again in the course of nearly every endeavour to answer any of the questions above. It seems by now to be an analytic difficulty that cannot be avoided.

Definition 1. *We say that a polynomial* $P \in \mathbb{Z}[x]$ yields to a square-free sieve *if*

$$\lim_{N\to\infty} \frac{1}{N} \#\{1 \le x \le N : \exists p > N^{1/2}\, s.t.\, p^2 | P(x)\} = 0. \tag{1.4.1}$$

We say that a homogeneous polynomial $P \in \mathbb{Z}[x, y]$ yields to a square-free sieve

$$\lim_{N\to\infty} \frac{1}{N^2} \#\{-N \le x, y \le N : \gcd(x, y) = 1, \exists p > N\, s.t.\, p^2 | P(x, y)\} = 0. \tag{1.4.2}$$

There is very little we can say unconditionally about a family $\mathcal{E}$ unless we can prove that $B'_{\mathcal{E}}(x, y)$ yields to a square-free sieve.

Conjecture $\mathfrak{A}_1$. *Every square-free polynomial* $P \in \mathbb{Z}[x]$ *yields to a square-free sieve.*

Conjecture $\mathfrak{A}_2$. *Every square-free homogeneous polynomial* $P \in \mathbb{Z}[x, y]$ *yields to a square-free sieve.*

Conjecture $\mathfrak{A}_1(P)$ is clear for P linear.[1] Estermann [Es] proved it for $\deg(P) = 2$. Hooley ([Hoo], Chapter 4) proved it for $\deg(P) = 3$. By then it was expected that $\mathfrak{A}_1$ would hold for any square-free polynomial; in some sense $\mathfrak{A}_1$ and $\mathfrak{A}_2$ are much weaker than the conjectures $\mathfrak{B}_1$, $\mathfrak{B}_2$ to be treated in section 1.6, though $\mathfrak{B}_i$ does not imply $\mathfrak{A}_i$. Greaves [Gre] proved $\mathfrak{A}_2(P)$ for $\deg(P) \le 6$. Both Hooley's and Greaves' bounds on the speed of convergence of (1.4.1) will be strengthened in Chapter 4.

Note that, if P_1 and P_2 have no factors in common and $\mathfrak{A}_{\mathfrak{i}}(P_1)$ and $\mathfrak{A}_{\mathfrak{i}}(P_2)$ both hold, then $\mathfrak{A}_{\mathfrak{i}}(P_1P_2)$ holds. Let

$$\deg_{\text{irr}}(P) = \max_i \deg(Q_i),$$

where $P = Q_1^{k_1} Q_2^{k_2} \cdots Q_n^{k_n}$ is the decomposition of P into irreducible factors. Given this notation, we can say that we know $\mathfrak{A}_1(P)$ for $\deg_{\text{irr}}(P) \le 3$ and $\mathfrak{A}_2(P)$ for

[1] By $X(P)$ we denote the validity of a conjecture X for a specific polynomial P. Thus Conjecture $\mathfrak{A}_1(P)$ is the same as the statement "P yields to a square-free sieve."

$\deg_{\text{irr}}(P) \leq 6$.

Granville has shown [Gran] that Conjectures $\mathfrak{A}_1$ and $\mathfrak{A}_2$ follow in general from the *abc* conjecture. Unlike the unconditional results just mentioned, this general conditional result does not give us any explicit bounds.

1.5 Previous results

We can now state what is known about the answers to the questions posed at the end of section 1.3. A family $\mathcal{E}$ will present one of three very different kinds of behaviour depending on whether $j(\mathcal{E}(t))$ or $M_{\mathcal{E}}(x, y)$ is constant. Notice that, if $j(\mathcal{E}(t))$ is constant, then $M_{\mathcal{E}}(x, y)$ is constant.

1. j constant

   In this case $\mathcal{E}$ consists of quadratic twists

   $$\mathcal{E}_d(t) : d(t)y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$$

   of a fixed elliptic curve over $\mathbb{Q}$. Rohrlich [Ro3] showed that, depending on the twisting function d, either (1) $\{t \in \mathbb{Q} : W(\mathcal{E}(t)) = 1\}$ and $\{t \in \mathbb{Q} : W(\mathcal{E}(t)) = -1\}$ are both dense in $\mathbb{Q}$, or (2) $W(\mathcal{E}(t))$ is constant on $\{t \in \mathbb{Q} : d(t) > 0\}$ and on $\{t \in \mathbb{Q} : d(t) < 0\}$. Rizzo [Riz1] pointed out that in the latter case the set of values of $\operatorname{av}_{\mathbb{Q}} W(\mathcal{E}(t))$ for different functions d is dense is $[-1, 1]$.

2. j non-constant, $M_{\mathcal{E}}$ constant

   Here Manduchi showed [Man] that $\{t \in \mathbb{Q} : d(t) > 0\}$ and on $\{t \in \mathbb{Q} : d(t) < 0\}$ are both dense provided that Conjecture $\mathfrak{A}_2(B'_{\mathcal{E}})$ holds.

   Rizzo has given examples [Riz2] of families $\mathcal{E}$ with non-constant j and $M_{\mathcal{E}} = 1$ such that $\operatorname{av}_{\mathbb{Z}} W(\mathcal{E}(n)) \neq 0$. In section 2.6.2 we will see an example of a familiy with non-constant j, $M_{\mathcal{E}} = 1$ and $\operatorname{av}_{\mathbb{Q}} W(\mathcal{E}(t)) \neq 0$.

3. j and $M_{\mathcal{E}}$ non-constant

   Manduchi [Man] showed that, if $\deg(M_{\mathcal{E}}) = 1$, then both $\{t \in \mathbb{Q} : d(t) > 0\}$ and on $\{t \in \mathbb{Q} : d(t) < 0\}$ are infinite. Nothing else has been known until now for this case.

The main difference between cases (1) and (2), on the other hand, and case (3), on the other, can be roughly outlined as follows. Assume $M_{\mathcal{E}}$ is constant; in other words, assume that $\mathcal{E}$ has no places of multiplicative reduction when considered as an elliptic curve over $\mathbb{Q}(t)$. Then for every ϵ there is a finite set S of primes such that, for any large N, the elliptic curve $\mathcal{E}(t)$ can have multiplicative reduction at places p not in S only for a proportion less than ϵ of all values of t. As will become clear later, this eliminates what would otherwise be the analytical heart of the matter, namely, the estimation of

$$\prod_{p \text{ mult.}} W_p(\mathcal{E}(t)),$$

that is, the product of the local root numbers at the places p of multiplicative reduction.

1.6 A conjecture of Chowla's. The parity problem

Our main purpose is to determine the behavior of the root number in families $\mathcal{E}$ with $M_{\mathcal{E}}$ non-constant. We will see that in this case all issues raised in Section 1.3 amount to a classical arithmetical question in disguise. Consider the *Liouville function*

$$\lambda(n) = \begin{cases} \prod_{p|n}(-1)^{v_p(n)} & \text{if } n \neq 0 \\ 0 & \text{if } n = 0. \end{cases}$$

Conjecture $\mathfrak{B}_1$. *Let $P \in \mathbb{Z}[x]$ be a polynomial not of the form $cQ^2(x)$, $c \in \mathbb{Z}$, $Q \in \mathbb{Z}[x]$. Then $\lambda(P(n))$ averages to zero over the integers.*

Conjecture $\mathfrak{B}_2$. *Let $P \in \mathbb{Z}[x,y]$ be a homogeneous polynomial not of the form $cQ^2(x,y)$, $c \in \mathbb{Z}$, $Q \in \mathbb{Z}[x,y]$. Then $\lambda(P(x,y))$ averages to zero over $\mathbb{Z}^2$.*

In the present form, Conjecture $\mathfrak{B}_1$ is credited to S. Chowla. (Some cases of $\mathfrak{B}_1$ were already included in the Hardy-Ramanujan conjectures.) As stated in [Ch], p. 96:

> If [P is linear, Conjecture $\mathfrak{B}_1(P)$] is equivalent to the Prime Number Theorem. If [the degree of P] is at least 2, this seems an extremely hard conjecture.

In fact $\mathfrak{B}_1(x(x+1))$ is commonly considered to be roughly as hard as the Twin Prime Number conjecture.

Conjecture $\mathfrak{B}_2(P)$ is equivalent to the Prime Number Theorem when P is linear. In the case of P quadratic, the main ideas needed for a proof of $\mathfrak{B}_2(P)$ were supplied by de la Vallée-Poussin ([DVP1], [DVP2]) and Hecke ([Hec]). (We provide a full treatment in section 3.3.) The attacks on $\mathfrak{B}_1(P)$ for $\deg(P) = 1$ and on $\mathfrak{B}_2(P)$ for $\deg(P) = 1, 2$ rely on the fact that one can reduce the problem to a question about L-functions. This approach breaks down for $\mathfrak{B}_1(P)$, $\deg(P) > 1$ and $\mathfrak{B}_2(P)$, $\deg(P) > 2$, as there seems to be no analytic object corresponding to $P \in \mathbb{Z}[x]$, $\deg P > 1$ or $P \in \mathbb{Z}[x,y]$, $\deg P > 2$.

A classical sieve treatment of conjectures $\mathfrak{B}_1$ and $\mathfrak{B}_2$ is doomed to fail; they may be said to represent the parity problem in its purest form. (The *parity problem* is the fact that, as was pointed out by Selberg [Se2], a standard sieve framework cannot distinguish between numbers with an even number of prime factors and numbers with an odd number of prime factors.) Until recently, the parity problem was seen as an unsurmountable difficulty whenever the sets to be examined were sparser than the integers. The sets in question here are $S_1(P) = \{P(n) : n \in \mathbb{Z}\}$ and $S_2(P) =$

$\{P(n,m) : n, m \in \mathbb{Z}\}$. For a set $S \in \mathbb{Z}$, define the *logarithmic density* $d(S)$ to be

$$d(S) = \lim_{N\to\infty} \frac{\log\left(\#\{x \in S : |x| < N\}\right)}{\log N}$$

when defined. A set S is said to be sparser than the integers if $d(S) < 1$. Since $d(S_1(P)) = 1/\deg(P)$ and $d(S_2(P)) = 2/\deg(P)$, the set S_1 is sparser than the integers for $\deg(P) > 1$ and S_2 is sparser than the integers for $\deg(P) > 2$.

We prove conjecture $\mathfrak{B}_2(P)$ for $\deg(P) = 3$. For P irreducible, the approach taken follows the same lines as the novel results of the last few years ([FI1], [FI2], [H-B], [HBM]) on the number of primes represented by a polynomial. Friedlander and Iwaniec ([FI1], [FI2]) broke through the difficulties imposed by the parity problem in proving that there are infinitely many primes of the form $x^2 + y^4$. While the specifics in their extremely ingenious method do not seem to carry over simply to any other polynomial, Heath-Brown ([H-B]) succeeded in proving the existence of infinitely many primes of the form $x^3 + 2y^3$ while following akin general lineaments. In the same way, while $\mathfrak{B}_2(P)$ for $\deg P = 3$ demands a great deal of ad-hoc work, it can be said to be a new instance of the general approach of Friedlander and Iwaniec. Note that one cannot deduce $\mathfrak{B}_2(P)$, $\deg P = 3$ from the corresponding result about the existence or number of primes represented by P; such an implication exists only for $\deg P = 1$. For $\mathfrak{B}_2(P)$, P reducible, there is not even a corresponding question on prime numbers, and in fact the methods used then are quite different from those for P irreducible.

1.7 Results

By **Theorem 0.0** ($\mathfrak{X}(P)$, $\mathfrak{Y}(Q)$) we mean a theorem conditional on conjectures $\mathfrak{X}$ and $\mathfrak{Y}$ in so far as they concern the objects P and Q, respectively. A result whose statement does not contain parentheses after the numeration should be understood

to be unconditional.

Theorem 1.7.1 ($\mathfrak{A}_1(B'_{\mathcal{E}}(1,t))$, $\mathfrak{B}_1(M_{\mathcal{E}}(1,t))$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $M_{\mathcal{E}}(1,t)$ is not constant. Then $W(\mathcal{E}(t))$ averages to zero over the integers.*

Theorem 1.7.2 ($\mathfrak{A}_1(B'_{\mathcal{E}}(1,t))$, $\mathfrak{B}_1(M_{\mathcal{E}}(1,t)M_{\mathcal{E}}(1,t+k))$ for all non-zero $k \in \mathbb{Z}$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Let k be an integer other than zero. Assume that $M_{\mathcal{E}}(1,t)$ is not constant. Then $W(\mathcal{E}(t))$ is white noise over the integers.*

Theorem 1.7.3 ($\mathfrak{A}_2(B'_{\mathcal{E}})$, $\mathfrak{B}_2(M_{\mathcal{E}})$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $M_{\mathcal{E}}$ is not constant. Then $W(\mathcal{E}(t))$ averages to zero over the rationals.*

Theorem 1.7.4 ($\mathfrak{A}_2(B'_{\mathcal{E}})$, $\mathfrak{B}_2(M_{\mathcal{E}}(x,y)M_{\mathcal{E}}(k_0x, k_0y+k_1x))$ for all non-zero $k_0 \in \mathbb{Z}$ and all $k_1 \in \mathbb{Z}$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Let $k = k_1/k_0$ be a non-zero rational number, $\gcd(k_0, k_1) = 1$. Assume that $M_{\mathcal{E}}$ is not constant. Then $W(\mathcal{E}(t))$ is white noise over the rationals.*

The unconditional cases of the theorems above can be stated as follows.

Theorem 1.1′. *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume $\deg_{\mathrm{irr}}(B'_{\mathcal{E}}(1,t)) \leq 3$ and $\deg(M_{\mathcal{E}}(1,t)) = 1$. Then $W(\mathcal{E}(t))$ averages to zero over the integers. Explicitly, for any arithmetic progression $a + m\mathbb{Z}$, $m \leq (\log N)^{A_1}$,*

$$\mathrm{av}_{a+m\mathbb{Z}}\, W(\mathcal{E}(n)) \ll \begin{cases} (\log N)^{-A_2} & \text{if } \deg_{\mathrm{irr}}(B'_{\mathcal{E}}(1,t)) = 1, 2, \\ (\log N)^{-0.5718\ldots} & \text{if } \deg_{\mathrm{irr}}(B'_{\mathcal{E}}(1,t)) = 3, \end{cases}$$

where A_1 and A_2 are arbitrarily large constants, and the implicit constant depends only on $\mathcal{E}$, A_1 and A_2.

Theorem 1.3′. *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $M_{\mathcal{E}}$ is not constant. Suppose that $\deg_{\mathrm{irr}}(B'_{\mathcal{E}}) \leq 6$ and $\deg(M_{\mathcal{E}}) \leq 3$. Then $W(\mathcal{E}(t))$ averages to zero over the rationals. Explicitly, for any sector $S \subset \mathbb{R}^2$ and every lattice coset $L \subset \mathbb{Z}^2$ of index $[\mathbb{Z}^2 : L] \leq (\log N)^{A_1}$, we have that $\mathrm{av}_{\mathbb{Q},S\cap L}(W(\mathcal{E}(t)))$ is bounded above by*

$$\begin{aligned} C \cdot (\log N)^{-A_2} &\ \textit{if}\ \deg_{\mathrm{irr}}(B'_{\mathcal{E}}) \leq 5,\ \deg(M_{\mathcal{E}}) = 1, 2, \\ C \cdot \frac{\log\log N}{\log N} &\ \textit{if}\ \deg_{\mathrm{irr}}(B'_{\mathcal{E}}) \leq 5,\ \deg(M_{\mathcal{E}}) = 3,\ M_{\mathcal{E}}\ \textit{red.}, \\ C \cdot \frac{(\log\log N)^5(\log\log\log N)}{\log N} &\ \textit{if}\ \deg_{\mathrm{irr}}(B'_{\mathcal{E}}) \leq 5,\ \deg(M_{\mathcal{E}}) = 3,\ M_{\mathcal{E}}\ \textit{irr.}, \\ C \cdot (\log N)^{-1/2} &\ \textit{if}\ \deg_{\mathrm{irr}}(B'_{\mathcal{E}}) = 6,\ \deg(M_{\mathcal{E}}) \leq 3, \end{aligned}$$

where A_1 and A_2 are arbitrarily large constants, and C depends only on $\mathcal{E}$, S, A_1 and A_2.

Theorem 1.4′. *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Suppose that $\deg_{\mathrm{irr}}(B'_{\mathcal{E}}) \leq 6$ and $\deg(M_{\mathcal{E}}) = 1$. Then $W(\mathcal{E})$ is white noise over the rationals. Explicitly, for any sector $S \subset \mathbb{R}^2$, any lattice coset $L \subset \mathbb{Z}^2$ of index $[\mathbb{Z}^2 : L] \leq (\log N)^{A_1}$, and any non-zero rational number t_0, we have that*

$$\gamma_{L\cap S,t_0}(W(\mathcal{E}(t))) \ll \begin{cases} (\log N)^{-A_2} & \textit{if}\ \deg_{\mathrm{irr}}(B'_{\mathcal{E}}) \leq 5, \\ (\log N)^{-0.5718\ldots} & \textit{if}\ \deg_{\mathrm{irr}}(B'_{\mathcal{E}}) = 6, \end{cases}$$

where A_1 and A_2 are arbitrarily large constants, and the implied constant depends only on $\mathcal{E}$, S, A_1 and A_2.

By $BSD(E)$ we denote the validity of the Birch-Swinnerton-Dyer conjecture for the elliptic curve E over $\mathbb{Q}$. As consequences of Theorems 1.7.1 and 1.7.3, we have

Corollary 1.7.5 ($\mathfrak{A}_1(B'_{\mathcal{E}}(1,t))$, $\mathfrak{B}_1(M_{\mathcal{E}}(1,t))$, $BSD(\mathcal{E}(t))$ for every $t \in \mathbb{Z}$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $j(\mathcal{E}(t))$ and $M_{\mathcal{E}}(1,t)$*

are not constant. Then

$$\mathrm{av}_{\mathbb{Z}}\,\mathrm{rank}(\mathcal{E}(t)) \geq \mathrm{rank}(\mathcal{E}) + 1/2$$

for every interval $I \subset \mathbb{R}$.

Corollary 1.7.6 ($\mathfrak{A}_2(B'_{\mathcal{E}})$, $\mathfrak{B}_2(M_{\mathcal{E}})$, *BSD*$(\mathcal{E}(t))$ for every $t \in \mathbb{Q}$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $j(\mathcal{E}(t))$ and $M_{\mathcal{E}}$ are not constant. Then*

$$\mathrm{av}_{I}\,\mathrm{rank}(\mathcal{E}(t)) \geq \mathrm{rank}(\mathcal{E}) + 1/2$$

for every interval $I \subset \mathbb{R}$.

For conditional upper bounds on $\mathrm{av}_{\mathbb{Z}}\,\mathrm{rank}(\mathcal{E}(t))$ and a general discussion of what is currently believed about the distribution of $\mathrm{rank}(\mathcal{E}(t))$, see [Si2].

From Corollaries 1.7.5 and 1.7.6 we obtain the following two statements, which are far weaker than the preceding but, in general, seem to be still inaccessible otherwise.

Corollary 1.7.7 ($\mathfrak{A}_1(B'_{\mathcal{E}}(1,t))$, $\mathfrak{B}_1(M_{\mathcal{E}}(1,t))$, *BSD*$(\mathcal{E}(t))$ for every $t \in \mathbb{Z}$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $j(\mathcal{E}(t))$ and $M_{\mathcal{E}}(1,t)$ are not constant. Then $\mathcal{E}(t)$ has infinitely many rational points for infinitely many $t \in \mathbb{Z}$.*

Corollary 1.7.8 ($\mathfrak{A}_2(B'_{\mathcal{E}})$, $\mathfrak{B}_2(M_{\mathcal{E}})$, *BSD*$(\mathcal{E}(t))$ for every $t \in \mathbb{Q}$). *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $j(\mathcal{E}(t))$ and $M_{\mathcal{E}}$ are not constant. Then $\mathcal{E}(t)$ has infinitely many rational points for infinitely many $t \in \mathbb{Q}$.*

The reader may wonder whether it is possible to dispense with conjectures $\mathfrak{B}_1$, $\mathfrak{B}_2$ and still obtain results along the lines of Theorems 1.7.1 and 1.7.3. That this is not the case is the import of the following two results.

Proposition 1.7.9 ($\mathfrak{A}_1(B'_{\mathcal{E}})$)**.** *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $M_{\mathcal{E}}(1,t)$ is not constant. Suppose that $W(\mathcal{E}(t))$ averages to zero over the integers. Then $\mathfrak{B}_1(M_{\mathcal{E}}(1,t))$ holds.*

Proposition 1.7.10 ($\mathfrak{A}_2(B'_{\mathcal{E}})$)**.** *Let $\mathcal{E}$ be a family of elliptic curves over $\mathbb{Q}$ on one variable. Assume that $M_{\mathcal{E}}$ is not constant. Suppose that $W(\mathcal{E}(t))$ averages to zero over the rationals. Then $\mathfrak{B}_2(M_{\mathcal{E}})$ holds.*

Thus, if we assume $\mathfrak{A}_1$ and $\mathfrak{A}_2$, or the *abc*-conjecture, which implies them, we have that the problem of averaging the root number is equivalent to the problem of averaging λ over the values taken by a polynomial.

1.8 Families of curves over number fields

We know considerably less about elliptic curves over arbitrary number fields than we do about elliptic curves over $\mathbb{Q}$. The L-function of an elliptic curve E over a number field K is known to have a functional equation only for some special choices of E over totally real number fields other than $\mathbb{Q}$ [SW]. Nevertheless, we know that, if the L-function of an elliptic curve over a number field K does have a functional equation, its sign must be equal to the product of the local root numbers [De]. Thus we can simply define the root number of an elliptic curve E over K as the product of the local root numbers $W_{\mathfrak{p}}(E)$, knowing that the sign of a hypothetical functional equation would have to equal such a product.

Let E be an elliptic curve over a number field K. The local root numbers $W_{\mathfrak{p}}(E)$ have been explicited by Rohrlich [Ro2] for every prime $\mathfrak{p}$ not dividing 2 or 3. To judge from Halberstadt's tables for $K = \mathbb{Q}$, $\mathfrak{p} = 2, 3$ [Ha], a solution for $\mathfrak{p}|2, 3$ and arbitrary K is likely to admit only an exceedingly unwieldy form. One of our results (Proposition 2.3.24) will allow us to ignore $W_{\mathfrak{p}}$ for finitely many $\mathfrak{p}$, and, in particular, for all $\mathfrak{p}$ dividing 2 or 3. Due to this simplification, we will find working with root

numbers over number fields no harder than working with root numbers over the rationals.

Averaging is a different matter. It is not immediately clear what kind of average should be taken when the elliptic surface in question is defined over $K \neq \mathbb{Q}$. Should one take the average root number of the fibers lying over $\mathbb{Z}$ or $\mathbb{Q}$, as before? Or should one take the average over all fibers, where the base K is ordered by norm? (It is not clear what this would mean when K has real embeddings.) Or should one consider all elements of the base inside a box in $K \otimes_{\mathbb{Q}} \mathbb{R}$? The basic descriptive machinery presented in Section 2.3 is independent of the kind of average settled upon. As our main purpose in generalizing our results is to understand the root number better, not to become involved in the difficulties inherent in applying analytic number theory to arithmetic over number fields, we choose to take averages over $\mathbb{Q}$ and $\mathbb{Z}$. However, we work over number fields whenever one can proceed in general without complicating matters; see subsections 2.3.1–2.3.3 and section 4.2.

By a *family* $\mathcal{E}$ of elliptic curves over a number field K on one variable we mean an elliptic curve over $K(t)$. Let $\mathfrak{O}_K$ be the ring of integers of K. We can state conjectures $\mathfrak{A}_1$, $\mathfrak{A}_2$, $\mathfrak{B}_1$ and $\mathfrak{B}_2$ almost exactly as before.

Definition 2. *Let K be a number field. We say that a polynomial $P \in \mathfrak{O}_K[x]$* yields to a square-free sieve *if*

$$\lim_{N\to\infty} \frac{1}{N} \#\{1 \leq x \leq N : \exists \mathfrak{p}\ s.t.\ \rho(\mathfrak{p}) > N^{1/2}, \mathfrak{p}^2 | P(x)\} = 0,$$

where $\rho(\mathfrak{p})$ is the positive integer generating $\mathfrak{p} \cap \mathbb{Z}$. We say that a homogeneous polynomial $P \in \mathfrak{O}_K[x, y]$ yields to a square-free sieve

$$\lim_{N\to\infty} \frac{1}{N^2} \#\{-N \leq x, y \leq N : \exists \mathfrak{p}\ s.t.\ \rho(\mathfrak{p}) > N, \mathfrak{p}^2 | P(x, y)\} = 0.$$

Definition 3. *Let K be a number field. We define the* generalized Liouville function

λ_K on the set of ideals of $\mathfrak{O}_K$ as follows:

$$\lambda_K(\mathfrak{a}) = \begin{cases} \prod_{\mathfrak{p}|\mathfrak{a}} (-1)^{v_{\mathfrak{p}}(\mathfrak{a})} & \text{if } \mathfrak{a} \neq 0, \\ 0 & \text{if } \mathfrak{a} = 0. \end{cases}$$

If $x \in \mathfrak{O}_K$, we take $\lambda_K(x)$ to mean $\lambda_K((x))$.

Conjecture $\mathfrak{A}_1$. *Let K be a number field. Every square-free polynomial $P \in \mathfrak{O}_K[x]$ yields to a square-free sieve.*

Conjecture $\mathfrak{A}_2$. *Let K be a number field. Every square-free homogeneous polynomial $P \in \mathfrak{O}_K[x, y]$ factors yields to a square-free sieve.*

Hypothesis $\mathfrak{B}_1$. *Let $P \in \mathfrak{O}_K[x]$ be a polynomial not of the form $cQ^2(x)$, $c \in \mathfrak{O}_K$, $Q \in \mathfrak{O}_K[x]$. Then $\lambda_K(P(n))$ averages to zero over the (rational) integers.*

Hypothesis $\mathfrak{B}_2$. *Let $P \in \mathfrak{O}_K[x, y]$ be a homogeneous polynomial not of the form $cQ^2(x, y)$, $c \in \mathfrak{O}_K$, $Q \in \mathfrak{O}_K[x, y]$. Then $\lambda_K(P(x, y))$ averages to zero over $\mathbb{Z}^2$.*

Notice that we speak of Hypotheses $\mathfrak{B}_1$ and $\mathfrak{B}_2$, not of Conjectures $\mathfrak{B}_1$ and $\mathfrak{B}_2$. This is so because $\mathfrak{B}_i$ fails to hold for some polynomials P over number fields other than $\mathbb{Q}$. Take, for example, $K = \mathbb{Q}(i)$, $P(x) = x$. Then $\lambda_K(P(x)) = 1$ for all $x \in \mathbb{Z}$ with $x \equiv 1 \bmod 4$.

We can, however, reduce Hypothesis $\mathfrak{B}_i(K, P)$ to the case $K = \mathbb{Q}$ for which it is thought always to hold, provided that K and P satisfy certain conditions. (The counterexample $K = \mathbb{Q}(i)$, $P(x) = x$ does not fulfill these criteria.) In particular, if $K/\mathbb{Q}$ is Galois, the situation can be described fully (Corollaries A.2.9 and A.2.10). Conjecture $\mathfrak{A}_i(K, P)$ can always be reduced to $\mathfrak{A}_i(\mathbb{Q}, P')$ for some polynomial P' over $\mathbb{Q}$. See Appendix A.2.

Theorems 1.1–1.4 and Propositions 1.7.9, 1.7.10 carry over word by word with $\mathbb{Q}$ replaced by K. Corollaries 1.7.5 to 1.7.8 carry over easily as well.

1.9 Guide to the text

The main body of the present work is divided into three parts. They are independent from each other as far as notation and background are concerned. The first part (Chapter 2) applies the main results of the other two parts, which address the analytical side of the matter. The reader who is interested only in the distribution of the root number may want to confine his attention to Chapter 2 on a first reading.

In the second part, we prove that λ and μ average to zero over the integers represented by a homogeneous polynomial of degree at most 3. In the third part, we strengthen the available results on square-free sieves by using a mixture of techniques based in part on elliptic curves. The appendices deal with several related topics of possible interest, including the behavior of $\lambda(x^2 + y^4)$, the relation between certain hypotheses for different number fields, and the average of the root number of cusp forms.

Chapter 2

The distribution of root numbers in families of elliptic curves

2.1 Outline

We will start by describing the behavior of the local root number $W_{\mathfrak{p}}(\mathcal{E}(t))$ for fixed $\mathfrak{p}$ and varying t. It will be necessary to introduce and explay a class of objects, *pliable functions*, which, among other properties, have desirable qualities as multipliers.

The global root number $W(\mathcal{E}(t))$ can be written as the product of a pliable function, a term of the form $\lambda(P(x,y))$ and a correction factor reflecting the fact that square-free polynomials may adopt values that are not square-free. The last factor will be dealt with by means of a square-free sieve.

2.2 Notation and preliminaries

Let n be a non-zero integer. We write $\tau(n)$ for the number of positive divisors of n, $\omega(n)$ for the number of the prime divisors of n, and $\mathrm{rad}(n)$ for the product of the prime divisors of n. For any $k \geq 2$, we write $\tau_k(n)$ for the number of k-tuples $(n_1, n_2, \ldots, n_k) \in (\mathbb{Z}^+)^k$ such that $n_1 \cdot n_2 \cdot \cdots \cdot n_k = |n|$. Thus $\tau_2(n) = \tau(n)$. We adopt

the convention that $\tau_1(n) = 1$. By $d|n^\infty$ we will mean that $p|n$ for every prime p dividing d. We let

$$\mathrm{sq}(n) = \prod_{p^2|n} p^{v_p(n)-1}.$$

We denote by $\mathfrak{O}_K$ the ring of integers of a global or local field K. We let I_K be the semigroup of non-zero ideals of $\mathfrak{O}_K$. If K is a global field and v is a place of K, we will write $\mathfrak{O}_v$ instead of $\mathfrak{O}_{K_v}$. By a $\mathfrak{p}$-*adic field* we mean a local field of characteristic zero and finite residue field.

Let K be a number field. Let $\mathfrak{a}$ be a non-zero ideal of $\mathfrak{O}_K$. We write $\tau_K(\mathfrak{a})$ for the number of ideals dividing $\mathfrak{a}$, $\omega_K(\mathfrak{a})$ for the number of prime ideals dividing $\mathfrak{a}$, and $\mathrm{rad}_K(\mathfrak{a})$ for the product of the prime ideals dividing $\mathfrak{a}$. Given a positive integer k, we write $\tau_{K,k}(\mathfrak{a})$ for the number of k-tuples $(\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k)$ of ideals of $\mathfrak{O}_K$ such that $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_k$. Thus $\tau_2(\mathfrak{a}) = \tau(\mathfrak{a})$. We let

$$\mathrm{sq}_K(\mathfrak{a}) = \begin{cases} \prod_{\mathfrak{p}^2|\mathfrak{a}} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})-1} & \text{if } \mathfrak{a} \neq 0, \\ 0 & \text{if } \mathfrak{a} = 0, \end{cases}$$

$$\mu_K(\mathfrak{a}) = \begin{cases} \prod_{\mathfrak{p}|\mathfrak{a}} (-1) & \text{if } \mathrm{sq}_K(\mathfrak{a}) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We define $\rho(\mathfrak{a})$ to be the positive integer generating $\mathfrak{a} \cap \mathbb{Z}$.

Let $\mathfrak{a}$, $\mathfrak{b}$ be ideals of $\mathfrak{O}_K$. By $\mathfrak{a}|\mathfrak{b}^\infty$ we mean that $\mathfrak{p}|\mathfrak{b}$ for every prime ideal $\mathfrak{p}$ dividing $\mathfrak{a}$. We write

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \prod_{\mathfrak{p}|\mathfrak{a},\mathfrak{b}} \mathfrak{p}^{\min(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b}))},$$

$$\mathrm{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cdot \mathfrak{b} \cdot (\gcd(\mathfrak{a}, \mathfrak{b}))^{-1}.$$

Throughout, we will say that two polynomials $f, g \in \mathfrak{O}_K[x]$ *have no common factors* if they are coprime as elements of $K[x]$. We will say that $f \in \mathfrak{O}_K[x]$ is *square-free* if there are no polynomials $f_1, f_2 \in K[x]$, $f_1 \notin K$, such that $f = f_1^2 \cdot f_2$.

The same usage will hold for polynomials in two variables: $f, g \in \mathfrak{O}_K[x, y]$ *have no common factors* if they are coprime in $K[x, y]$, and $f \in \mathfrak{O}_K[x, y]$ is *square-free* if it is not of the form $f_1^2 \cdot f_2$, $f_1, f_2 \in K[x]$, $f_1 \in K$.

We define the resultant $\mathrm{Res}(f, g)$ of two polynomials $f, g \in \mathfrak{O}_K[x]$ as the determinant of the corresponding Sylvester matrix:

$$\begin{pmatrix} a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 & 0 \\ 0 & \cdots & 0 & 0 & a_n & a_{n-1} & \cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 \\ 0 & \cdots & 0 & 0 & b_m & b_{m-1} & \cdots & b_1 & b_0 \end{pmatrix} \tag{2.2.1}$$

where we write out $f = \sum_{j=0}^{n} a_j x^j$, $g = \sum_{j=0}^{m} b_i x^i$.

Assume f and g have no common factors. Then $\mathrm{Res}(f, g)$ is a non-zero element of $\mathfrak{O}_K$. Moreover, $\gcd(f(x), g(x)) | \mathrm{Res}(f, g)$ for any integer x. We adopt the convention that the discriminant $\mathrm{Disc}(f)$ equals $\mathrm{Res}(f, f')$.

The resultant of two homogeneous polynomials $f, g \in \mathfrak{O}_K[x, y]$ is also defined as the determinant of the Sylvester matrix (2.2.1), where we write out

$$f = \sum_{j=0}^{n} a_j x^j y^{n-j}, \quad g = \sum_{j=0}^{m} b_i x^i y^{m-i}.$$

Assume f and g have no common factors. Then $\mathrm{Res}(f, g)$ is a non-zero element of $\mathfrak{O}_K$. Moreover, $\gcd(f(x, y), g(x, y)) | \mathrm{Res}(f, g)$ for any coprime integers x, y.

For a homogeneous polynomial $f \in \mathfrak{O}_K[x, y]$ we define

$$\mathrm{Disc}(f) = \mathrm{lcm}\left(\mathrm{Res}\left(f(x,1), \frac{\partial f(x,1)}{\partial x}\right), \mathrm{Res}\left(f(1,y), \frac{\partial f(1,x)}{\partial x}\right)\right).$$

Note that a polynomial $f \in \mathfrak{O}_K[x]$ has a factorization (in general not unique) into polynomials $f_1, \cdots, f_n \in \mathfrak{O}_K[x]$ irreducible in $\mathfrak{O}_K[x]$. In any such factorization, $f_1, \cdots, f_n$ are in fact irreducible in $K[x]$. The same is true for homogeneous polynomials $f \in \mathfrak{O}_K[x, y]$ and factorization into irreducibles in $\mathfrak{O}_K[x, y]$ and $K[x, y]$.

A *lattice* is a subgroup of $\mathbb{Z}^n$ of finite index; a *lattice coset* is a coset of such a subgroup. By the *index* of a lattice coset we mean the index of the lattice of which it is a coset. For any lattice cosets L_1, L_2 with $\gcd([\mathbb{Z}^n : L_1], [\mathbb{Z}^n : L_2]) = 1$, the intersection $L_1 \cap L_2$ is a lattice coset with

$$[\mathbb{Z}^n : L_1 \cap L_2] = [\mathbb{Z}^n : L_1][\mathbb{Z}^n : L_2]. \tag{2.2.2}$$

In general, if L_1, L_2 are lattice cosets, then $L_1 \cap L_2$ is either the empty set or a lattice coset such that

$$\begin{aligned} \mathrm{lcm}([\mathbb{Z}^n : L_1], [\mathbb{Z}^n : L_2]) &\mid [\mathbb{Z}^n : L_1 \cap L_2], \\ [\mathbb{Z}^n : L_1 \cap L_2] &\mid [\mathbb{Z}^n : L_1][\mathbb{Z}^n : L_2]. \end{aligned} \tag{2.2.3}$$

Let L_1, L_2 be lattices in $\mathbb{Z}^2$. Let $m = \mathrm{lcm}([\mathbb{Z}^2 : L_1], [\mathbb{Z}^2 : L_2])$. Let $R = \{(x, y) \in \mathbb{Z}^2 : \gcd(m, \gcd(x, y)) = 1\}$. Then $(R \cap L_1) \cap (R \cap L_2)$ is either the empty set or the intersection of R and a lattice L_3 of index m:

$$[\mathbb{Z}^2 : L_3] = m = \mathrm{lcm}([\mathbb{Z}^2 : L_1], [\mathbb{Z}^2 : L_2]). \tag{2.2.4}$$

For $S \subset [-N, N]^n$ a convex set and $L \subset \mathbb{Z}^n$ a lattice coset,

$$\#(S \cap L) = \frac{\mathrm{Area}(S)}{[\mathbb{Z}^n : L]} + O(N^{n-1}), \tag{2.2.5}$$

where the implied constant depends only on n.

The following lemma will serve us better than (2.2.5) when L is a lattice of index greater than N.

Lemma 2.2.1. *Let L be a lattice of index $[\mathbb{Z}^2 : L] \leq N^2$. Then*

$$\#(\{-N \leq x, y \leq N : \gcd(x, y) = 1\} \cap L) \ll \frac{N^2}{[\mathbb{Z}^2 : L]}.$$

Proof. Let

$$M_0 = \min_{(x,y)\in L} \max(|x|, |y|).$$

By [Gre], Lemma 1,

$$\#([-N, N]^2 \cap L) \ll \frac{N^2}{[\mathbb{Z}^2 : L]} + O\left(\frac{N}{M_0}\right).$$

If $M_0 \geq \frac{[\mathbb{Z}^2:L]}{2N}$ we are done. Assume $M_0 < \frac{[\mathbb{Z}^2:L]}{2N}$. Suppose

$$\#(\{-N \leq x, y \leq N : \gcd(x, y) = 1\} \cap L) > 2.$$

Let (x_0, y_0) be a point such that $\max(|x_0|, |y_0|) = M_0$. Let (x_1, y_1) be a point in $\#(\{-N \leq x, y \leq N : \gcd(x, y) = 1\} \cap L)$ other than (x_0, y_0) and $(-x_0, -y_0)$. Since $\gcd(x_0, y_0) = \gcd(x_1, y_1) = 1$, it cannot happen that 0, (x_0, y_0) and (x_1, y_1) lie on the same line. Therefore we have a non-degenerate parallelogram $(0, (x_0, y_0), (x_1, y_1), (x_0 + x_1, y_0 + y_1))$ whose area has to be at least $[\mathbb{Z}^2 : L]$. On the other hand, its area can be at most $\sqrt{x_0^2 + y_0^2} \cdot \sqrt{x_1^2 + y_1^2} \leq \sqrt{2}M_0 \cdot \sqrt{2}N = 2M_0N$. Since we have assumed $M_0 < \frac{[\mathbb{Z}^2:L]}{2N}$ we arrive at a contradiction. □

By a *sector* we will mean a connected component of a set of the form $\mathbb{R}^n - (T_1 \cap T_2 \cap \cdots \cap T_n)$, where T_i is a hyperplane going through the origin. Every sector S is convex.

Let $x \in \mathbb{R}$ be given. We write $\lfloor x \rfloor$ for the largest integer no greater than x, $\lceil x \rceil$

for the smallest integer no smaller than x, and $\{x\}$ for $x - \lfloor x \rfloor$.

We define [true] to be 1 and [false] to be 0. Thus, for example, $x \mapsto [x \in S]$ is the characteristic function of a set S.

2.3 Pliable Functions

Since this section is devoted to a newly defined class of objects, we might as well start by attempting to give an intuitive sense of their meaning. Take a function $f : \mathbb{Z}_p \to \mathbb{C}$. For f to be *affinely pliable*, it is necessary but not sufficient that f be locally constant almost everywhere. We say that f is *affinely pliable at* 0 if there is an integer $k \geq 0$ such that the value of $f(x)$ depends only on $v_p(x)$ and on $p^{-v_p(x)}x \bmod p^k$. Thus, if, say, $p = 3$ and $k = 1$, each of the following values is uniquely defined:

$$\begin{array}{llllll}
f(\ldots 01_3) & f(\ldots 02_3) & f(\ldots 11_3) & f(\ldots 12_3) & f(\ldots 21_3) & f(\ldots 22_3) \\
f(\ldots 010_3) & f(\ldots 020_3) & f(\ldots 110_3) & f(\ldots 120_3) & f(\ldots 210_3) & f(\ldots 220_3) \\
f(\ldots 0100_3) & f(\ldots 0200_3) & f(\ldots 1100_3) & f(\ldots 1200_3) & f(\ldots 2100_3) & f(\ldots 2200_3) \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

A function f on $\mathbb{Z}_p$ is affinely pliable at $t_1, \ldots, t_n$ if it displays the same behaviour near $t_1, t_2, \ldots, t_n$ as the example above displays near 0. A function f on $\mathbb{R}$ is affinely pliable at $t_1 < \cdots < t_n$ if it is constant on $(-\infty, t_1)$, (t_1, t_2), $\ldots$, (t_n, ∞). A function f on $\mathbb{Q}$ is affinely pliable if it is affinely pliable when seen at finitely many places simultaneously, in a sense to be made precise now.

2.3.1 Definition and basic properties

Definition 4. *Let K be a number field or a $\mathfrak{p}$-adic field. A function f on a subset S of K is said to be* affinely pliable *if there are finitely many triples*

$$(v_j, U_j, t_j)$$

with v_j a place of K, U_j an open subgroup of $K^*_{v_j}$ and t_j an element of K_{v_j} such that $f(t) = f(t')$ for all $t, t' \in S$ such that $t - t_j$ and $t' - t_j$ are non-zero and equal in $K^*_{v_j}/U_j$ for all j.

If K is a $\mathfrak{p}$-adic field, then v_j has no choice but to equal the valuation $v_\mathfrak{p}$ of K. When f is affinely pliable with respect to (v_1, U_1, t_1),...,(v_n, U_n, t_n), we say f is *affinely pliable at t_1,...,t_n.*

Definition 5. *Let K be a number field or a $\mathfrak{p}$-adic field. A function f on a subset of K^n is said to be* pliable *if there are finitely many triples*

$$(v_j, U_j, \vec{q}_j)$$

with v_j a place of K, U_j an open subgroup of $K^*_{v_j}$ and $\vec{q}_j$ an element of $K^n_{v_j} - \{(0, \ldots, 0)\}$ such that $f(x_1, x_2, \cdots, x_n) = f(x'_1, x'_2, \cdots, x'_n)$ whenever the scalar products $\vec{x} \cdot \vec{q}_j$ and $\vec{x}' \cdot \vec{q}_j$ are non-zero and equal in $K^*_{v_j}/U_j$ for all j.

The following are some typical examples of pliable and affinely pliable functions. Let K be a number field or a $\mathfrak{p}$-adic field, v a place of K. Then $t \mapsto v(t)$ is affinely pliable. So are $t \mapsto t \bmod \mathfrak{p}_v$ (defined on $K \cap \mathfrak{O}_{K_v}$) and $t \mapsto t\pi_v^{-v(t)} \bmod \mathfrak{p}_v$ (defined on K^*), where $\mathfrak{p}_v$ is the prime ideal of $\mathfrak{O}_v$ and π_v is a generator of $\mathfrak{p}_v$. If K is a $\mathfrak{p}$-adic field, any continuous character $\chi : K^* \mapsto \mathbb{C}$ is affinely pliable. For any ball $B = \{t \in K : |t - t_0|_v < r\}$, the characteristic function $x \mapsto [x \in B]$ is affinely pliable. An example of a pliable function would be $(x, y) \mapsto v_\mathfrak{p}(3x + 5y)$, or

$(x, y, z) \mapsto \chi(3y - 2x + z)$. A function is affinely pliable at 0 if and only if it is a pliable function on one variable ($n = 1$). Of the examples of affinely pliable functions given above, all are affinely pliable at 0, save for $x \mapsto [x \in B]$, which is affinely pliable at t_0.

It is clear that $g \circ (f_1 \times f_2 \times ... \times f_n)$ is pliable (resp. affinely pliable) for $f_1, f_2, \cdots f_n$ pliable (resp. affinely pliable) and g an arbitrary function whose domain is a subset of the range of $f_1 \times f_2 \times \cdots \times f_n$. Note, in particular, that $f_1 f_2 \cdots f_n$ is pliable (resp. affinely pliable) for $f_1, \ldots, f_n$ pliable. We will now prove that, under certain circumstances, pliability is preserved under composition in the other order: not only is $t \mapsto \chi^3(t) + \chi(t) + 5$ affinely pliable, but $t \mapsto \chi(t^3 + t + 5)$ is affinely pliable as well.

Lemma 2.3.1. *Let K be a number field or a $\mathfrak{p}$-adic field. Let v be a place of K, $f \in K_v(t)$ a rational function and U an open subgroup of K_v^*. Let $t_1, t_2, \ldots, t_n \in K$ be the zeroes and poles of f in K_v. Let $t_0 = 0$. Then there is an open subgroup U_v' of K_v^* such that $f(t)$ is in the same coset rU_v of U_v as $f(t')$ whenever $t - t_j$ and $t' - t_j$ lie in the same coset $r_j U_v$ of U_v for every $0 \leq j \leq m$.*

Proof. We will choose $U_v \subset \mathfrak{O}_{K_v}^*$. If t and t' belong to the same coset of U_v, then $t \in \mathfrak{O}_{K_v}$ implies $t' \in \mathfrak{O}_{K_v}$. For any $t \in K_v$, either $t \in \mathfrak{O}_{K_v}$ or $1/t \in \mathfrak{O}_{K_v}$. Let $\hat{f} \in K_v(t)$ be the rational function taking t to $f(1/t)$. If we prove the statement of the lemma for both f and $\hat{f}$ under the assumption that $t, t' \in \mathfrak{O}_{K_v}$, we will have proven it for any $t, t' \in K_v$. Thus we need consider only $t, t' \in \mathfrak{O}_{K_v}$.

As in Lemma 2.3.4, we can assume f is an irreducible polynomial with integer coefficients. If f is linear, the statement is immediate. Hence we can assume $f \in \mathfrak{O}_{K_v}[t]$, f irreducible, $\deg(f) \geq 2$.

Hensel's lemma implies that $v(f(t)) \leq 2v(\mathrm{Disc}(f))$ for every $t \in \mathfrak{O}_{K_v}$, as the contrary would be enough for $f(x) = 0$ to have a non-trivial solution in K_v. Since U_v is open, it contains a set of the form $1 + \pi^k \mathfrak{O}_{K_v}$, where π is a prime of $\mathfrak{O}_{K_v}$. Set $U_v' = 1 + \pi^{k+2v(\mathrm{Disc}(f))}$. Suppose $t, t' \in \mathfrak{O}_{K_v}$ lie in the same coset of U_v'. Then

$v(t-t') \geq k + 2v(\mathrm{Disc}(f)) + v(t)$. Since v is non-archimedean,

$$|f(t) - f(t')| \leq |t - t'| \leq |\pi|^{k+2\,\mathrm{Disc}(f)+v(t)} \leq |\pi|^{k+f(t)} = |\pi|^k |f(t)|.$$

Therefore $f(t)$ and $f(t')$ lie in the same coset of U_v. □

Proposition 2.3.2. *Let K be a number field or a $\mathfrak{p}$-adic field. Let $f \in K(t)$. Let a function g on $S \subset K$ be affinely pliable. Then $g \circ f$ on $S' = \{t \in K : f(t) \in S\}$ is affinely pliable.*

Proof. Immediate from Definition 4 and Lemma 2.3.1. □

Proposition 2.3.3. *Let K be a number field or a $\mathfrak{p}$-adic field. Let $f_1, \cdots, f_n \in K(t)$. Let a function g on $S \subset K^n$ be pliable. Then the map $t \mapsto g(f_1(t), \cdots, f_n(t))$ on $S' = \{t \in K : (f_1(t), \cdots, f_n) \in S\}$ is affinely pliable.*

Proof. Immediate from Definitions 4 and 5 and Lemma 2.3.1. □

Lemma 2.3.4. *Let K be a number field or a $\mathfrak{p}$-adic field. Let v be a place of K, $F \in K_v[x, y]$ a homogeneous polynomial and U_v an open subgroup of K_v^*. Then there is an open subgroup U_v' of K_v^* and a finite subset $\{\vec{x}_j\}$ of K_v^2 such that $F(x, y)$ is in the same coset rU_v of U_v as $F(x', y')$ whenever $(x, y) \cdot \vec{x}_j$ and $(x', y') \cdot \vec{x}_j$ lie in the same coset $r_j U_v'$ of K_v^* for all j.*

Proof. Suppose that $F = F_1 F_2$ and that the lemma holds for (F_1, v, U_v) and (F_2, v, U_v) with conditions $(U_{v,1}', \{\vec{x}_{i,1}\})$ and $(U_{v,2}', \{\vec{x}_{k,2}\})$, respectively. Set $U_v' = U_{v,1}' \cap U_{v,2}'$ and $\{\vec{x}_j\} = \{\vec{x}_{i,1}\} \cup \{\vec{x}_{k,2}\}$. Assume that $(x, y) \cdot \vec{x}_j$ and $(x', y') \cdot \vec{x}_j$ lie in the same coset of U_v' for all j. Then $F_1(x, y)$ is in the same coset of U_v as $F_1(x', y')$ and $F_2(x, y)$ is in the same coset as $F_2(x', y')$. Hence $F_1(x, y)F_2(x, y)$ is in the same coset as $F_1(x', y')F_2(x', y')$.

We can thus assume that F is irreducible. Suppose F is linear. Write $F(x, y) =$

$ax + by$. Then the lemma holds with $U'_v = U_v$ and $\{\vec{x}_j\} = \{(a, b)\}$. We are left with the case when F is irreducible of degree greater than one.

Suppose v is finite. We can assume $F \in \mathfrak{O}_v[x, y]$. Hensel's Lemma implies that $v(F(x, y)) - (\deg F)\min(v(x), v(y)) \leq 2v(\mathrm{Disc}(F))$ for all $x, y \in K^*$, as the contrary would be enough for $F(x, y) = 0$ to have a non-trivial solution in K_v^2. Since U_v is open, it contains a set of the form $1 + \pi^k\mathfrak{O}_v$, where π is a prime of $\mathfrak{O}_v$. Set $U'_v = 1 + \pi^{k+2v(\mathrm{Disc}(F))}\mathfrak{O}_v$, $\vec{x}_1 = (1, 0)$, $\vec{x}_2 = (0, 1)$. Suppose that (x, y) and (x', y') satisfy the conditions in the lemma, that is, x and x' lie in the same coset of U'_v, and so do y and y'. It follows that $v(x - x') \geq k + 2v(\mathrm{Disc}(F)) + v(x)$ and $v(y - y') \geq k + 2v(\mathrm{Disc}(F)) + v(y)$. Since v is non-archimedean,

$$|F(x, y) - F(x', y')|_v \leq |\pi|^{(\deg(F)-1)\min(v(x),v(y))} \max(|x - x'|_v, |y - y'|_v).$$

Now

$$\begin{aligned}
\max(|x - x'|_v, |y - y'|_v) &= |\pi|_v^{\min(v(x-x'),v(y-y'))} \\
&\leq |\pi|_v^k |\pi|_v^{-(\deg(F)-1)\min(v(x),v(y))} |\pi|^{2v(\mathrm{Disc}(F))+\deg(F)\min(v(x),v(y))} \\
&\leq |\pi|_v^k |\pi|_v^{-(\deg(F)-1)\min(v(x),v(y))} |F(x, y)|_v.
\end{aligned}$$

Thus

$$|F(x, y) - F(x', y')|_v \leq |\pi|^k |F(x, y)|_v.$$

This means that $F(x, y)$ and $F(x', y')$ are in the same coset of U_v.

Suppose now that v is infinite and $F(x, y)$ is irreducible and of degree greater than one. Then the degree of F must be two. We have either $U_v = \mathbb{R}^*$ or $U_v = \mathbb{R}^+$. Since F is either positive definite or negative definite, $F(x, y)$ and $F(x', y')$ lie in the same coset of U_v for any x, y not both zero. Since we are given that x and y are coprime they cannot both be zero. Choose $U'_v = \mathbb{R}^*$, $\{x_j\}$ empty. $\square$

As usual, we write $\vec{e}_1 = (1, 0, \ldots, 0), \vec{e}_2 = (0, 1, \ldots, 0), \ldots, \vec{e}_n = (0, 0, \ldots, 1)$.

Proposition 2.3.5. *Let K be a number field or a $\mathfrak{p}$-adic field. Let $F_1, F_2, \ldots, F_n \in K[x, y]$ be homogeneous polynomials. Let a function f on $S \subset K^n$ be pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}_j$. Suppose $\vec{q}_j \in \{\vec{e}_1, \vec{e}_2, \cdots, \vec{e}_n\}$ for every j. Then $(x, y) \mapsto f(F_1(x, y), F_2(x, y), \cdots, F_n(x, y))$ is a pliable function on*

$$S' = \{(x, y) \in K^2 : (F_1(x, y), \cdots, F_n(x, y)) \in S\}.$$

Proof. Immediate from Definition 5 and Lemma 2.3.4. □

Proposition 2.3.6. *Let K be a number field or a $\mathfrak{p}$-adic field. Let $F_1, F_2, \ldots, F_n \in K[x, y]$ be homogeneous polynomials of the same degree. Let a function f on $S \subset K^n$ be pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}_j$. Then*

$$(x, y) \mapsto f(F_1(x, y), F_2(x, y), \cdots, F_n(x, y))$$

is a pliable function on $S' = \{(x, y) \in K^2 : (F_1(x, y), \cdots, F_n(x, y)) \in S\}$.

Proof. Immediate from Definition 5 and Lemma 2.3.4. □

Lemma 2.3.7. *Let K be a number field or a $\mathfrak{p}$-adic field. Let f be an affinely pliable function on a subset S of K. Then the map*

$$(x, y) \to f(y/x)$$

on $S' = \{(x, y) \in K^2 : y/x \in S\}$ is pliable.

Proof. Say f is affinely pliable with respect to $\{(v_j, U_j, t_j)\}_j$. Let $(x, y), (x', y') \in S'$, be such that $t_j x - y$ and $t_j x' - y'$ belong to the same coset $r_j U_j \subset K^*_{v_k}$ of U_j for every j. Assume furthermore that x and x' belong to the same coset of U_j. Then $y/x - t_j$

and $y'/x' - t_j$ belong to the same coset of U_j for every j. Therefore $(x, y) \to f(y/x)$ is pliable with respect to $\{(v_j, U_j, (t_j, -1))\}_j \cup \{(v_j, U_j, (1, 0))\}_j$. $\square$

Lemma 2.3.8. *Let K be a number field or a $\mathfrak{p}$-adic field. Let f be a pliable function on a subset S of K^2. Then the map*

$$t \mapsto f(1, t)$$

on $S' = \{t \in K : (1, t) \in S\}$ is affinely pliable.

Proof. Say f is pliable with respect to $\{v_j, U_j, (q_{j1}, q_{j2})\}_{j \in J}$. Let $t, t' \in S$ be such that $t + q_{j1}/q_{j2}$ and $t' + q_{j1}/q_{j2}$ belong to the same coset $r_j U_j \subset K_{v_j}^*$ of U_j for every j such that $q_{j2} \neq 0$. Then $q_{j1} + q_{j2}t$ and $q_{j1} + q_{j2}t'$ belong to the same coset $r_j U_j \subset K_{v_j}^*$ of U_j for every j. Therefore $t \mapsto f(1, t)$ is affinely pliable with respect to $\{(v_j, U_j, -q_{j1}/q_{j2})\}_{j \in J'}$, where $J' = \{j \in J : q_{j2} \neq 0\}$. $\square$

Lemma 2.3.9. *If K is a number field or a $\mathfrak{p}$-adic field, L a finite extension of K, and f a pliable function on a subset S of L^n, then $f|(S \cap K^n)$ is pliable as a function on the subset $S \cap K^n$ of K^n. If K is a number field or a $\mathfrak{p}$-adic field, L a finite extension of K, and f an affinely pliable function on a subset S of L, then $f|(S \cap K)$ is affinely pliable as a function on the subset $S \cap K$ of K.*

Proof. The intersection of K and an open subgroup of L^* is an open subgroup of K^*. $\square$

Lemma 2.3.10. *Let f be a pliable function on a subset S of $\mathbb{Z}^2$. Let m be a positive integer. Then*

$$(x, y) \mapsto f\left(\frac{x}{\gcd(x, y, m)}, \frac{y}{\gcd(x, y, m)}\right)$$

is a pliable function on $S' = \{(x, y) \in \mathbb{Z}^2 : (x/\gcd(x, y, m), y/\gcd(x, y, m)) \in S\}$.

Proof. Suppose f is pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}_{j\in J}$. Then

$$(x, y) \mapsto f\left(\frac{x}{\gcd(x, y, m)}, \frac{y}{\gcd(x, y, m)}\right)$$

is pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}_{j\in J} \cup \{(v_{\mathfrak{p}}, \mathfrak{O}_{K_{\mathfrak{p}}}, (1, 0))\}_{\mathfrak{p}|m} \cup \{(v_{\mathfrak{p}}, \mathfrak{O}_{K_{\mathfrak{p}}}, (0, 1))\}_{\mathfrak{p}|m}$.

□

Lemma 2.3.11. *Let K be a number field or a $\mathfrak{p}$-adic field. Let f be a pliable function from $X \subset K^n$ to Y (resp. an affinely pliable function from $X \subset K$ to Y). Let $x_0 \in K^n - X$ (resp. $x_0 \in K - X$), $y_0 \in Y$. Define $f' : S \cup \{x_0\} \to Y$ by*

$$f'(x) = \begin{cases} f(x) & \text{if } x \in S, \\ y_0 & \text{if } x = x_0. \end{cases}$$

Then f is pliable (resp. affinely pliable).

Proof. If f is pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}_j$ (resp. aff. pliable with respect to $\{(v_j, U_j, t_j)\}_j$) then f' is pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}_j \cup \{(v, K, \vec{v})\}$, where v is an arbitrary place of K and $\vec{v}$ is any vector orthogonal to x_0 (resp. aff. pliable with respect to $\{(v_j, U_j, t_j)\}_j \cup \{(v, K, x_0)\}$, where v is an arbitrary place of K). □

Lemma 2.3.12. *Let f be an affinely pliable function on $\mathbb{Z}$. Then there are integers a, m and t_0, $m > 0$, such that f is constant on the set $\{t \in \mathbb{Z} : t \equiv a \bmod m,\ t > t_0\}$.*

Proof. Immediate from Definition 4. □

Lemma 2.3.13. *Let f be a pliable function on $\mathbb{Z}^2$. Then there are a lattice $L \subset \mathbb{Z}^2$ and a sector $S \subset \mathbb{R}^2$ such that f is constant on $L \cap S$.*

Proof. Immediate from Definition 5. □

2.3.2 Pliability of local root numbers

Let E be an elliptic curve over a field K. Given an extension L/K, we write $E(L)$ for the set of L-rational points of E. We define $E[m] \subset E(\overline{K})$ to be the set of points of order m on E. We write $K(E[m])$ for the minimal subextension of K over which all elements of $E[m]$ are rational. The extension $K(E[m])/K$ is always finite and Galois.

Write $\widetilde{K}$ for the maximal unramified extension of a local field K.

Lemma 2.3.14. *Let K be a $\mathfrak{p}$-adic field. Let E be an elliptic curve over K with potential good reduction. Then there is a minimal algebraic extension L of $\widetilde{K}$ over which E acquires good reduction. Moreover, $L = \widetilde{K}(E[m])$ for all $m \geq 3$ prime to the characteristic of the residue field of K.*

Proof. See [ST], Section 2, Corollary 3. □

Lemma 2.3.15. *Let K be a $\mathfrak{p}$-adic field. Then there is a finite extension $K'/\widetilde{K}$ such that every elliptic curve over K with potential good reduction acquires good reduction over K'.*

Proof. We can check directly from the explicit formulas for the group law (see e.g. [Si], Chap III, 2.3) that $K(E[3])/K$ is an extension of degree at most 6 and $K(E[4])/K$ is an extension of degree at most 12. Since K is a $\mathfrak{p}$-adic field, it has only finitely many extensions of given degree (see e.g. [La], II, §5, Prop. 14). Let K_{12}/K be the composition of all extensions of K of degree at most 12. Since K_{12}/K is the composition of finitely many finite extensions, it is itself a finite extension. By Lemma 2.3.14, every elliptic curve over K with potential good reduction acquires good reduction over $L = K_{12} \cdot \widetilde{K}$. Since K_{12}/K is a finite extension, $L/\widetilde{K}$ is a finite extension. □

Lemma 2.3.16. *Let K be a local field of ramification degree e over $\mathbb{Q}_p$. Let π be a prime of K. Then the reduction* $\bmod \mathfrak{p}$ *of an elliptic curve E over K depends only*

on

$$c_4 \cdot \pi^{-4\min(\lfloor v(c_4)/4\rfloor, \lfloor v(c_6)/6\rfloor, \lfloor v(\Delta)/12\rfloor)} \bmod \mathfrak{p}^{5e+1},$$

$$c_6 \cdot \pi^{-6\min(\lfloor v(c_4)/4\rfloor, \lfloor v(c_6)/6\rfloor, \lfloor v(\Delta)/12\rfloor)} \bmod \mathfrak{p}^{5e+1},$$

where c_4, c_6 and Δ are any choice of parameters for E.

Proof. Let k be the residue field of K. Let E be an elliptic curve over K with parameters $c_4, c_6, \Delta \in K$. Let

$$c_4' = c_4 \cdot \pi^{-4\min(\lfloor v(c_4)/4\rfloor, \lfloor v(c_6)/6\rfloor, \lfloor v(\Delta)/12\rfloor)},$$

$$c_6' = c_6 \cdot \pi^{-6\min(\lfloor v(c_4)/4\rfloor, \lfloor v(c_6)/6\rfloor, \lfloor v(\Delta)/12\rfloor)}.$$

Suppose $\mathrm{char}(k) \neq 2, 3$. Then a minimal Weierstrass equation for E is given by

$$y^2 = x^3 - \frac{c_4'}{48} - \frac{c_6'}{864}.$$

Both $\frac{-c_4'}{48}$ and $\frac{-c_6'}{864}$ are integral. The reduction $\bmod \mathfrak{p}$ is simply

$$y^2 = x^3 - (c_4' \cdot 48^{-1} \bmod \mathfrak{p}) - (c_6' \cdot 864^{-1} \bmod \mathfrak{p}).$$

This depends only on $c_4', c_6' \bmod \mathfrak{p}$.

Consider now $\mathrm{char}(k) = 2, 3$. Let m be the smallest positive integer such that there are $r, s, t \in K$, $u \in \mathfrak{O}_K^*$, for which the equation

$$(u^3y' + su^2x' + t)^2 = (u^2x' + r)^3 - \frac{\pi^{4m}c_4'}{48}(u^2x' + r) - \frac{\pi^{6m}c_6'}{864} \tag{2.3.1}$$

has integral coefficients when expanded on x' and y'. (Clearly $m \leq e$.) Then, for m and any choice of $r, s, t \in K$, $u \in \mathfrak{O}_K^*$, giving integral coefficients, (2.3.1) is a minimal Weierstrass equation for E, and its reduction $\bmod \mathfrak{p}$ gives us the reduction $E \bmod \mathfrak{p}$.

By [Si], III, Table 1.2, $r, s, t \in K$, $u \in \mathfrak{O}_K^*$ can give us integral coefficients only if $3r, s, t \in \mathfrak{O}_K$ (if $\mathrm{char}(k) = 3$) or $2r, s, 2t \in \mathfrak{O}_K$ (if $\mathrm{char}(k) = 2$). Thus, both the

existence of (2.3.1) and its coefficients $\bmod \mathfrak{p}$ depend only on $\frac{c_4'}{2\cdot 3\cdot 48}, \frac{c_6'}{864} \bmod \mathfrak{p}$. Since c_4' and c_6' are integral, $\frac{c_4'}{2\cdot 3\cdot 48}, \frac{c_6'}{864} \bmod \mathfrak{p}$ depend only on $c_4' \bmod \mathfrak{p}^{5e+1}$ and $c_6' \bmod \mathfrak{p}^{5e+1}$ (if $\mathrm{char}(k) = 2$) or on $c_4' \bmod \mathfrak{p}^{2e+1}$ and $c_6' \bmod \mathfrak{p}^{3e+1}$ (if $\mathrm{char}(k) = 3$). The statement follows. □

Lemma 2.3.17. *Let K be a $\mathfrak{p}$-adic field of ramification degree e over $\mathbb{Q}_p$. Let L be an extension of K of finite ramification degree over K. Let $\mathfrak{p}_K$ be the prime ideal of K, $\mathfrak{p}_L$ the prime ideal of L. Then the reduction mod $\mathfrak{p}_L$ of an elliptic curve E defined over K depends only on K, L, $v_K(c_4)$, $v_K(c_6)$, $v_K(\Delta)$, $c_4 \cdot (1 + \mathfrak{O}_K \mathfrak{p}_K^{5e+1})$ and $c_6 \cdot (1 + \mathfrak{O}_K \mathfrak{p}_K^{5e+1})$, where c_4, c_6 and Δ are any choice of parameters for E.*

Proof. Let e' be the ramification degree of L over K. Let π_L be a prime of L, $\pi_K = \pi_L^{e'}$ a prime of K. By Lemma 2.3.16, the reduction $E \bmod \mathfrak{p}_L$ depends only on $c_4' \bmod \mathfrak{p}_L^{5ee'+1}$ and $c_6' \bmod \mathfrak{p}_L^{5ee'+1}$, where

$$c_4' = c_4 \cdot \pi_L^{-4\min(\lfloor v_L(c_4)/4\rfloor, \lfloor v_L(c_6)/6\rfloor, \lfloor v_L(\Delta)/12\rfloor)}$$
$$c_6' = c_6 \cdot \pi_L^{-6\min(\lfloor v_L(c_4)/4\rfloor, \lfloor v_L(c_6)/6\rfloor, \lfloor v_L(\Delta)/12\rfloor)}.$$

Since $4[v_L(c_4)/4] \le v_L(c_4) = e' v_K(c_4)$ and $6[v_L(c_4)/6] \le v_L(c_6) = e' v_K(c_6)$, we can tell $c_4' \bmod \mathfrak{p}_L^{5ee'+1}$ and $c_6' \bmod \mathfrak{p}_L^{5ee'+1}$ from $v_L(c_4)$, $v_L(c_6)$, $v_L(\Delta)$,

$$c_4 \cdot \pi_L^{-e' v_K(c_4)} \bmod \mathfrak{p}_L^{5ee'+1} \text{ and}$$
$$c_6 \cdot \pi_L^{-e' v_K(c_6)} \bmod \mathfrak{p}_L^{5ee'+1}.$$

(Either of the last two may not be defined, but we can tell as much from whether $v_L(c_4)$ and $v_L(c_6)$ are finite.) Since $v_L(c_4) = e' v_K(c_4)$, $v_L(c_6) = e' v_K(c_6)$, $v_L(\Delta) = e' v_K(\Delta)$, $\pi_K = \pi_L^{e'}$ and $\mathfrak{p}_K = \mathfrak{p}_L^{e'}$, it is enough to know $v_K(c_4)$, $v_K(c_6)$, $v_K(\Delta)$, $c_4 \cdot \pi^{-v_K(c_4)} \bmod \mathfrak{p}^{5e+1}$ and $c_6 \cdot \pi^{-v_K(c_6)} \bmod \mathfrak{p}^{5e+1}$. The statement follows immediately. □

Lemma 2.3.18. *Let K be a Henselian local field. Let k be the residue field of K. Let $m \ge 2$ be an integer prime to* $\mathrm{char}(k)$. *Let E be an elliptic curve defined over K*

with good reduction at $\mathfrak{p}_K$; denote its reduction by $\widehat{E}$. Then the natural map

$$E[m] \to \widehat{E}[m]$$

is bijective.

Proof. The map is injective by [Si], Ch. VII, Prop. 3.1(b). It remains to show that it is surjective. We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(\overline{K}) & \xrightarrow{f_1} & E(\overline{K}) & \xrightarrow{f_2} & \widehat{E}(\overline{k}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \downarrow{\scriptstyle \cdot m} & & \\ 0 & \longrightarrow & E_1(\overline{K}) & \xrightarrow{f_1} & E(\overline{K}) & \xrightarrow{f_2} & \widehat{E}(\overline{k}) & \longrightarrow & 0, \end{array}$$

where $E_1(\overline{K})$ is the set of points on $E(\overline{K})$ reducing to 0. Let x be an element of $\widehat{E}[m]$. Let $y \in f_2^{-1}(\{x\})$. Let $z \in f_1^{-1}(\{m \cdot y\})$. By [Si], Ch. VII, Prop. 2.2 and Ch. IV, Prop. 2.3(b), the map $E_1(\overline{K}) \xrightarrow{\cdot m} E_1(\overline{K})$ is surjective. Choose $w \in E_1(\overline{K})$ such that $mw = z$. Then $m \cdot f_1(w) = f_1(m \cdot w) = f_1(z) = m \cdot y$. Hence $m \cdot (y - f_1(w)) = 0$. Since $f_2 \circ f_1 = 0$, $f_2(y - f_1(w)) = f_2(y) = x$. Thus $(y - f_1(w))$ is an element of $E(\overline{K})[m]$ mapping to x. $\square$

Lemma 2.3.19. *Let K be a $\mathfrak{p}$-adic field. Let L be a finite Galois extension of $\widetilde{K}$. Let E_1, E_2 be elliptic curves over K with good reduction over L. Suppose that E_1 and E_2 reduce to the same curve over the residue field of L. Then $W_{\mathfrak{p}}(E_1) = W_{\mathfrak{p}}(E_2)$.*

Proof. Let p be the characteristic of the residue field of K. Let k and l be the residue fields of K and L, respectively. The root number $W_{\mathfrak{p}}(E)$ of an elliptic curve E over K is determined by the canonical representation of the Weil-Deligne group $\mathcal{W}'(\overline{K}/K)$ on the Tate module $T_\ell(E)$, where ℓ is any prime different from p. If E has potential good reduction, we can consider the Weil group $\mathcal{W}(\overline{K}/K)$ together with its natural representation on $T_\ell(E)$ instead of the Weil-Deligne group and its representation.

Now let E have good reduction over L. Let $\mathfrak{q}$ be the prime ideal of L. The natural

map f from $E[\ell^n]$, $n \geq 1$, to $(E \bmod \mathfrak{q})[\ell^n]$ commutes with the natural actions of $\mathcal{W}(\overline{K}/K)$ on $E[\ell^n]$ and on $(E \bmod \mathfrak{q})[\ell^n]$. By Lemma 2.3.18, f is bijective. Hence the action of $\mathcal{W}(\overline{K}/K)$ on $E[\ell^n]$ is given by the action of $\mathcal{W}(\overline{K}/K)$ on $(E \bmod \mathfrak{q})[\ell^n]$. Since l is algebraically closed, $(E \bmod \mathfrak{q})[\ell^n]$ is a subset of $E \bmod \mathfrak{q}$. Therefore, the action of $W(\overline{K}/K)$ on $E[\ell^n]$ is given by the action of $W(\overline{K}/K)$ on $E \bmod \mathfrak{q}$. The action of $\mathcal{W}(\overline{K}/K)$ on

$$T_\ell(E) = \lim_{\leftarrow} E[\ell^n]$$

is thus given by its action on $E \bmod \mathfrak{q}$.

Therefore, if E_1 and E_2 have the same reduction $\bmod \mathfrak{q}$, they have the same local root number $W_\mathfrak{p}(E_1) = W_\mathfrak{p}(E_1)$. □

Lemma 2.3.20. *Let K be a $\mathfrak{p}$-adic field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let S be the set of all $t \in K$ such that $\mathcal{E}(t)$ is an elliptic curve over K with potential good reduction. Then the map*

$$t \mapsto W_\mathfrak{p}(\mathcal{E}(t))$$

on S is affinely pliable.

Proof. Let $K'/\widetilde{K}$ be as in Lemma 2.3.15. Let $L/\widetilde{K}$ be the Galois closure of $K'/\widetilde{K}$. Since $L/\widetilde{K}$ is the Galois closure of a finite extension, it is itself a finite extension. The statement then follows immediately from Lemmas 2.3.17 and 2.3.19. □

Lemma 2.3.21. *Let K be a $\mathfrak{p}$-adic field. Let E be an elliptic curve over K given by $c_4, c_6 \in K$. Assume E has potentially multiplicative reduction. Then*

$$W_\mathfrak{p}(E) = \left(\frac{-1}{p}\right) \qquad \text{if } E \text{ has additive reduction over } K,$$

$$W_\mathfrak{p}(E) = -\left(\frac{-c_6(E)\pi^{-v(c_6(E))}}{\mathfrak{p}}\right) \qquad \text{if } E \text{ has multiplicative reduction over } K,$$

where π is any prime element of K.

Proof. This is a classical result that we will translate from the terms presented in [Ro], Section 19. The statement there is as follows. If E has additive reduction over K, then $W_{\mathfrak{p}} = \chi(-1)$, where χ is the ramified character of K^*. If E has multiplicative reduction over K, then

$$W_{\mathfrak{p}} = \begin{cases} -1 & \text{if } E \text{ has split multiplicative reduction,} \\ 1 & \text{if } E \text{ has non-split multiplicative reduction.} \end{cases}$$

Suppose E has additive reduction over K. Since $v_K(-1) = 0$, $\chi(-1)$ equals $\left(\frac{-1}{\mathfrak{p}}\right)$ and we are done.

Suppose that E has multiplicative reduction over K and $\mathfrak{p}$ does not lie over 2. Then the reduced curve $E \bmod \mathfrak{p}$ has an equation of the form

$$y^2 = x^3 + ax^2, \quad a \in (\mathfrak{O}_K/\mathfrak{p})^*$$

(see, e.g., [Si], App. A, Prop. 1.1). The tangents of the curve at the node $(x, y) = (0, 0)$ are $\pm\sqrt{a}$. Thus, the reduction is split if and only if a is a square. Since the parameter $\overline{c}_6$ of $E \bmod \mathfrak{p}$ equals $-64a^3$, we have that a is a square if and only if $\left(\frac{-\overline{c}_6}{\mathfrak{p}}\right) = 1$. Now $\overline{c}_6$ is the reduction $\bmod \mathfrak{p}$ of the parameter c_6' of a minimal Weierstrass equation for E. Since E has multiplicative reduction, we can take $c_6' = c_6 \cdot \pi^{-v_{\mathfrak{p}}(c_6)}$. (Notice that $v_{\mathfrak{p}}$ is even, and thus the choice of π is irrelevant.) The statement follows immediately.

Suppose that E has multiplicative reduction over K and $\mathfrak{p}$ lies over 2. Then every element of $\mathfrak{O}_K/\mathfrak{p}$ is a square, and thus (a) the reduction must be split, and (b) $\left(\frac{-c_6(E)\pi^{-v(c_6(E))}}{\mathfrak{p}}\right) = 1$. The statement follows. $\square$

Lemma 2.3.22. *Let K be a $\mathfrak{p}$-adic field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let S be the set of all $t \in K$ such that $\mathcal{E}(t)$ is an elliptic curve over K with potential*

multiplicative reduction. Then the map

$$t \mapsto W_{\mathfrak{p}}(t)$$

on S is affinely pliable.

Proof. For $t \in S$, the curve $\mathcal{E}(t)$ has multiplicative reduction over K if and only if $v(c_6(\mathcal{E}(t)))$ is divisible by 6. If $\mathcal{E}(t)$ has multiplicative reduction over K, its root number

$$W_{\mathfrak{p}}(E) = -\left(\frac{-c_6(E)\pi^{-v(c_6(E))}}{\mathfrak{p}}\right)$$

depends only on the coset $c_6(\mathcal{E}(t)) \cdot (1 + \pi\mathfrak{O}_K)$. If $\mathcal{E}(t)$ has additive reduction over K, its root number equals the constant $\left(\frac{-1}{\mathfrak{p}}\right)$.

Therefore $W_{\mathfrak{p}}(\mathcal{E}(t))$ depends only on the coset of $c_6(\mathcal{E}(t)) \cdot (1 + \pi\mathfrak{O}_K)$ in which $c_6(\mathcal{E}(t))$. By Proposition 2.3.2 it follows that $W_{\mathfrak{p}}(\mathcal{E}(t))$ is affinely pliable. □

Lemma 2.3.23. *Let K be a $\mathfrak{p}$-adic field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. For $t \in K$, let*

$$f_1(t) = [\mathcal{E}(t) \textit{ has potential good reduction}],$$

$$f_2(t) = [\mathcal{E}(t) \textit{ has potential multiplicative reduction}],$$

$$f_3(t) = [\mathcal{E}(t) \textit{ is singular}].$$

Then $f_1, f_2, f_3 : K \to \{0, 1\}$ are affinely pliable.

Proof. Since $\mathcal{E}(t)$ is singular for finitely many $t \in K$, f_1 is affinely pliable. If $\mathcal{E}(t)$ is non-singular, then $\mathcal{E}(t)$ has potential multiplicative reduction if and only if $v(j(\mathcal{E}(t))) > 0$. Thus, for all but finitely many t, both $f_2(t)$ and $f_3(t)$ depend only on $v(j(\mathcal{E}(t)))$. By Proposition 2.3.2, f_2 and f_3 are affinely pliable. □

Proposition 2.3.24. *Let K be a $\mathfrak{p}$-adic field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Then the map*

$$t \mapsto W_{\mathfrak{p}}(\mathcal{E}(t))$$

on K is affinely pliable.

Proof. Immediate from Lemmas 2.3.20, 2.3.22 and 2.3.23. □

Proposition 2.3.25. *Let K be a number field. Let $\mathfrak{p} \in I_K$ be a prime ideal. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Then the map*

$$t \mapsto W_{\mathfrak{p}}(\mathcal{E}(t))$$

on K is affinely pliable.

Proof. Denote by $\mathcal{E}_{\mathfrak{p}}$ be the elliptic curve over $K_{\mathfrak{p}}(t)$ defined by the same equation as $\mathcal{E}$. For $t \in K$, the elliptic curve $\mathcal{E}_{\mathfrak{p}}(t)$ is the localization $(\mathcal{E}(t))_{\mathfrak{p}}$ of $\mathcal{E}(t)$ at $\mathfrak{p}$. The local root number $W_{\mathfrak{p}}(E)$ of an elliptic curve over K is by definition equal to the root number $W_{\mathfrak{p}}(E_{\mathfrak{p}})$ of the localization $E_{\mathfrak{p}}$ of E at $\mathfrak{p}$. By Proposition 2.3.24, $t \mapsto W_{\mathfrak{p}}(\mathcal{E}_{\mathfrak{p}}(t))$ is an affinely pliable map on $K_{\mathfrak{p}}$. Therefore, its restriction

$$t \mapsto W_{\mathfrak{p}}(\mathcal{E}_{\mathfrak{p}}(t)) = W_{\mathfrak{p}}((\mathcal{E}(t))_{\mathfrak{p}}) = W_{\mathfrak{p}}(\mathcal{E}(t))$$

to K is an affinely pliable map on K. □

2.3.3 Pliable functions and reciprocity

For the following it will be convenient to work in a slightly more abstract fashion. Let K be a number field. Let $\mathcal{C}_i$, $i \geq 0$, be a multiplicatively closed set of functions from $\mathfrak{O}_K^i$ to a multiplicative abelian group $\mathcal{G}$. Let $\mathcal{D}$ be a multiplicatively closed set of functions from $\mathfrak{O}_K^2$ to $\mathcal{G}$ such that $(x, y) \mapsto f(F_1(x, y), \ldots, F_n(x, y))$ belongs to $\mathcal{D}$ for any $f \in \mathcal{C}_n$ and any homogeneous polynomials $F_1, \ldots, F_n \in \mathfrak{O}_K[x, y]$.

We want to define a family of operators $[,]$ that we may manipulate much like reciprocity symbols. Consider a function $[,]_{\mathfrak{d}} : \{(x, y) \in (\mathfrak{O}_K - \{0\})^2 : \gcd(x, y) | \mathfrak{d}^\infty\} \to \mathcal{G}$ for every non-zero ideal $\mathfrak{d} \in I_K$. Assume that $[,]_{\mathfrak{d}}$ satisfies the following conditions:

1. $[ab, c]_{\mathfrak{d}} = [a, c]_{\mathfrak{d}} \cdot [b, c]_{\mathfrak{d}}$,

2. $[a, bc]_{\mathfrak{d}} = [a, b]_{\mathfrak{d}} \cdot [a, c]_{\mathfrak{d}}$,

3. $[a, b]_{\mathfrak{d}} = [a + bc, b]_{\mathfrak{d}}$ provided that $a + bc \neq 0$,

4. $[a, b]_{\mathfrak{d}} = f_{\mathfrak{d}}(a, b) \cdot [b, a]_{\mathfrak{d}}$, where $f_{\mathfrak{d}}$ is a function in $\mathcal{C}_2$,

5. $[a, b]_{\mathfrak{d}} = f_{\mathfrak{d},b}(a)$, where $f_{\mathfrak{d},b}$ is a function in $\mathcal{C}_1$,

6. $[a, b]_{\mathfrak{d}_1} = f_{\mathfrak{d}_1,\mathfrak{d}_2}(a, b)[a, b]_{\mathfrak{d}_2}$ for $\mathfrak{d}_1|\mathfrak{d}_2$, where f is a function in $\mathcal{C}_2$.

Proposition 2.3.26. *Let $F, G \in \mathfrak{O}_K[x, y]$ be homogeneous polynomials without common factors. Let $\mathfrak{d}$ be a non-zero ideal of $\mathfrak{O}_K$ such that $\gcd(F(x, y), G(x, y))|\mathfrak{d}^\infty$ for all coprime $x, y \in \mathfrak{O}_K$. Then there is a function f in $\mathcal{D}$ such that*

$$[F(x, y), G(x, y)]_{\mathfrak{d}} = f(x, y)[x, y]_1^{(\deg F)(\deg G)}$$

for all but finitely many elements (x, y) of $\{(x, y) \in (\mathfrak{O}_K - \{0\})^2 : \gcd(x, y) = 1\}$.

Proof. If $\deg(G) = 0$ the result follows from condition (5). If $\deg(F) = 0$ the result follows from (4) and (5). If F and G is reducible, the statement follows by (1) or (2) from cases with lower $\deg(F) + \deg(G)$. If F is irreducible and $G = cx$, c non-zero, then by (1), (2), (3) and (4),

$$\begin{aligned}
[F(x, y), G(x, y)]_{\mathfrak{d}} &= [a_0x^k + a_1x^{k-1}y + \cdots + a_ky^k, cx]_{\mathfrak{d}} \\
&= [F(x, y), c]_{\mathfrak{d}} \cdot [a_ky^k, x]_{\mathfrak{d}} \\
&= [F(x, y), c]_{\mathfrak{d}} \cdot [a_k, x]_{\mathfrak{d}} \cdot [y, x]_{\mathfrak{d}}^k \\
&= [F(x, y), c]_{\mathfrak{d}} \cdot [a_k, x]_{\mathfrak{d}} \cdot f_{\mathfrak{d}}^{-k}(x, y)g_{1,\mathfrak{d}}^k(x, y)[x, y]_1^k
\end{aligned}$$

for some $f_{\mathfrak{d}}, g_{1,\mathfrak{d}} \in \mathcal{C}$, and the result follows from (5), the definition of $\mathcal{D}$ and the already treated case of $[\text{constant}, x]_{\mathfrak{d}}$. The same works for F irreducible, $G = cy$.

The case of G irreducible, $F = cx$ or cy follows from (4) and the foregoing. For F, G irreducible, $\deg(F) < \deg(G)$, we apply (4). We are left with the case of F, G irreducible, $F, G \neq cx, cy$, $\deg(F) \geq \deg(G)$. Write $F = a_0x^k + \cdots + a_ky^k$, $G = b_0x^l + b_1x^{l-1}y + \cdots + b_ly^l$. Then

$$\begin{aligned}
[F(x,y), G(x,y)]_{\mathfrak{d}} &= f_{\mathfrak{d},b_0\mathfrak{d}}(x,y)[F(x,y), G(x,y)]_{\mathfrak{d}b_0} \\
&= f_{\mathfrak{d},b_0\mathfrak{d}}(x,y)[b_0, G(x,y)]_{b_0\mathfrak{d}}[b_0F(x,y), G(x,y)]_{b_0\mathfrak{d}} \\
&= f_{\mathfrak{d},b_0\mathfrak{d}}(x,y)[b_0, G(x,y)]_{b_0\mathfrak{d}}[b_0F(x,y) - a_0G(x,y), G(x,y)]_{b_0\mathfrak{d}}
\end{aligned}$$

for all coprime x, y such that $b_0F(x,y) - a_0G(x,y) \neq 0$. (Since $b_0F(x,y) - a_0G(x,y)$ is a non-constant homogeneous polynomial, there are only finitely many such pairs (x,y).) The coefficient of x^k in $b_0F(x,y) - a_0G(x,y)$ is zero. Hence $b_0F(x,y) - a_0G(x,y)$ is a multiple of y. Either it is reducible or it is a constant times y. Both cases have already been considered. $\square$

Now let $\mathcal{G}$ be the group $\{-1, 1\}$, $\mathcal{C}_1$ the set of pliable functions on $\mathfrak{O}_K$, $\mathcal{C}_2$ the set of pliable functions on $\mathfrak{O}_K^2$ with $\vec{q}_j \in \{(1,0),(0,1)\}$ for every j and $\mathcal{D}$ the set of pliable functions on $\mathfrak{O}_K^2$. Let

$$[a,b]_{\mathfrak{d}} = \prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)}, \tag{2.3.2}$$

where $\left(\frac{\cdot}{\mathfrak{p}}\right)$ is the quadratic reciprocity symbol. The defining condition on $\mathcal{D}$ holds by Proposition 2.3.5. Properties (1), (2) and (3) are immediate. Property (5) follows immediately from the fact that $\left(\frac{a}{\mathfrak{p}}\right)$ depends on a only as an element of $K^*/(K^*)^2$; clearly $(K^*)^2$ is an open subgroup of K^*. It remains to prove (4) and (6).

Lemma 2.3.27. *Given a non-zero ideal $\mathfrak{d}$ of $\mathfrak{O}_K$, there is a pliable function f on $\mathfrak{O}_K^2$*

with $q_j \in \{(1,0),(0,1)\}$ *such that*

$$\prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} = f(a,b) \prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{b}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)}$$

for all non-zero $a, b \in \mathfrak{O}_K$ *with* $\gcd(a,b)|\mathfrak{d}$.

Proof. Let $\left(\frac{a,b}{\mathfrak{p}}\right)$ be the quadratic Hilbert symbol. For a, b coprime,

$$\prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} = \prod_{\substack{\mathfrak{p}\nmid 2\mathfrak{d}\\ \mathfrak{p}|b}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} = \prod_{\substack{\mathfrak{p}\nmid 2\mathfrak{d}\\ \mathfrak{p}|b\\ \mathfrak{p}\nmid a}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} = \prod_{\substack{\mathfrak{p}\nmid 2\mathfrak{d}\\ \mathfrak{p}|b\\ \mathfrak{p}\nmid a}} \left(\frac{b,a}{\mathfrak{p}}\right) = \prod_{\substack{\mathfrak{p}\nmid 2\mathfrak{d}\\ \mathfrak{p}|b\\ \mathfrak{p}\nmid a}} \left(\frac{a,b}{\mathfrak{p}}\right).$$

Similarly

$$\prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{b}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)} = \prod_{\substack{\mathfrak{p}\nmid 2\mathfrak{d}\\ \mathfrak{p}|a\\ \mathfrak{p}\nmid b}} \left(\frac{a,b}{\mathfrak{p}}\right).$$

Hence

$$\begin{aligned}\prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)} \prod_{\mathfrak{p}\nmid 2\mathfrak{d}} \left(\frac{b}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(a)} &= \prod_{\substack{\mathfrak{p}\nmid 2\mathfrak{d}\\ \mathfrak{p}|ab}} \left(\frac{a,b}{\mathfrak{p}}\right) = \prod_{\substack{\mathfrak{p}\nmid 2\\ \mathfrak{p}\nmid b \text{ or } \mathfrak{p}\nmid ab}} \left(\frac{a,b}{\mathfrak{p}}\right)\\ &= \left(\frac{a,b}{\infty}\right)\left(\frac{a,b}{2}\right) \prod_{\mathfrak{p}|\gcd(\mathfrak{d},ab)} \left(\frac{a,b}{\mathfrak{p}}\right).\end{aligned}$$

Now note that $\left(\frac{a,b}{\mathfrak{p}}\right)$ and $\left(\frac{a,b}{\infty}\right)$ are pliable on $(\mathfrak{O}_K - \{0\})^2$ with

$$\{(v_j, U_j, \vec{q}_j)\} = \{(v, (K^*)^2, (1,0)), (v, (K^*)^2, (0,1))\}.$$

Therefore

$$\left(\frac{a,b}{\infty}\right)\left(\frac{a,b}{2}\right) \prod_{\mathfrak{p}|\gcd(\mathfrak{d},ab)} \left(\frac{a,b}{\mathfrak{p}}\right)$$

is pliable on $\{\mathfrak{O}_K - \{0\}\}^2$ with $q_j \in \{(1,0),(0,1)\}$. Set

$$f(a,b) = \left(\frac{a,b}{\infty}\right)\left(\frac{a,b}{2}\right)\prod_{\mathfrak{p}|\gcd(\mathfrak{d},ab)}\left(\frac{a,b}{\mathfrak{p}}\right)$$

□

Lemma 2.3.28. *Given non-zero $\mathfrak{d}_1$, $\mathfrak{d}_2$ with $\mathfrak{d}_1|\mathfrak{d}_2$, there is a pliable function f such that*

$$\prod_{\mathfrak{p}\nmid 2\mathfrak{d}_1}\left(\frac{a}{\mathfrak{p}}\right) = f(a,b)\prod_{\mathfrak{p}\nmid 2\mathfrak{d}_2}\left(\frac{a}{\mathfrak{p}}\right)$$

for all a, b with $\gcd(a,b)|\mathfrak{d}_1$.

Proof. We have

$$\prod_{\mathfrak{p}\nmid 2\mathfrak{d}_1}\left(\frac{a}{\mathfrak{p}}\right) = \prod_{\substack{\mathfrak{p}|2\mathfrak{d}_2\\ \mathfrak{p}\nmid 2\mathfrak{d}_1}}\left(\frac{a}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(b)}\cdot\prod_{\mathfrak{p}\nmid 2\mathfrak{d}_2}\left(\frac{a}{\mathfrak{p}}\right).$$

Since $a \to \left(\frac{a}{\mathfrak{p}}\right)$ is pliable, we are done. □

Hence we obtain

Corollary 2.3.29 (to Proposition 2.3.26). *Let $F, G \in \mathfrak{O}_K[x,y]$ be homogeneous polynomials without common factors. Let $\mathfrak{d}$ be a non-zero ideal of $\mathfrak{O}_K$ such that*

$$\gcd(F(x,y),G(x,y))|\mathfrak{d}^\infty$$

for all coprime integers x, y. Let $[,]$ be as in (2.3.2). Then there is a pliable function f on $\mathfrak{O}_K^2$ such that

$$[F(x,y),G(x,y)]_{\mathfrak{d}} = f(x,y) \quad \textit{(if } \deg F \textit{ or } \deg G \textit{ is even)}$$

$$[F(x,y),G(x,y)]_{\mathfrak{d}} = f(x,y)[x,y]_1 \quad \textit{(if } \deg F \textit{ and } \deg G \textit{ are odd)}$$

for all coprime $x, y \in \mathfrak{O}_K$ (if $\deg F$ or $\deg G$ is even) or all coprime, non-zero $x, y \in \mathfrak{O}_K$ (if $\deg F$ and $\deg G$ are odd).

Proof. By Proposition 2.3.26, the statement holds for all but finitely many elements (x, y) of $\{(x, y) \in (\mathfrak{O}_K - \{0\})^2 : \gcd(x, y) = 1\}$. By Lemma 2.3.11, f can be redefined for finitely many elements of the domain and still be pliable. □

2.3.4 Averages and pliable functions

What we will now show is essentially that, given a pliable function f and a function g whose average over lattices of small index is well-known, we can tell the average of $f \cdot g$ over $\mathbb{Z}^2$. By Corollary 2.3.29 this will imply, for example, that $\sum[x^2 + 3xy - 2y^2, 4x^3 - xy^2 + 7y^3]_{\mathfrak{d}}\, g(x, y) = o(N^2)$ provided that $\sum_{(x,y)\in L} g(x, y) = o(N^2)$ for L small.

We may start with the parallel statements for affinely pliable functions.

Lemma 2.3.30. *Let U be an open subgroup of $\mathbb{R}^*$. Let $t_1 < t_2 < \cdots < t_n$ be real numbers. If t, t' are real numbers with $t < t_1$, $t' < t_1$ or $t > t_n$, $t' > t_n$, then $t - t_i$ and $t' - t_i$ lie in the same coset of U for every $1 \le i \le n$.*

Proof. If $U = \mathbb{R}^*$, the statement is trivially true. If $U = \mathbb{R}^+$, note that $t - t_i$ and $t' - t_i$ lie in the same coset of U if and only if $\operatorname{sgn}(t - t_i) = \operatorname{sgn}(t' - t_i) \neq 0$. The statement is then obvious. □

Lemma 2.3.31. *Let p be a prime. Let U be an open subgroup of $\mathbb{Q}_p^*$. Let $t_1, \ldots, t_n \in \mathbb{Q}_p$. Then there is a partition*

$$\mathbb{Z} = A_\infty \cup \bigcup_{i \ge 0} \bigcup_{k \in K} A_{i,k}$$

such that

1. *K is a finite set,*

2. *A_∞ is a finite subset of $\mathbb{Z}$,*

3. *$A_{i,k}$ is a disjoint union of at most c_1 arithmetic progressions of modulus p^{i+c_2},*

4. *for every $i_0 \geq 0$, $A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}$ is a disjoint union of at most c_1 arithmetic progressions of modulus p^{i_0},*

5. *for any choice of $i \geq 0$, $j = 1, \ldots, n$, $k \in K$ and all $t, t' \in A_{i,k}$, $t - t_j$ and $t' - t_j$ lie in the same coset of U.*

The positive integers c_1, c_2 depend only on p, U and $t_1, \ldots, t_n$.

Proof. We can assume that $U = 1 + p^l \mathbb{Z}_p$, $l \geq 1$. If t, t' lie in the same coset of U, then $t - t_j$ and $t' - t_j$ lie in the same coset of U for all $t_j \in \mathbb{Q}_p - \mathbb{Z}_p$. Hence we can assume $t_j \in \mathbb{Z}_p$ for all $1 \leq j \leq n$.

Let $d = 1 + \max_{j_1 \neq j_2} v_p(t_{j_1} - t_{j_2})$. Define

$$\begin{aligned}
K &= ((\mathbb{Z}_p/U)^* \times \{0, 1, \ldots, d\})^n, \\
A_i &= \{t \in \mathbb{Z} : \max_j v_p(t - t_j) = i\}, \\
A_\infty &= \{t_1, \ldots, t_n\} \cap \mathbb{Z}, \\
A_{i,((k_{11},k_{12}),\ldots,(k_{n1},k_{n2}))} &= \{t \in A_i : \frac{t - t_j}{p^{v_p(t-t_j)}} \equiv k_{j1} \bmod p^l, \min(v_p(t - t_j), d) = k_{j2}\}.
\end{aligned}$$

Statements (1) and (2) hold by definition. We can write A_i in the form

$$A_i = \bigcup_{1 \leq j \leq n} (t_j + p^i \mathbb{Z})$$

Since any two arithmetic progressions $t_j + p^i \mathbb{Z}$, $t_{j'} + p^i \mathbb{Z}$ of the same modulus are either disjoint or identical, it follows that A_i is the union of at most n disjoint arithmetic progressions of modulus p^i. Clearly $A_{i_0} = A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}$. Hence (4) holds.

For $i < d$,

$$A_{i,((k_{11},k_{12}),\ldots,(k_{n1},k_{n2}))} = \{t \in A_i : \frac{t-t_j}{p^{v_p(t-t_j)}} \equiv k_{j1} \bmod p^l,\ v_p(t-t_j) = k_{j2}\}.$$

If $\max_j k_{j2} \neq i$, then $A_{i,((k_{11},k_{12}),\ldots,(k_{n1},k_{n2}))} = \emptyset$. Otherwise,

$$\begin{aligned} A_{i,((k_{11},k_{12}),\ldots,(k_{n1},k_{n2}))} &= \bigcap_{1\le j\le n} \{t \in \mathbb{Z} : t \equiv p^{k_{j2}}k_{j1} + t_j \bmod p^{l+k_{j2}}\} \\ &= \bigcap_{1\le j\le n} \{t \in \mathbb{Z} : t - t_j \in k_{j1}p^{k_{j2}}U\}. \end{aligned}$$

Both (3) and (5) follow immediately.

For $i \geq d$,

$$A_{i,((k_{11},k_{12}),\ldots,(k_{n1},k_{n2}))} = \{t \in A_i : \frac{t-t_j}{p^{v_p(t-t_j)}} \equiv k_{j1} \bmod p^l,\ v_p(t-t_j) = k'_{j2}\},$$

where

$$k'_{j2} = \begin{cases} k_{j2} & \text{if } k_{j2} < d, \\ i & \text{if } k_{j2} \geq d. \end{cases}$$

Then

$$\begin{aligned} A_{i,((k_{11},k_{12}),\ldots,(k_{n1},k_{n2}))} &= \bigcap_{1\le j\le n} \{t \in \mathbb{Z} : t \equiv p^{k'_{j2}}k_{j1} + t_j \bmod p^{l+k'_{j2}}\} \\ &= \bigcap_{1\le j\le n} \{t \in \mathbb{Z} : t - t_j \in k_{j1}p^{k'_{j2}}U\}. \end{aligned}$$

Again, (3) and (5) follow. □

Lemma 2.3.32. *Let p be a prime. Let U be an open subgroup of $\mathbb{Q}_p^*$. Let $t_1, \ldots, t_n \in \mathbb{Q}_p$. Let a be an integer, m a non-negative integer. Then there is a partition*

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} = B_\infty \cup \bigcup_{i\geq m} \bigcup_{k\in K} B_{i,k}$$

such that

1. *K is a finite set,*

2. *B_∞ is a finite subset of $\mathbb{Z}$,*

3. *$B_{i,k}$ is a disjoint union of at most c_1 arithmetic progressions of modulus p^{i+c_2},*

4. *for every $i_0 \geq m$, $B_\infty \cup \bigcup_{i\geq i_0}\bigcup_{k\in K} B_{i,k}$ is a disjoint union of at most c_1 arithmetic progressions of modulus p^{i_0},*

5. *for any choice of $i \geq m$, $j = 1, \ldots, n$, $k \in K$ and all $t, t' \in B_{i,k}$, $t - t_j$ and $t' - t_j$ lie in the same coset of U.*

The positive integers c_1, c_2 depend only on p, U and $t_1, \ldots, t_n$.

Proof. Let A_∞, $A_{i,k}$ be as in Lemma 2.3.31. By Lemma 2.3.31, (4),

$$A_\infty \cup \bigcup_{i\geq i_0}\bigcup_{k\in K} A_{i,k}$$

is a union of arithmetic progressions of modulus p^{i_0}. Hence, for $i_0 \leq m$, either

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} \cap (A_\infty \cup \bigcup_{i\geq i_0}\bigcup_{k\in K} A_{i,k}) = \emptyset$$

or

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} \subset A_\infty \cup \bigcup_{i\geq i_0}\bigcup_{k\in K} A_{i,k}.$$

Suppose

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} \cap (A_\infty \cup \bigcup_{i\geq m}\bigcup_{k\in K} A_{i,k}) = \emptyset.$$

Let $i_0 \geq 0$ be the largest integer such that

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} \subset A_\infty \cup \bigcup_{i\geq i_0}\bigcup_{k\in K} A_{i,k}.$$

Then

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} = \bigcup_{k \in K} (A_{i_0,k} \cap \{t \in \mathbb{Z} : t \equiv a \bmod p^m\}).$$

Set $B_{m,k} = A_{i_0,k} \cap \{t \in \mathbb{Z} : t \equiv a \bmod p^m\}$, $B_{i,k} = \emptyset$ for $i \neq m$, $B_\infty = \{t \in A_\infty : t \equiv a \bmod p^m\}$.

Suppose now

$$\{t \in \mathbb{Z} : t \equiv a \bmod p^m\} \subset A_\infty \cup \bigcup_{i \geq m} \bigcup_{k \in K} A_{i,k}.$$

For every $i \geq m$, $k \in K$, $A_{i,k} \cap \{t \in \mathbb{Z} : t \equiv a \bmod p^m\}$ is equal to either the empty set or to $A_{i,k}$. Set $B_{i,k} = \emptyset$ for $i < m$, $B_{i,k} = A_{i,k} \cap \{t \in \mathbb{Z} : t \equiv a \bmod p^m\}$ for $i \geq m$, $B_\infty = \{t \in A_\infty : t \equiv a \bmod p^m\}$. □

Lemma 2.3.33. *Let M, R and C be positive integers. Let $\{a_n\}_{n=1}^\infty$ be such that*

1. *$a_n = 0$ for all n for which $\mathrm{rad}(n) \nmid R$,*
2. *$s_d = \sum_n |a_{dn}|$ converges for every d,*
3. *$s_d = O(C/d)$ for $M < d \leq p_0 M$, where p_0 is the largest prime factor of R.*

Then

$$\sum_n a_n = \sum_{n \leq M} a_n + O\left(\frac{C(\log p_0 M)^{\omega(R)}}{M}\right),$$

where the implied constant is absolute.

Proof. Every $n > M$ satisfying $\mathrm{rad}(n)|R$ has a divisor $M < d \leq p_0 M$. Hence

$$\sum_n a_n = \sum_{n \leq M} a_n + O\left(\sum_{n > M} |a_n|\right) = \sum_{n \leq M} a_n + O\left(\sum_{\substack{M < d \leq p_0 M \\ \mathrm{rad}(d)|R}} \sum_{\substack{n \\ d|n}} |a_n|\right)$$

$$= \sum_{n \leq M} a_n + O\left(\sum_{\substack{M < d \leq p_0 M \\ \mathrm{rad}(d)|R}} C/d\right).$$

There are at most $\prod_{p|R}(1+\log_p p_0 M)$ terms in $\sum_{M<d\le p_0 M,\,\mathrm{rad}(d)|R}$. Hence

$$\sum_n a_n = \sum_{n\le M} a_n + O\left(\frac{C(\log p_0 M)^{\omega(R)}}{M}\right).$$

□

Lemma 2.3.34. *Let $f, g : \mathbb{Z} \to \mathbb{C}$ be given with $\max|f(x)| \le 1$, $\max|g(x)| \le 1$. Let f be affinely pliable with respect to $\{(v_j, U_j, t_j)\}$. Assume that there are $\eta_N \le N$, $\epsilon_N \ge 0$ such that for any $a, m \in \mathbb{Z}$, $0 < m \le \eta_N$,*

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} g(x) \ll \frac{\epsilon_N N}{m}. \tag{2.3.3}$$

Then, for any $a, m \in \mathbb{Z}$, $0 < m \le \eta_N$,

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} f(x)g(x) \ll \left(\frac{\epsilon_N}{m} + \frac{(\log \eta_N)^c}{\eta_N}\right) N,$$

where c is the number of distinct finite places among $\{v_j\}$ and the implied constant depends only on the implied constant in (2.3.3) and on $\{v_j, U_j, t_j\}$.

Proof. Let $\{p_l\}$ be the set of all finite places among $\{v_j\}$. Let $\{t_{l,1}, \cdots, t_{l,n_l}\}$ be the set of all t_j such that v_j is induced by p_l. For every p_l, Lemma 2.3.32 yields a partition

$$\{x \in \mathbb{Z} : x \equiv a \bmod p_l^{v_{p_l}(m)}\} = B_{l,\infty} \cup \bigcup_{i\ge v_{p_l}(m)} \bigcup_{k\in K_l} B_{l,i,k}$$

such that $t - t_{l,j}$ and $t' - t_{l,j}$ lie in the same coset of U_l for any $t, t' \in B_{l,i,k}$ and any i, j, k. Let

$$m_0 = \frac{m}{\prod_l p_l^{v_{p_l}(m)}}.$$

Clearly

$$\{x \in \mathbb{Z} : x \equiv a \bmod m\} = \bigcap_l \left(B_{l,\infty} \cup \bigcup_{i \geq v_{p_l}(m)} \bigcup_{k \in K_l} B_{l,i,k} \right) \cap (a + m_0\mathbb{Z})$$
$$= \left(\bigcap_l B_{l,\infty} \right) \cup \bigcup_{\substack{n \geq 1 \\ \mathrm{rad}(n)|R}} \bigcup_{\{k_l\} \in \prod_l K_l} \bigcap_l B_{l,v_p(mn),k_l} \cap (a + m_0\mathbb{Z}), \tag{2.3.4}$$

where $R = \prod_l p_l$. Let t_0 be the largest of all t_j such that v_j is an infinite place; see Lemma 2.3.30. Since f is affinely pliable with respect to $\{v_j, U_j, t_j\}$, it is constant on

$$\{x \in \mathbb{Z} : x > t_0\} \cap \bigcap_l B_{l,v_p(mn),k_l} \tag{2.3.5}$$

for any $n \geq 1$ and any $\{k_l\} \in \prod_l K_l$. Denote the value of f on (2.3.5) by $f_{n,\{k_l\}}$. Thanks to (2.3.4), we can write

$$\sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m}} f(x)g(x) = \sum_{1 \leq x \leq t_0} f(x)g(x) + \sum_{\substack{t_0 < x \leq N \\ x \in \cap_l B_{l,\infty}}} f(x)g(x)$$
$$+ \sum_{\substack{n \geq 1 \\ \mathrm{rad}(n)|R}} \sum_{\{k_l\} \in \prod_l K_l} \sum_{\substack{t_0 < x \leq N \\ x \in \cap_l B_{l,v_p(mn),k_l} \\ x \in a + m_0\mathbb{Z}}} f(x)g(x)$$
$$= O(1) + \sum_{\{k_l\} \in \prod_l K_l} \sum_{\substack{n \geq 1 \\ \mathrm{rad}(n)|R}} f_{n,\{k_l\}} \sum_{\substack{1 \leq x \leq N \\ x \in \cap_l B_{l,v_p(mn),k_l} \\ x \in a + m_0\mathbb{Z}}} g(x).$$

Fix $\{k_l\} \in \prod_l K_l$. Set

$$a_n = f_{n,\{k_l\}} \sum_{\substack{1 \leq x \leq N \\ x \in \cap_l B_{l,v_p(mn),k_l} \\ x \in a + m_0\mathbb{Z}}} g(x)$$

if $\mathrm{rad}(n)|R$, $a_n = 0$ otherwise. Then

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} f(x)g(x) = \sum_n a_n.$$

Let $s_d = \sum_n |a_{dn}|$. From Lemma 2.3.32, (4), and the fact that $\max|g(x)| \le 1$, we get that $s_d \ll \frac{N}{mn}$. Set $C = N/m$. By Lemma 2.3.32, (3), $\bigcap_l B_{l,v_p(mn),k_l} \cap (a + m_0\mathbb{Z})$ is the union of at most $c_3 = c_1^{\#\{p_l\}}$ arithmetic progressions of modulus $c_4 mn$, where $c_4 = \prod_l p_l^{c_2}$. Set $M = \min\left(\frac{\eta_N}{c_4 m}, \frac{N}{p_0 m}\right)$, where $p_0 = \max_l p_l$. We can now apply Lemma 2.3.33, obtaining

$$\begin{aligned}\sum_n a_n &= \sum_{n\le M} a_n + O\left(\frac{C(\log p_0 M)^{\omega(R)}}{M}\right)\\ &= \sum_{n\le M} a_n + \max\left(\frac{N}{\eta_N}(\log \eta_N/m)^{w(R)}, (\log N/m)^{w(R)}\right)\\ &= \sum_{n\le M} a_n + O\left(\frac{N}{\eta_N}(\log \eta_N)^{\omega(R)}\right).\end{aligned} \tag{2.3.6}$$

By (2.3.3),

$$\begin{aligned}\sum_{n\le M} a_n &\ll \sum_{\substack{n\le M\\ \mathrm{rad}(n)|R}} \frac{\epsilon_N N}{mn} \le \sum_{\mathrm{rad}(n)|R} \frac{\epsilon_N N}{mn}\\ &= \frac{\epsilon N}{m}\cdot\prod_{p|R}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \ll \frac{\epsilon N}{m}.\end{aligned} \tag{2.3.7}$$

We conclude that

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} f(x)g(x) \ll \frac{\epsilon N}{m} + \frac{N(\log \eta_N)^{\omega(R)}}{\eta_N}.$$

□

Lemma 2.3.35. *Let U be an open subgroup of $\mathbb{R}^*$. Let $\{\vec{q}_j\}$ be a finite subset of $\mathbb{R}^n$.*

Then there is a partition

$$\mathbb{R}^n = T_1 \cup \cdots \cup T_k \cup S_1 \cup \cdots \cup S_l$$

such that

1. *T_j is a hyperplane,*

2. *S_i is a sector,*

3. *$\vec{q}_j \cdot \vec{v}_1$ and $\vec{q}_j \cdot \vec{v}_2$ lie in the same coset rU of U for any $\vec{v}_1, \vec{v}_2 \in S_i$ and all j.*

Proof. We can assume $U = \mathbb{R}^+$. Set $T_i = \{(x, y) \in \mathbb{R}^n : (x, y) \cdot \vec{q}_j = 0\}$. Let $S_1, \ldots, S_l$ be the connected components of $\mathbb{R}^n - (T_1 \cap T_2 \cap \cdots \cap T_k)$. □

We define $\mathbb{A}_p = \{(x, y) \in \mathbb{Z}^2 : p \nmid \gcd(x, y)\}$.

Lemma 2.3.36. *Let p be a prime. Let n be a non-negative integer. For any two distinct lattices $L, L' \subset \mathbb{Z}^2$ of index $[\mathbb{Z}^2 : L] = [\mathbb{Z}^2 : L'] = p^n$, the two sets $\mathbb{A}_p \cap L$, $\mathbb{A}_p \cap L'$ are disjoint.*

Proof. Both L and L' contain $(p^n, 0)$ and $(0, p^n)$. Suppose $(x, y) \in L \cap L'$, $p \nmid \gcd(x, y)$. Then the lattice L'' generated by $(p^n, 0)$, $(0, p^n)$ and (x, y) is contained in $L \cap L'$. Since the index $[\mathbb{Z}^2 : L'']$ of L'' is p^n, it follows that $L = L'$. Contradiction. □

Lemma 2.3.37. *Let p be a prime. Let U be an open subgroup of $\mathbb{Q}_p^*$. Let $\{\vec{q}_j\}_{j \in J}$ be a finite subset of $\mathbb{Q}_p^2$. Then there is a partition*

$$\mathbb{A}_p = A_\infty \cup \bigcup_{i \geq 0} \bigcup_{k \in K} A_{i,k}$$

such that

1. *K is a finite set,*

2. *A_∞ is the union of finitely many sets of the form $A_{x,y} = \{(nx, ny) : n \in \mathbb{Z}, p \nmid n\}$,*

3. *$A_{i,k}$ is a disjoint union of at most c_1 lattice cosets of index p^{i+c_2},*

4. *for every $i_0 \geq 0$, the set $A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}$ is a disjoint union of at most c_1 sets of the form $R \cap \mathbb{A}_p$, where R is a lattice of index p^{i_0}; any given $A_{i,k}$, $i \geq i_0$, lies entirely within one such set $R \cap \mathbb{A}_p$;*

5. *for any choice of $i \geq 0$, $j \in J$, $k \in K$ and all $(x_1, y_1), (x_2, y_2) \in A_{i,k}$, the inner products $\vec{q}_j \cdot (x_1, y_1)$ and $\vec{q}_j \cdot (x_2, y_2)$ lie in the same coset of U.*

Proof. We can assume that $U \subset \mathbb{Z}_p^*$ and $\vec{q}_j \in \mathbb{Z}_p^2 - (p\mathbb{Z}_p)^2$. Furthermore we can suppose that for every pair of indices j_1, j_2, $j_1 \neq j_2$, there is no rational number c such that $\vec{q}_{j_1} = c\vec{q}_{j_2}$. Hence the determinant

$$D_{j_1,j_2} = \begin{vmatrix} q_{j_1,1} & q_{j_1,2} \\ q_{j_2,1} & q_{j_2,2} \end{vmatrix}$$

is non-zero. Take $(x, y) \in \mathbb{Z}^2$ with $p \nmid x$. Then

$$\begin{aligned} \min(v_p(\vec{q}_{j_1} \cdot (x, y)), v_p(\vec{q}_{j_2} \cdot (x, y))) &\leq v_p \left(\begin{vmatrix} \vec{q}_{j_1} \cdot (x, y) & q_{j_1,2} \\ \vec{q}_{j_2} \cdot (x, y) & q_{j_2,2} \end{vmatrix} \right) \\ &= v_p \left(\begin{vmatrix} q_{j_1,1} & q_{j_1,2} \\ q_{j_2,1} & q_{j_2,2} \end{vmatrix} \cdot \begin{vmatrix} x & 0 \\ y & 1 \end{vmatrix} \right) = v_p(D_{j_1,j_2}). \end{aligned}$$

In the same way

$$\min(v_p(\vec{q}_{j_1} \cdot (x, y)), v_p(\vec{q}_{j_2} \cdot (x, y))) \leq v_p(D_{j_1,j_2})$$

for $(x, y) \in \mathbb{Z}^2$ with $p \nmid y$. Setting $d = \max_{j_1 \neq j_2} v_p(D_{j_1,j_2})$ we obtain that for any

given pair $(x, y) \in \mathbb{Z}^2$ with $p \nmid \gcd(x, y)$ there can be at most one index j for which $v_p(\vec{q}_j \cdot (x, y)) > d$.

Let the cosets of U in $\mathbb{Z}_p^*$ be $U_1, U_2, \ldots U_m$. Let r be the least positive integer such that $p^r\mathbb{Z}_p + 1 \subset U$. Define

$$K = \{(x_0, y_0, a) \in (\mathbb{Z}/p^{d+r})^2 \times \{1, 2, \ldots, m\} : p \nmid x_0 \vee p \nmid y_0\},$$
$$A_\infty = \{(x, y) \in \mathbb{Z}^2 : \exists j \text{ s.t. } (x, y) \cdot \vec{q}_j = 0\} \cap \{(x, y) \in \mathbb{Z}^2 : p \nmid \gcd(x, y)\}.$$

For $i > d$, let $A_{i,(x_0,y_0,a)}$ be the set of all $(x, y) \in \mathbb{Z}^2$ such that $x \equiv x_0 \bmod p^{d+r}$, $y \equiv y_0 \bmod p^{d+r}$, $\max_j v_p((x, y) \cdot \vec{q}_j) = i$ and $p^{-i}(\vec{q}_{j_0} \cdot (x, y)) \in U_a$, where j_0 is the only j for which the maximum $\max_j v_p((x, y) \cdot \vec{q}_j) = i$ is attained. For $i \leq d$ and $a > 1$, let $A_{i,(x_0,y_0,a)}$ be the empty set. For $i \leq d$ and $a = 1$, let $A_{i,(x_0,y_0,a)}$ be the set of all $(x, y) \in \mathbb{Z}^2$ such that $x \equiv x_0 \bmod p^{d+r}$, $y \equiv y_0 \bmod p^{d+r}$ and $\max_j v_p(\vec{q}_j \cdot (x, y)) = i$. These definitions for $A_{i,k}$, $k \in K$, give us that

$$A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k} = \{(x, y) \in \mathbb{Z}^2 : p \nmid \gcd(x, y), \max_j v_p((x, y) \cdot \vec{q}_j) \geq i_0\}. \tag{2.3.8}$$

Properties (1) and (2) follow immediately from our definitions of K, A and $A_{i,(x_0,y_0,a)}$. Let us verify properties (3) and (4). For $i_0 \geq 0$,

$$A \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k} = \bigcup_{j \in J} \left(\{(x, y) \in \mathbb{Z}^2 : v_p((x, y) \cdot \vec{q}_j) \geq i_0\} \cap \mathbb{A}_p\right). \tag{2.3.9}$$

By Lemma 2.3.36, any two distinct sets in the union on the right hand side of (2.3.9) are disjoint. Since $\{(x, y) \in \mathbb{Z}^2 : v_p((x, y) \cdot \vec{q}_j) \geq i_0\}$ is a lattice of index p^{i_0}, we have proven the first half of (4). Let $(x, y) \in A_{i,(x_0,y_0,a)}$, $i \geq i_0$, $j \in J$. To prove the second half of (4), we must show that we can tell whether $v_p((x, y) \cdot \vec{q}_k) \geq i_0$ from i, i_0, x_0, y_0, a and j alone. If $i_0 \leq d$, this is clear: $x_0, y_0 \bmod p^d$ give us $x, y \bmod p^d$. If $i_0 > d$, then $v_p((x, y) \cdot \vec{q}_j) \geq i_0$ if and only if $v_p((x, y) \cdot \vec{q}_j) > d$. We can tell whether

$v_p((x,y)\cdot\vec{q}_j) > d$ from $x_0, y_0 \bmod p^{d+1}$. Hence (4) holds.

For $i \le d$, each set $A_{i,(x_0,y_0,a)}$ is either empty or a lattice coset of index $p^{2(d+r)}$. Then $A_{i,(x_0,y_0,a)}$ can be written as a disjoint union $A_{i,(x_0,y_0,a)} = \bigcup_{j\in J} A'_{i,j,(x_0,y_0,a)}$, where $A'_{i,j,(x_0,y_0,a)}$ is the set of all $(x,y)\in\mathbb{Z}^2$ such that

$$x \equiv x_0 \bmod p^{d+r},\ y \equiv y_0 \bmod p^{d+r},\ v_p(\vec{q}_j\cdot(x,y)) = i,\ p^{-i}(\vec{q}_j\cdot(x,y)) \in U_a.$$

The union is disjoint because $v_p((x,y)\cdot\vec{q}_j) = i$ cannot hold for two different j when $i > d$. Since $1 + p^r\mathbb{Z}_p \subset U$, we can write $A'_{i,j,(x_0,y_0,a)}$ as a disjoint union of at most p^r sets of the form

$$\begin{aligned} L_{i,j,(x_0,y_0,b)} = \{(x,y)\in\mathbb{Z}^2 : x \equiv x_0 \bmod p^{d+r}, y \equiv y_0 \bmod p^{d+r}\} \\ \cap \{(x,y)\in\mathbb{Z}^2 : \vec{q}_j\cdot(x,y) \equiv b \bmod p^{i+r}\}. \end{aligned}$$

Since this is the intersection of a lattice coset of index p^{2d+2r} and a lattice coset of index p^{i+r}, $L_{i,j,(x_0,y_0,b)}$ must be a lattice coset of index n_i satisfying $p^{i+r}|n_i|p^{i+2d+3r}$. Hence (3) is satisfied for any $i \ge 0$.

It remains to prove (5). For $i > d$, this is immediate from the definition of $A_{i,(x_0,y_0,a)}$. Let $i \le d$. Any two elements (x_1,y_1), (x_2,y_2) of $A_{i,(x_0,y_0,a)}$ must satisfy $x_1 \equiv x_2 \bmod p^{d+r}$, $y_1 \equiv y_2 \bmod p^{d+r}$. Hence $\vec{q}_j\cdot(x_1,y_1) \cong \vec{q}_j\cdot(x_2,y_2) \bmod p^{d+r}$ for every j. Since $\max_j v_p(\vec{q}_j\cdot(x_1,y_1)) = \max_j v_p(\vec{q}_j\cdot(x_2,y_2)) = i \le d$, we can conclude that $\vec{q}_j\cdot(x_1,y_1)$ and $\vec{q}_j\cdot(x_1,y_1)$ lie in the same coset of $1+p^r\mathbb{Z}_p$. Hence $\vec{q}_j\cdot(x_1,y_1)$ and $\vec{q}_j\cdot(x_1,y_1)$ lie in the same coset of U. □

Lemma 2.3.38. *Let $L \subset \mathbb{Z}^2$ be a lattice. Let $L', L'' \subset L$ be lattice cosets contained in L. Then the intersection $L' \cap L''$ is either the empty set or a lattice coset of index $[\mathbb{Z}^2 : L' \cap L'']$ dividing $\frac{[\mathbb{Z}^2:L']\cdot[\mathbb{Z}^2:L'']}{[\mathbb{Z}^2:L]}$.*

Proof. Since L and $\mathbb{Z}^2$ are isomorphic, it is enough to prove the statement for $L = \mathbb{Z}^2$. It holds in general that, given two subgroup cosets L', L'' of an abelian group Z, the

intersection $L' \cap L''$ is either the empty set or a subgroup coset of index dividing $[Z : L'] \cdot [Z : L]$. $\square$

Lemma 2.3.39. *Let p be a prime. Let U be an open subgroup of $\mathbb{Q}_p^*$. Let $\{\vec{q}_j\}_{j \in J}$ be a finite subset of $\mathbb{Q}_p^2$. Let L be a lattice of index $[\mathbb{Z}^2 : L] = p^m$. Then there is a partition*

$$L \cap \mathbb{A}_p = B_\infty \cup \bigcup_{i \geq m} \bigcup_{k \in K} B_{i,k}$$

such that

1. *K is a finite set,*
2. *B_∞ is the union of finitely many sets of the form $A_{x,y} = \{(nx, ny) : n \in \mathbb{Z}, p \nmid n\}$,*
3. *$B_{i,k}$ is a disjoint union of at most c_1 lattice cosets of index p^{i+c_2},*
4. *for every $i_0 \geq 0$, the set $B_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} B_{i,k}$ is a disjoint union of at most c_1 sets of the form $R \cap \mathbb{A}_p$, where R is a lattice of index p^{i_0},*
5. *for any choice of $i \geq 0$, $j \in J$, $k \in K$ and all $(x_1, y_1), (x_2, y_2) \in A_{i,k}$, the inner products $\vec{q}_j \cdot (x_1, y_1)$ and $\vec{q}_j \cdot (x_2, y_2)$ lie in the same coset of U.*

Proof. Let A_∞, $A_{i,k}$ be as in Lemma 2.3.37. By Lemma 2.3.37, (4),

$$A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}$$

is a disjoint union of at most c_1 lattices of index p^{i_0}. Hence, for $i_0 \leq m$, it follows from Lemma 2.3.36 that either

$$(L \cap \mathbb{A}_p) \cap (A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}) = \emptyset$$

or

$$L \cap \mathbb{A}_p \subset (A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k})$$

must hold. Suppose $(L \cap \mathbb{A}_p) \cap (A_\infty \cup \bigcup_{i \geq m} \bigcup_{k \in K} A_{i,k}) = \emptyset$. Let $i_0 \geq 0$ be the largest integer such that

$$(L \cap \mathbb{A}_p) \subset (A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}).$$

Then

$$L \cap \mathbb{A}_p = \bigcup_{k \in K} (A_{i_0,k} \cap L).$$

Set $B_{m,k} = A_{i_0,k} \cap L$, $B_{i,k} = \emptyset$ for $i \neq m$, $B_\infty = A_\infty \cap L$. Conditions (1), (2), (4) and (5) follow trivially from the definitions of $A_{i_0,k}$ and m. By Lemma 2.3.37, (3), $A_{i_0,k}$ is the disjoint union of at most c_1 lattice cosets of index $p^{i_0+c_2}$. Take one such lattice coset and call it R_0. By Lemma 2.3.37, (4), R_0 is contained in a set of the form $R \cap \mathbb{A}_p$, where R is a lattice of index p^{i_0}. Since $p^{i_0} | p^m$, L is contained in a lattice R' of index p^{i_0}. By Lemma 2.3.36, either $R \cap R' \cap \mathbb{A}_p = \emptyset$ or $R = R'$. In the former case, $R_0 \cap (L \cap \mathbb{A}_p) = \emptyset$. In the latter case, Lemma 2.3.38 yields that $R_0 \cap L$ is a lattice coset of index dividing $p^{(i_0+c_2)+m-i_0} = p^{m+c_2}$ and divided by $[\mathbb{Z}^2 : R \cap L] = [\mathbb{Z}^2 : L] = p^m$. Condition (4) follows.

Now suppose

$$L \cap \mathbb{A}_p \subset (A_\infty \cup \bigcup_{i \geq m} \bigcup_{k \in K} A_{i,k}).$$

By Lemma 2.3.37, $A_\infty \cup \bigcup_{i \geq i_0} \bigcup_{k \in K} A_{i,k}$ is a disjoint union of sets of the form $R \cap \mathbb{A}_p$, R a lattice of index p^m. By Lemma 2.3.36, one such R is equal to L. For $i \geq m$, set $B_{i,k} = A_{i,k}$ if $A_{i,k} \subset L$, $B_{i,k} = 0$ otherwise. Set $B_\infty = A_\infty \cap L$. Conditions (1) to (5) follow easily. $\square$

Proposition 2.3.40. *Let $f, g : \mathbb{Z}^2 \to \mathbb{C}$ be given with* $\max |f(x,y)|, |g(x,y)| \leq 1$. *Let f be pliable with respect to $\{(v_j, U_j, \vec{q}_j)\}$. Assume that there are $\eta_N \leq N$, $\epsilon_N \geq 0$ such*

that for any sector S and any lattice coset L of index $[\mathbb{Z}^2 : L] \leq \eta_N$,

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} g(x,y) \ll \frac{\epsilon_N N^2}{[\mathbb{Z}^2 : L]}. \tag{2.3.10}$$

Then, for any sector S and any lattice L,

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} f(x,y)g(x,y) \ll \left(\frac{\epsilon_N}{[\mathbb{Z}^2 : L]} + \frac{(\log \eta_N)^c}{\eta_N}\right) N^2,$$

where c is the number of distinct finite places among $\{v_j\}$ and the implied constant depends only on the implied constant in (2.3.10) and on $\{(v_j, U_j, \vec{q}_j)\}$.

Proof. By Lemma 2.3.35 we can partition $\mathbb{R}^2$ into

$$\mathbb{R}^2 = T_1 \cup \cdots \cup T_k \cup S_1 \cup \cdots \cup S_l$$

such that $\vec{q}_j \cdot (x_1, y_1)$ and $\vec{q}_j \cdot (x_2, y_2)$ lie in the same coset of $\bigcup_j U_j$ for all (x_1, y_1), (x_2, y_2) in S_i and all j with $v_j = \infty$. The contribution of $T_1, T_2, \ldots, T_k$ to the final sum is $O(1)$. As there is a finite number of S_i's, it is enough to prove the desired bound for every S_i separately. Fix i and let $S' = S_i \cap S$.

Let $\{p_l\}$ be the set of all finite places among $\{v_j\}$. Let $\{\vec{q}_{l,j}\}$ be the set of all $\vec{q}_j$ such that v_j is induced by p_l. Let $m = [\mathbb{Z}^2 : L]$. We can write

$$L = \bigcap_l L_{p_l} \cap L_{m_0},$$

where L_{p_l} is a lattice of index $p_l^{v_{p_l}(m)}$ and L_{m_0} is a lattice of index $m_0 = \frac{m}{\prod_l p_l^{v_{p_l}(m)}}$.

For every p_l, Lemma 2.3.37 yields a partition

$$L_{p_l} \cap \mathbb{A}_{p_l} = B_\infty \cup \bigcup_{i \geq v_{p_l}(m)} \bigcup_{k \in K_l} B_{l,i,k}$$

such that $\vec{q}_{l,j} \cdot (x_1, y_1)$ and $\vec{q}_{l,j} \cdot (x_2, y_2)$ lie in the same coset of U for any (x_1, y_1), (x_2, y_2) in $B_{l,i,k}$ and any i, j, k.

Let $\mathbb{A} = \{x, y \in \mathbb{Z}^2 : \gcd(x, y) = 1\}$. Clearly

$$\begin{aligned} L \cap \mathbb{A} &= \bigcup_l \left(B_{l,\infty} \cup \bigcup_{i \geq v_{p_l}(m)} \bigcup_{k \in K_l} B_{l,i,k} \right) \cap \mathbb{A} \\ &= \left(\bigcup_l B_{l,\infty} \cap \mathbb{A} \right) \cup \bigcup_{\substack{n \geq 1 \\ \mathrm{rad}(n) | R}} \bigcup_{\{k_l\} \in \prod_l K_l} \left(\bigcap_l B_{l, v_p(mn), k_l} \cap L_{m_0} \right) \cap \mathbb{A}. \end{aligned} \tag{2.3.11}$$

Note that $(\bigcup_l B_{l,\infty} \cap \mathbb{A})$ is a finite set. Since f is affinely pliable with respect to $\{v_j, U_j, \vec{q}_j\}$, it is constant on $S' \cap \bigcap_l B_{l, v_p(mn), k_l}$ for any $n \geq 1$ and any $\{k_l\} \in \prod_l K_l$. Denote the value of f on $\bigcap_l B_{l, v_p(mn), k_l}$ by $f_{n, \{k_l\}}$. Thanks to (2.3.11), we can write

$$\begin{aligned} \sum_{\substack{(x,y) \in S' \cap [-N,N]^2 \cap L \\ \gcd(x,y)=1}} f(x,y) g(x,y) &= \sum_{(x,y) \in \cap_l B_{l,\infty} \cap \mathbb{A}} f(x,y) g(x,y) \\ &+ \sum_{\substack{n \geq 1 \\ \mathrm{rad}(n) | R}} \sum_{\{k_l\} \in \prod_l K_l} \sum_{\substack{(x,y) \in B_{l, v_p(mn), k_l} \cap L_{m_0} \\ (x,y) \in \mathbb{A}}} f(x,y) g(x,y) \\ &= \sum_{\{k_l\} \in \prod_l K_l} \sum_{\substack{n \geq 1 \\ \mathrm{rad}(n) | R}} f_{n, \{k_l\}} \sum_{\substack{(x,y) \in B_{l, v_p(mn), k_l} \cap L_{m_0} \\ (x,y) \in \mathbb{A}}} g(x,y) \\ &+ O(1). \end{aligned}$$

Fix $\{k_l\} \in \prod_l K_l$. Set

$$a_n = f_{n,\{k_l\}} \sum_{\substack{(x,y)\in B_{l,v_p(mn),k_l}\cap L_{m_0} \\ (x,y)\in\mathbb{A}}} g(x,y)$$

if $\mathrm{rad}(n)|R$, $a_n = 0$ otherwise. Then

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} f(x,y)g(x,y) = \sum_n a_n.$$

Let $s_d = \sum_n |a_{dn}|$. From Lemma 2.3.39, (4), Lemma 2.2.1 and $|g(x,y)| \leq 1$, we get that $s_d \ll \frac{N^2}{mn}$. Set $C = N^2/m$. By Lemma 2.3.39, (3), $\bigcap_l B_{l,v_p(mn),k_l} \cap L_{m_0}$ is the union of at most $c_3 = c_1^{\#\{p_l\}}$ lattice cosets of modulus $c_4 mn$, where $c_4 = \prod_l p_l^{c_2}$. Set $M = \min\left(\frac{\eta_N}{c_4 m}, \frac{N}{p_0 m}\right)$, where $p_0 = \max_l p_l$. We can now apply Lemma 2.3.33, obtaining

$$\sum_n a_n = \sum_{n\leq M} a_n + O\left(\frac{N}{\eta_N}(\log\eta_N)^{\omega(R)}\right).$$

By (2.3.10),

$$\begin{aligned}\sum_{n\leq M} a_n &\ll \sum_{\substack{n\leq M \\ \mathrm{rad}(n)|R}} \frac{\epsilon_N N}{mn} \leq \sum_{\mathrm{rad}(n)|R} \frac{\epsilon_N N}{mn} \\ &= \frac{\epsilon N}{m}\cdot\prod_{p|R}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) \ll \frac{\epsilon N}{m} = \frac{\epsilon N}{[\mathbb{Z}^2 : L]}.\end{aligned}$$

We conclude that

$$\sum_{\substack{(x,y)\in S'\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} f(x,y)g(x,y) \ll \left(\frac{\epsilon_N}{[\mathbb{Z}^2 : L]} + \frac{(\log\eta_N)^c}{\eta_N}\right) N^2.$$

As said in the beginning of the proof, it follows immediately that

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} f(x,y)g(x,y) \ll \left(\frac{\epsilon_N}{[\mathbb{Z}^2:L]} + \frac{(\log\eta_N)^c}{\eta_N}\right) N^2.$$

□

2.4 Using the square-free sieve

We will now state the results we need from Chapter 4, as well as some simple consequences.

2.4.1 Conditional results

We introduce the following quantitative versions of Conjectures $\mathfrak{A}_1$ and $\mathfrak{A}_2$.

Conjecture $\mathfrak{A}_1(K,P,\delta(N))$. *The polynomial $P\in\mathfrak{O}_K[x]$ obeys*

$$\#\{1\le x\le N : \exists\mathfrak{p}\ s.t.\ \rho(\mathfrak{p})>N^{1/2}, \mathfrak{p}^2|P(x)\} \ll \delta(N),$$

where $1\ll\delta(N)\ll N$ and $\rho(\mathfrak{p})$ is the rational prime lying under $\mathfrak{p}$.

Conjecture $\mathfrak{A}_2(K,P,\delta(N))$. *The homogeneous polynomial $P\in\mathfrak{O}_K[x,y]$ obeys*

$$\#\{-N\le x,y\le N : \exists\mathfrak{p}\ s.t.\ \rho(\mathfrak{p})>N, \mathfrak{p}^2|P(x)\} \ll \delta(N),$$

where $1\ll\delta(N)\ll N$ and $\rho(\mathfrak{p})$ is the rational prime lying under $\mathfrak{p}$.

We can now restate Propositions 4.2.16 and 4.2.17 as conditional results.

Proposition 2.4.1 ($\mathfrak{A}_1(K,P,\delta(N))$). *Let K be a number field. Let $f: I_K\times\mathbb{Z}\to\mathbb{C}$, $g:\mathbb{Z}\to\mathbb{C}$ be given with $\max|f(\mathfrak{a},x)|\le 1$, $\max|g(x)|\le 1$. Assume that $f(\mathfrak{a},x)$*

depends only on $\mathfrak{a}$ *and on* $x \bmod \mathfrak{a}$. *Let* $P \in \mathfrak{O}_K[x]$. *Suppose there are* $\epsilon_{1,N}, \epsilon_{2,N} \geq 0$ *such that for any integer* a *and any positive integer* m,

$$\sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m}} g(x) \ll \left(\frac{\epsilon_{1,N}}{m} + \epsilon_{2,N}\right) N. \tag{2.4.1}$$

Then, for any integer a *and any positive integer* m,

$$\sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m}} f(\mathrm{sq}_K(P(x)), x) g(x) \ll \left(\frac{\epsilon_{1,N}}{m} + (\log N)^{c_1} \sqrt{\max(\epsilon_{2,N}, m/N^{1/2})}\right)$$
$$\cdot \tau_{c_2}(m) N + \delta(N),$$

where c_1 *and* c_2 *depend only on* P *and* K, *and the implied constant depends only on* P, K *and the implied constant in (2.4.1).*

Proposition 2.4.2 ($\mathfrak{A}_2(K, P, \delta(N))$). *Let* K *be a number field. Let* $f : I_K \times \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1\} \to \mathbb{C}$, $g : \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1\} \to \mathbb{C}$ *be given with* $\max |f(\mathfrak{a}, x, y)| \leq 1$, $\max |g(x, y)| \leq 1$. *Assume that* $f(\mathfrak{a}, x, y)$ *depends only on* $\mathfrak{a}$ *and on* $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$. *Let* $P \in \mathfrak{O}_K[x, y]$ *be a homogeneous polynomial. Let* S *be a convex set. Suppose there are* $\epsilon_{1,N}, \epsilon_{2,N} \geq 0$ *such that for any lattice coset* $L \subset \mathbb{Z}^2$,

$$\sum_{\substack{(x,y) \in S \cap [-N,N]^2 \cap L \\ \gcd(x,y)=1}} g(x, y) \ll \left(\frac{\epsilon_{1,N}}{\phi([\mathbb{Z}^2 : L])} + \epsilon_{2,N}\right) N^2. \tag{2.4.2}$$

Then, for any lattice coset $L \subset \mathbb{Z}^2$,

$$\sum_{\substack{(x,y) \in S \cap [-N,N]^2 \cap L \\ \gcd(x,y)=1}} f(\mathrm{sq}_K(P(x, y)), x, y) g(x, y)$$
$$\ll \left(\frac{\epsilon_{1,N}}{[\mathbb{Z}^2 : L]} + (\log N)^{c_1} \sqrt{\max(\epsilon_{2,N}, [\mathbb{Z}^2 : L]/N)}\right) \tau_{c_2}(m) N + \delta(N),$$

where c_1 *and* c_2 *depend only on* P *and* K, *and the implied constant depends only on*

P, K and the implied constant in (2.4.2).

See Appendices A.1 and A.2 for all proven instances of $\mathfrak{A}_i(K, P, \delta(N))$.

2.4.2 Miscellanea

We will need the following simple lemmas.

Lemma 2.4.3. *For any positive integer n,*

$$\prod_{p|n}\left(1+\frac{1}{p}\right) \ll \log\log n,$$

where the implied constant is absolute.

Proof. Obviously

$$\log\prod_{p|n}\left(1+\frac{1}{p}\right) \le \sum_{p|n}\frac{1}{p}.$$

Define

$$S(m,r) = \max_{n\le r}\sum_{\substack{p|n\\ p>m}}\frac{1}{p}.$$

Then, for any r,

$$S(m,r) \le \frac{1}{p} + S(p, r/p)$$

for some $p > m$. Clearly

$$S(m_1,n) \ge S(m_2,n) \ \text{ if } m_1 \le m_2,$$

$$S(m,n_1) \ge S(m,n_2) \ \text{ if } n_1 \ge n_2.$$

Hence

$$\begin{aligned} S(1,n) &\le \frac{1}{2} + S(2,n/2) \le \frac{1}{2}+\frac{1}{3}+S(3,n/2\cdot 3)\\ &\le \frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p}+S\left(m,\frac{n}{\prod_{p\le m}p}\right). \end{aligned}$$

Now

$$\prod_{p\le m} p = \left(\frac{m}{2}\right)^{O((m/2)/(\log m/2))} = e^{O(m)}.$$

Thus, the least m such that $\prod_{p\le m} p > n/2$ is at most $O(\log n)$. Therefore

$$S(1,n) \le \sum_{p\le m} \frac{1}{p} \le \log\log\log n + o(1).$$

The statement follows. □

Lemma 2.4.4. *Let $g : \mathbb{Z}^2 \to \mathbb{C}$ be given with $|g(x,y)| \le 1$ for all $x, y \in \mathbb{Z}$. Let $\eta(N) \le N$. Suppose that, for every sector S and every lattice L of index $[\mathbb{Z}^2 : L] \le \eta(N)$,*

$$\sum_{(x,y)\in S\cap[-N,N]^2\cap L} g(x,y) \ll \frac{\epsilon(N)N^2}{[\mathbb{Z}^2 : L]}. \tag{2.4.3}$$

Then, for every sector S and every lattice L of index $[\mathbb{Z}^2 : L] \le \eta(N)$,

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} g(x,y) \ll \max\left(\epsilon(N)\log\log N, \frac{1}{(\eta(N))^{1/2-\epsilon}}\right)\frac{N^2}{[\mathbb{Z}^2 : L]}.$$

Proof. For every positive integer a, let

$$S_a = \{0\},$$

$$\gamma(a) = [\mathbb{Z}^2 : L \cap a\mathbb{Z}^2],$$

$$f_a(0) = \begin{cases} 1 & \text{if } a = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$$g_a(0) = \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=a}} \lambda_K(P(x,y)).$$

Clearly

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} g(x,y).$$

By Lemma 4.2.1,

$$\begin{aligned}
\sum_{a=1}^{\infty} f_a(0)g_a(0) &= \sum_{\gamma(d)\le\eta(N)} \left(\sum_{d'|d}\mu(d')[d/d'=1]\right) \sum_{\substack{a\\ d|a}} g_a(0)\\
&\quad + 2\sum_{\eta(N)<\gamma(d)\le\eta(N)^2} \tau_3(a)\sum_{\substack{a\\ d|a}} |g_a(0)| + 2\sum_{\substack{p \text{ prime}\\ \gamma(p)>\eta(N)}}\sum_{\substack{a\\ d|a}} |g_a(0)|\\
&= \sum_{\gamma(d)\le M}\mu(d)\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ a|x,\, a|y}} g(x,y)\\
&\quad + 2\sum_{\eta(N)<\gamma(d)\le\eta(N)^2}\tau_3(d)\sum_{\substack{a\\ d|a}}\left|\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=a}} g(x,y)\right|\\
&\quad + 2\sum_{\substack{p \text{ prime}\\ \gamma(p)>\eta(N)}}\tau_3(d)\sum_{\substack{a\\ d|a}}\left|\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=a}} g(x,y)\right|.
\end{aligned}$$

Then, by (2.4.3),

$$\sum_{a=1}^{\infty} f_a(0)g_a(0) = \sum_{\gamma(d)\le\eta(N)}\frac{\epsilon(N)N^2}{\gamma(d)} + 2\sum_{\eta(N)<\gamma(d)\le\eta(N)^2}\tau_3(d)\frac{N^2}{\gamma(d)} + 2\sum_{\substack{p \text{ prime}\\ \gamma(p)>\eta(N)}}\frac{N^2}{\gamma(p)}.$$

We can assume that L is not contained in any set of the form $a\mathbb{Z}^2$, $a>1$, as otherwise the statement is trivial. Thus $\gamma(d) = d\cdot\operatorname{lcm}(d,[\mathbb{Z}^2:L])$. Hence

$$\sum_{d=1}^{\infty}\frac{1}{\gamma(d)} \le \sum_{d'|[\mathbb{Z}^2:L]}\frac{1}{d'[\mathbb{Z}^2:L]}\sum_{d}\frac{1}{d^2} \ll \sum_{d'|[\mathbb{Z}^2:L]}\frac{1}{d'[\mathbb{Z}^2:L]},$$

$$\sum_{\gamma(d)>\eta(N)} \frac{\tau_3(d)}{\gamma(d)} = \sum_{d'|[\mathbb{Z}^2:L]} \frac{\tau_3(d')}{d'[\mathbb{Z}^2:L]} \sum_{d>(\eta(N)/d')^{1/2}} \frac{\tau_3(d)}{d^2} \ll \sum_{d'|[\mathbb{Z}^2:L]} \frac{\tau_3(d')}{[\mathbb{Z}^2:L]\sqrt{d'\eta(N)}}.$$

By 2.4.3,

$$\sum_{d'|[\mathbb{Z}^2:L]} \frac{1}{d'} \ll \log\log N.$$

Clearly

$$\sum_{d'|[\mathbb{Z}^2:L]} \frac{\tau_3(d')}{\sqrt{d'}} \ll \tau_4([\mathbb{Z}^2:L]) \ll [\mathbb{Z}^2:L]^{\epsilon}.$$

The statement follows. □

Lemma 2.4.5. *Let K be a number field. Let $F \in \mathfrak{O}_K[x]$ be a square-free polynomial. Let a be an integer, m a positive integer. If $\mathfrak{A}_1(K, F, \delta(N))$ holds, then $\mathfrak{A}_1(K, F(mx+a), \delta(mN))$ holds.*

Proof. Immediate from the statement of Conjecture $\mathfrak{A}_1$. □

Lemma 2.4.6. *Let K be a number field. Let $F \in \mathfrak{O}_K[x, y]$ be a square-free homogeneous polynomial. Let $A \in SL_2(\mathbb{Z})$, $m_A = \max(|a_{11}| + |a_{12}|, |a_{21}| + |a_{22}|)$. If $\mathfrak{A}_2(K, F, \delta(N))$ holds, then $\mathfrak{A}_2(K, F(a_{11}x + a_{12}y, a_{21}x + a_{22}y), \delta(m_A N))$ holds.*

Proof. Immediate from the statement of Conjecture $\mathfrak{A}_2$. □

Lemma 2.4.7. *Let K be a number field. Let $F, G \in \mathfrak{O}_K[x]$ be square-free polynomials without common factors. Then $\mathfrak{A}_1(K, F \cdot G, \delta(N))$ holds if and only if $\mathfrak{A}_1(K, F, \delta(N))$ and $\mathfrak{A}_2(K, G, \delta(N))$ both hold.*

Proof. We can assume $N^{1/2}$ to be larger than $\max_{\mathfrak{p}|\operatorname{Disc}(F,G)} \rho(\mathfrak{p})$. Then, for any $\mathfrak{p}$ such that $\rho(\mathfrak{p}) > N$, we have that $\mathfrak{p}$ cannot divide both $F(x)$ and $G(x)$. Hence

$$\{1 \le x \le N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p}) > N^{1/2}, \mathfrak{p}^2 | F(x)\}$$

equals

$$\{1 \le x \le N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p}) > N^{1/2}, \mathfrak{p}^2 | G(x)\} \ \cup$$
$$\{1 \le x \le N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p}) > N^{1/2}, \mathfrak{p}^2 | F(x) \cdot G(x)\}.$$

□

Lemma 2.4.8. *Let K be a number field. Let $F, G \in \mathfrak{O}_K[x, y]$ be square-free homogenous polynomials without common factors. Then $\mathfrak{A}_2(K, F \cdot G, \delta(N))$ holds if and only if $\mathfrak{A}_2(K, F, \delta(N))$ and $\mathfrak{A}_2(K, G, \delta(N))$ both hold.*

Proof. Same as that of Lemma 2.4.7. □

Lemma 2.4.9. *Let K be a number field. Let $F, G, H \in \mathfrak{O}_K[x]$ be square-free polynomials. Assume that F, G and H are coprime as elements of $K[x]$. Then there is an ideal $\mathfrak{m}$ such that, for any $\mathfrak{M} \in I_K$, $\mathfrak{m} | \mathfrak{M}$, we can tell*

$$\mathrm{sq}_K(F(x)H(x))/\gcd(\mathrm{sq}_K(F(x)H(x)), \mathfrak{M}^\infty) \quad \textit{and}$$
$$\mathrm{sq}_K(G(x)H(x))/\gcd(\mathrm{sq}_K(G(x)H(x)), \mathfrak{M}^\infty)$$

from

$$\mathrm{sq}_K(F(x)G(x)H(x))/\gcd(\mathrm{sq}_K(F(x)G(x)H(x)), \mathfrak{M}^\infty)$$

and $x \bmod \mathfrak{p}$ for $\mathfrak{p} | \mathrm{sq}_K(F(x)G(x)H(x))$, $\mathfrak{p} \nmid \mathfrak{M}$.

Proof. Let $\mathfrak{m} = \mathrm{Disc}(F, G) \cdot \mathrm{Disc}(F, H) \cdot \mathrm{Disc}(G, H)$. Take a prime ideal $\mathfrak{p} \nmid \mathfrak{M}$. Suppose

$$\mathfrak{p} | (\mathrm{sq}_K(F(x)G(x)H(x))/\gcd(\mathrm{sq}_K(F(x)G(x)H(x)), \mathfrak{M}^\infty)).$$

We can tell which one of $\mathrm{sq}_K(F(x))$, $\mathrm{sq}_K(G(x))$ or $\mathrm{sq}_K(H(x))$ is divided by $\mathfrak{p}$ if we know which one of $F(x)$, $G(x)$, $H(x)$ is divided by $\mathfrak{p}$. The latter question can be answered given $x \bmod \mathfrak{p}$. □

Given two square-free polynomials $A, B \in \mathfrak{O}_K[x]$, we can always find square-free polynomials $F, G, H \in \mathfrak{O}_K[x]$ such that

- F, G and H are pairwise coprime as elements of $K[x]$,
- $A = FH$, $B = GH$.

Write $\mathrm{Lcm}(A, B)$ for $F \cdot G \cdot H$. Notice that $\mathrm{Lcm}(A, B)$ is defined only up to multiplication by a unit of $\mathfrak{O}_K$.

Corollary 2.4.10. *Let K be a number field. Let $A, B \in \mathfrak{O}_K[x]$ be square-free polynomials. Then there is an ideal $\mathfrak{m}_{A,B}$ such that, for any $\mathfrak{M} \in I_K$, $\mathfrak{m}_{A,B}|\mathfrak{M}$, we can tell*

$$\mathrm{sq}_K(A(x))/\gcd(\mathrm{sq}_K(A(x)), \mathfrak{m}^\infty) \quad \textit{and}$$
$$\mathrm{sq}_K(B(x))/\gcd(\mathrm{sq}_K(B(x)), \mathfrak{m}^\infty)$$

from

$$\mathrm{sq}_K(\mathrm{Lcm}(A, B)(x))/\gcd(\mathrm{sq}_K(\mathrm{Lcm}(A, B)(x)), \mathfrak{M}^\infty)$$

and $x \bmod \mathfrak{p}$ for $\mathfrak{p}|\,\mathrm{sq}_K(\mathrm{Lcm}(A, B))$, $\mathfrak{p} \nmid \mathfrak{M}$.

Proof. Immediate from Lemma 2.4.9. □

We can define Lcm for homogeneous polynomials in two variables in the same way we defined it for polynomials in one variable.

Lemma 2.4.11. *Let K be a number field. Let $A, B \in \mathfrak{O}_K[x, y]$ be homogeneous square-free polynomials. Then there is an ideal $\mathfrak{m}_{A,B}$ such that, for any $\mathfrak{M} \in I_K$, $\mathfrak{m}_{A,B}|\mathfrak{M}$, we can tell, for x, y coprime,*

$$\mathrm{sq}_K(A(x, y))/\gcd(\mathrm{sq}_K(A(x, y)), \mathfrak{M}^\infty) \quad \textit{and}$$
$$\mathrm{sq}_K(B(x, y))/\gcd(\mathrm{sq}_K(B(x, y)), \mathfrak{M}^\infty)$$

from

$$\mathrm{sq}_K(\mathrm{Lcm}(A, B)(x, y))/\gcd(\mathrm{sq}_K(\mathrm{Lcm}(A, B)(x, y)), \mathfrak{M}^\infty)$$

and $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}} \in \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$ for $\mathfrak{p}|\,\mathrm{sq}_K(\mathrm{Lcm}(A, B))$, $\mathfrak{p} \nmid \mathfrak{M}$.

Proof. Same as for Lemma 2.4.9 and Corollary 2.4.10. □

2.5 The global root number and its distribution

2.5.1 Background and definitions

We may as well start by reviewing the valuative criteria for the reduction type of an elliptic curve. Let K_v be a Henselian field of characteristic neither 2 nor 3. Let E be an elliptic curve over K_v. Let $c_4, c_6, \Delta \in K_v$ be a set of parameters corresponding to E. Then the reduction of E at v is

- *good* if $v(c_4) = 4k$, $v(c_6) = 6k$, $v(\Delta) = 12k$ for some integer k;
- *multiplicative* if $v(c_4) = 4k$, $v(c_6) = 6k$, $v(\Delta) > 12k$ for some integer k;
- *additive* and *potentially multiplicative* if $v(c_4) = 4k + 2$, $v(c_6) = 6k + 3$ and $v(\Delta) > 12k + 6$ for some integer k;
- *additive* and *potentially good* in all remaining cases.

From now on, K will be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$ given by $c_4, c_6 \in K(t)$. Let $q_0 \in K(t)$ be a generator of the fractional ideal of $K(t)$ consisting of all $q \in K(t)$ such that $q^4 c_4$ and $q^6 c_6$ are both in $K[t]$. Choose $q_1 \in \mathfrak{O}_K - \{0\}$ such that $(q_1 q_0)^4 c_4$, $(q_1 q_0)^6 c_6$ and $(q_1 q_0)^{12}\Delta = (q_1 q_0)^{12} \frac{c_4^3 - c_6^2}{1728}$ are all in $\mathfrak{O}_K[t]$. Let $Q(x, y) = q_1 q_0 (y/x) x^{\max(\lceil \deg(q_0^4 c_4)/4 \rceil, \lceil \deg(q_0^6 c_6)/6 \rceil)}$. Then

$$C_4(x, y) = Q^4(x, y) c_4(y/x),$$
$$C_6(x, y) = Q^6(x, y) c_6(y/x),$$
$$D(x, y) = Q^{12}(x, y)\Delta(y/x)$$

are homogeneous polynomials in $\mathfrak{O}_K[x, y]$. Note that $\deg C_6(x, y) = 6 \deg Q$, and thus $\deg C_6$ is even.

We define P_v as in the introduction: for v a place of $K(t)$, let $P_v \in \mathfrak{O}_K[t_0, t_1]$ to be $P_v = t_0$ if v is the place $\deg(\text{den}) - \deg(\text{num})$, $P_v = t_0^{\deg Q} Q\left(\frac{t_1}{t_0}\right)$ if v is given by a primitive irreducible polynomial $Q_v \in \mathfrak{O}_K[t]$. (We now note that, for any v, there are several possible choices for Q_v, all the same up to multiplication by elements of $\mathfrak{O}_K^*$; we choose one Q_v for each v arbitrarily and fix it once and for all.) We can write

$$\begin{aligned} C_4(x,y) &= C_{4,0} \prod_v (P_v(x,y))^{e_{v,4}}, \\ C_6(x,y) &= C_{6,0} \prod_v (P_v(x,y))^{e_{v,6}}, \\ D(x,y) &= D_0 \prod_v (P_v(x,y))^{e_{v,D}}, \end{aligned} \tag{2.5.1}$$

where $C_{4,0}, C_{6,0}, D_0 \in \mathfrak{O}_K[x,y]$, $e_{v,4}, e_{v,6}, e_{v,D} \geq 0$. For all but finitely many places v of $K(t)$, we have $e_{v,4} = 0$, $e_{v,6} = 0$, $e_{v,D} = 0$.

For any place v of $K(t)$, we can localize $\mathcal{E}$ at v, thus making it an elliptic curve over the Henselian field $(K(t))_v$, and then reduce it modulo v. We can restate the the standard valuative criteria for the reduction type in terms of $e_{v,4}$, $e_{v,6}$, $e_{v,D}$. The reduction of $\mathcal{E}$ at v is

- good if $e_{v,D} = 0$,
- multiplicative if $e_{v,4} = 0$, $e_{v,6} = 0$, $e_{v,D} > 0$,
- additive and potentially multiplicative if $e_{v,4} = 2$, $e_{v,6} = 3$, $e_{v,D} > 6$,
- additive and potentially good in all remaining cases.

As before, let $\mathbb{A} = \{(x,y) \in \mathfrak{O}_K : x,\ y \text{ coprime}\}$. Let

$$\mathbb{A}_{\mathcal{E}} = \{(x,y) \in \mathbb{A} : x \neq 0, c_4(y/x) \neq \infty, c_6(y/x) \neq \infty, \Delta(y/x) \neq 0, \infty,\ q_0(y/x) \neq 0\}. \tag{2.5.2}$$

Let $(x, y) \in \mathbb{A}_{\mathcal{E}}$. Then $c_4(y/x)$ (resp. $c_6(y/x)$, $\Delta(y/x)$) differs from $C_4(x, y)$ (resp. $C_6(x, y)$, $\Delta(x, y)$) by a non-zero fourth power $Q^4(x, y)$ (resp. a non-zero sixth power $Q^6(x, y)$, a non-zero twelfth power $Q^{12}(x, y)$). Hence, for every prime ideal $\mathfrak{p} \in I_K$, the reduction of $\mathcal{E}(y/x)$ at $\mathfrak{p}$ is

- good if $v_{\mathfrak{p}}(C_4(x, y)) = 4k$, $v_{\mathfrak{p}}(C_6(x, y)) = 6k$, $v_{\mathfrak{p}}(D(x, y)) = 12k$ for some integer k;
- multiplicative if $v_{\mathfrak{p}}(C_4(x, y)) = 4k$, $v_{\mathfrak{p}}(C_6(x, y)) = 6k$, $v_{\mathfrak{p}}(D(x, y)) > 12k$ for some integer k;
- additive and potentially multiplicative if $v_{\mathfrak{p}}(C_4(x, y)) = 4k + 2$, $v_{\mathfrak{p}}(C_6(x, y)) = 6k + 3$ and $v_{\mathfrak{p}}(D(x, y)) > 12k + 6$ for some integer k;
- additive and potentially good in all remaining cases.

The *root number* of an elliptic curve over a global field K is the product of its local root numbers

$$W(E) = \prod_v W_v(E)$$

over all places v of K. Similarly, given $\mathfrak{d} \in I_K$, we define the *putative root number* $V_{\mathfrak{d}}(\mathcal{E})$ of an elliptic curve $\mathcal{E}$ over $K(t)$ to be the product of its local putative root numbers

$$V_{\mathfrak{d}}(\mathcal{E}) = \prod_v V_{\mathfrak{d},v}(E)$$

over all places v of $K(t)$. We will define *local putative root numbers* shortly. Note for now that $V^{\mathfrak{d},v}(\mathcal{E}) = 1$ for all but finitely many places v of $K(t)$, just as $W_v(E) = 1$ for all but finitely many places v of K.

Proposition 2.5.1. *Let K be a number field. Let $\mathfrak{p}$ be prime ideal of K unramified over $\mathbb{Q}$. Assume $\mathfrak{p}$ lies over a rational prime p greater than three. Let E be an elliptic curve over K whose reduction at $\mathfrak{p}$ is additive and potentially good. Then*

1. $W_{\mathfrak{p}}(E) = \left(\frac{-1}{\mathfrak{p}}\right)$ *if* $v_{\mathfrak{p}}(\Delta(E))$ *is even but not divisible by four,*

2. $W_{\mathfrak{p}}(E) = \left(\frac{-2}{\mathfrak{p}}\right)$ *if* $v_{\mathfrak{p}}(\Delta(E))$ *is odd and divisible by three,*

3. $W_{\mathfrak{p}}(E) = \left(\frac{-3}{\mathfrak{p}}\right)$ *if* $v_{\mathfrak{p}}(\Delta(E))$ *is divisible by four but not by three.*

Proof. Let a be any rational integer not divisible by $\mathfrak{p}$. If $\deg(K_{\mathfrak{p}}/\mathbb{Q}_p)$ is even, then $\left(\frac{a}{\mathfrak{p}}\right) = 1$. If $\deg(K_{\mathfrak{p}}/\mathbb{Q}_p)$ is odd, then $\left(\frac{a}{\mathfrak{p}}\right) = \left(\frac{a}{p}\right)$. Apply [Ro2], Theorem 2, to the case of the trivial one-dimensional representation. $\square$

Define $M_{\mathcal{E}}$, $B_{\mathcal{E}}$, $B'_{\mathcal{E}}$ as in (1.2.1) and (1.3.1). Let $[a,b]_{\mathfrak{d}}$ be as in (2.3.2). Let $\mathfrak{d}_0 \in I_K$ be the principal ideal generated by

$$6\, D_0 \prod_{\substack{v_1 \neq v_2 \\ \mathcal{E} \text{ has bad red. at } v_1,\, v_2}} \operatorname{Res}(P_{v_1}, P_{v_2}), \tag{2.5.3}$$

where D_0 is as in (2.5.1).

Definition 6. *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let $\mathfrak{d} \in I_K$ be an ideal divisible by $\mathfrak{d}_0$. Let v be a place of $K(t)$. Define the* local putative root number *$V_v(\mathcal{E})$ to be a map from $\mathbb{A}_{\mathcal{E}}$ to $\{-1, 1\}$ whose values are given as follows:*

1. $V_{\mathfrak{d},v}(\mathcal{E}) = 1$ *if the reduction $\mathcal{E} \bmod v$ is good,*

2. $V_{\mathfrak{d},v}(\mathcal{E}) = \lambda_K(P_v(x,y)) \cdot [-C_6(x,y), P_v(x,y)]_{\mathfrak{d}}$ *if the reduction is multiplicative,*

3. $V_{\mathfrak{d},v}(\mathcal{E}) = [-1, P_v(x,y)]_{\mathfrak{d}}$ *if the reduction is additive and potentially multiplicative,*

4. $V_{\mathfrak{d},v}(\mathcal{E}) = [-1, P_v(x,y)]_{\mathfrak{d}}$ *if the reduction is additive and potentially good, and $v(\Delta)$ is even but not divisible by four,*

5. $V_{\mathfrak{d},v}(\mathcal{E}) = [-2, P_v(x,y)]_{\mathfrak{d}}$ *if the reduction is additive and potentially good, and $v(\Delta)$ is odd and divisible by three,*

6. $V_{\mathfrak{d},v}(\mathcal{E}) = [-3, P_v(x,y)]_{\mathfrak{d}}$ *if the reduction is additive and potentially good, and* $v(\Delta)$ *is divisible by four but not by three.*

We define *half bad* and *quite bad* reduction as in section 1.3. The reduction of $\mathcal{E}$ at v is

- *half bad* if $e_{v,4} \geq 2$, $e_{v,6} \geq 3$, $e_{v,D} = 6$,
- *quite bad* if it is bad but not half bad.

The reduction of $\mathcal{E}(y/x)$ at $\mathfrak{p}$ is

- *half bad* if $v_{\mathfrak{p}}(C_4(x,y)) \geq 4k+2$, $v_{\mathfrak{p}}(C_6(x,y)) \geq 6k+3$ and $v_{\mathfrak{p}}(D(x,y)) = 12k+6$ for some integer k,
- *quite bad* if it is bad but not half bad.

It should be clear that half-bad reduction is a special case of additive, potentially good reduction.

As in subsection 1.2, we set $W(\mathcal{E}(y/x)) = 1$ when $\mathcal{E}(y/x)$ is undefined or singular. Note that the set $\{x, y \in \mathfrak{O}_K : \gcd(x,y) = 1, \mathcal{E}(y/x) \text{ undefined or singular}\}$ is finite, as is its superset $\{x, y \in \mathfrak{O}_K : \gcd(x,y) = 1\} - \mathbb{A}_{\mathcal{E}}$.

2.5.2 From the root number to Liouville's function

Lemma 2.5.2. *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let $\mathfrak{d}_0$ be as in 2.5.3. Let $\mathfrak{d} \in I_K$ be an ideal divisible by $\mathfrak{d}_0$. The putative root number $V_{\mathfrak{d}}(\mathcal{E})$ is of the form*

$$V_{\mathfrak{d}}(\mathcal{E}) = f(x,y) \cdot \lambda_K(M_{\mathcal{E}}(x,y)),$$

where f is a pliable function on $\{(x,y) \in \mathfrak{O}_K^2 : x,\ y \text{ coprime}\}$.

Proof. Let v be a place of $\mathcal{E}$. If the reduction of $\mathcal{E}$ at v is good, then $V_{\mathfrak{d},v}(\mathcal{E})$ is equal to the constant 1 and hence is pliable. If the reduction of $\mathcal{E}$ at v is additive, $V_{\mathfrak{d},v}(\mathcal{E})$

is pliable by properties (4) and (5) of $[,]_{\mathfrak{d}}$ (see subsection 2.3.3). If the reduction of $\mathcal{E}$ at v is multiplicative, then $V_{\mathfrak{d},v}(\mathcal{E})$ is equal to the product of $\lambda_K(P_v(x,y))$ and a pliable function by Corollary 2.3.29 and by the fact that $\deg(C_6(x,y))$ is even.

The reduction of $\mathcal{E}$ at v is bad for only a finite number of places v. Since the product of finitely many pliable functions is pliable, we obtain

$$V_{\mathfrak{d}}(\mathcal{E}) = f(x,y) \prod_{\mathcal{E} \text{ has mult. red. at } v} \lambda_K(P_v(x,y)) = f(x,y) \cdot \lambda_K(M_{\mathcal{E}}(x,y)),$$

where $f(x,y)$ is a pliable function on $\{(x,y) \in \mathfrak{O}_K^2 : x,\, y \text{ coprime}\}$. □

Lemma 2.5.3. *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let v be a place of $K(t)$ where $\mathcal{E}$ has bad reduction. Let $\mathbb{A}_{\mathcal{E}}$ be as in (2.5.2). Let $\mathfrak{d}$ be as in (2.5.3). Then, for any $(x,y) \in \mathbb{A}_{\mathcal{E}}$,*

$$\prod_{\substack{\mathfrak{p} \nmid \mathfrak{d} \\ \mathfrak{p} | P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = g_v(x,y) \cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) \qquad \textit{if } v \textit{ is half bad,}$$

$$\prod_{\substack{\mathfrak{p} \nmid \mathfrak{d} \\ \mathfrak{p} | P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = g_v(x,y) \cdot h(\mathrm{sq}_K(P_v(x,y)), x, y) \cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) \quad \textit{if } v \textit{ is quite bad,}$$

where $g_v : \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$, $h : I_K \times \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$ satisfy the following conditions:

1. *g_v is pliable,*
2. *$h(\mathfrak{a},x,y)$ depends only on $\mathfrak{a}$ and on $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$,*
3. *$h(\mathfrak{a}_1\mathfrak{a}_2,x,y) = h(\mathfrak{a}_1,x,y)h(\mathfrak{a}_2,x,y)$ for any $\mathfrak{a}_1, \mathfrak{a}_2 \in I_K$,*
4. *$h(\mathfrak{a},x,y) = 1$ for $\mathfrak{a}|\mathfrak{d}^\infty$.*

Proof. The reduction of $\mathcal{E}$ at v can be multiplicative or additive. If it is additive, it can be potentially multiplicative or potentially good. If it is additive and potentially good, it can be half bad or quite bad. If it is additive, potentially good and quite bad, then $\gcd(e_{v,D}, 12)$ is 2, 3 or 4. We speak of reduction type pg_2, pg_3, pg_4 accordingly.

We will construct $h_m, h_{mp}, h_{pg_2}, h_{pg_3}, h_{pg_4} : I_K \times \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$, each of them satisfying the conditions (2)-(4) enunciated for h in the statement. We will also define a pliable function $g_v : \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$ depending on v. Our aim is to prove that $\prod_{\mathfrak{p}\nmid\mathfrak{d},\mathfrak{p}|P_v(x,y)} W_{\mathfrak{p}}(\mathcal{E}(y/x))$ equals

$$\begin{aligned}
g_v(x,y)\cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) &\text{ if } \mathcal{E} \bmod v \text{ is half bad,}\\
g_v(x,y)\cdot h_{pg_2}(\mathrm{sq}(P_v(x,y)),x,y)\cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) &\text{ if } \mathcal{E} \bmod v \text{ is of type } pg_2,\\
g_v(x,y)\cdot h_{pg_3}(\mathrm{sq}(P_v(x,y)),x,y)\cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) &\text{ if } \mathcal{E} \bmod v \text{ is of type } pg_3,\\
g_v(x,y)\cdot h_{pg_4}(\mathrm{sq}(P_v(x,y)),x,y)\cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) &\text{ if } \mathcal{E} \bmod v \text{ is of type } pg_4,\\
g_v(x,y)\cdot h_{pm}(\mathrm{sq}(P_v(x,y)),x,y)\cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) &\text{ if } \mathcal{E} \bmod v \text{ is additive and pot. mult.,}\\
g_v(x,y)\cdot h_{m}(\mathrm{sq}(P_v(x,y)),x,y)\cdot V_{\mathfrak{d},v}(\mathcal{E})(x,y) &\text{ if } \mathcal{E} \bmod v \text{ is multiplicative.}
\end{aligned} \tag{2.5.4}$$

Then we can define $h : I_K \times \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$ to be the function such that $h(\mathfrak{p}^n, x, y) = 1$ for $\mathfrak{p}|\mathfrak{d}$,

$$h(\mathfrak{p}^n,x,y) = \begin{cases} h_m(\mathfrak{p}^n,x,y) & \text{if } \mathfrak{p}|\prod_{v \text{ mult.}} P_v(x,y),\\ h_{mp}(\mathfrak{p}^n,x,y) & \text{if } \mathfrak{p}|\prod_{v \text{ add. and pot. mult.}} P_v(x,y),\\ h_{pg_2}(\mathfrak{p}^n,x,y) & \text{if } \mathfrak{p}|\prod_{v \text{ is } pg_2} P_v(x,y),\\ h_{pg_3}(\mathfrak{p}^n,x,y) & \text{if } \mathfrak{p}|\prod_{v \text{ is } pg_3} P_v(x,y),\\ h_{pg_4}(\mathfrak{p}^n,x,y) & \text{if } \mathfrak{p}|\prod_{v \text{ is } pg_4} P_v(x,y),\\ 1 & \text{otherwise} \end{cases} \tag{2.5.5}$$

for $\mathfrak{p} \nmid \mathfrak{d}$, and $h(\mathfrak{a}_1\mathfrak{a}_2, x, y) = h(\mathfrak{a}_1, x, y)h(\mathfrak{a}_2, x, y)$ for any $\mathfrak{a}_1, \mathfrak{a}_2 \in I_K$.

First note that no more than one case can hold in (2.5.5), as $\mathfrak{p} \nmid \mathfrak{d}$ implies that $\mathfrak{p}$ cannot divide both $P_v(x,y)$ and $P_u(x,y)$ for v, u distinct (see (2.5.3)). Notice, too, that condition (2) in the statement is fulfilled: since P_v is homogeneous, whether

or not $\mathfrak{p}|P_v(x,y)$ for given x, y depends only on $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}$. Finally, it is an immediate consequence of (2.5.5) that

$$h(\mathrm{sq}_K(P_v(x,y)),x,y) = \begin{cases} h_m(\mathrm{sq}_K(P_v(x,y)),x,y) & \text{if } \mathcal{E} \bmod v \text{ is multiplicative,} \\ h_{pm}(\mathrm{sq}(P_v(x,y)),x,y) & \text{if } \mathcal{E} \bmod v \text{ is add. and pot. m.,} \\ h_{pg_2}(\mathrm{sq}(P_v(x,y)),x,y) & \text{if } \mathcal{E} \bmod v \text{ is } pg_2 \\ h_{pg_3}(\mathrm{sq}(P_v(x,y)),x,y) & \text{if } \mathcal{E} \bmod v \text{ is } pg_3 \\ h_{pg_4}(\mathrm{sq}(P_v(x,y)),x,y) & \text{if } \mathcal{E} \bmod v \text{ is } pg_4. \end{cases}$$

The statement then follows from (2.5.4). It remains to construct g_v, h_m, h_{pm}, h_{pg_2}, h_{pg_3}, h_{pg_4} and to prove (2.5.4).

Let $e_{v,4}$ $e_{v,6}$, $e_{v,D}$ be as in (2.5.1). Suppose $\mathfrak{p} \nmid \mathfrak{d}$, $\mathfrak{p}|P_v(x,y)$. Then $\mathfrak{p} \nmid P_u(x,y)$ for every $u \neq v$. Hence

$$\begin{aligned} v_{\mathfrak{p}}(C_4(x,y)) &= e_{v,4} \cdot v_{\mathfrak{p}}(P_v(x,y)), \\ v_{\mathfrak{p}}(C_6(x,y)) &= e_{v,6} \cdot v_{\mathfrak{p}}(P_v(x,y)), \\ v_{\mathfrak{p}}(D(x,y)) &= e_{v,D} \cdot v_{\mathfrak{p}}(P_v(x,y)). \end{aligned} \tag{2.5.6}$$

Case 1: $\mathcal{E}$ has multiplicative reduction at v. We are given that $e_{v,4} = 0$, $e_{v,6} = 0$, $e_{v,D} > 0$. Hence $v_{\mathfrak{p}}(C_4(x,y)) = 0$, $v_{\mathfrak{p}}(C_6(x,y)) = 0$, $v_{\mathfrak{p}}(D(x,y)) > 0$. Therefore, $\mathcal{E}(y/x)$ has multiplicative reduction at $\mathfrak{p}$. By Lemma 2.3.21,

$$W_{\mathfrak{p}}(\mathcal{E}(y/x)) = -\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right).$$

Thus

$$\begin{aligned}
\prod_{\substack{\mathfrak{p}\nmid\mathfrak{d}\\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) &= \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d}\\ \mathfrak{p}|P_v(x,y)}} \left(-\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)\right) \\
&= \prod_{\substack{\mathfrak{p}|\mathfrak{d}\\ \mathfrak{p}|P_v(x,y)}} (-1)^{v_{\mathfrak{p}}(P_v(x,y))} \prod_{\mathfrak{p}\nmid\mathfrak{d},\mathfrak{p}^2|P_v(x,y)} (-1)^{v_{\mathfrak{p}}(P_v(x,y))-1} \\
&\cdot \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d}\\ \mathfrak{p}^2|P_v(x,y)}} \left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(P_v(x,y))-1} \\
&\cdot \prod_{\mathfrak{p}|P_v(x,y)} (-1)^{v_{\mathfrak{p}}(P_v(x,y))} \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d}\\ \mathfrak{p}|P_v(x,y)}} \left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(P_v(x,y))}.
\end{aligned}$$

Let

$$\begin{aligned}
g_v(x,y) &= \prod_{\mathfrak{p}|\mathfrak{d},\mathfrak{p}|P_v(x,y)} (-1)^{v_{\mathfrak{p}}(P_v(x,y))}, \\
h_m(\mathfrak{a},x,y) &= \lambda_K\left(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{d}^\infty)}\right)\cdot[-C_6(x,y),\mathfrak{a}]_{\mathfrak{d}}.
\end{aligned}$$

Then $\prod_{\mathfrak{p}\nmid\mathfrak{d},\mathfrak{p}|P_v(x,y)} W_{\mathfrak{p}}(\mathcal{E}(y/x))$ is

$$g_v(x,y)\cdot h_m(\mathrm{sq}_K(P_v(x,y)),x,y)\cdot\lambda_K(P_v(x,y))[-C_6(x,y),P_v(x,y)]_{\mathfrak{d}}. \tag{2.5.7}$$

The map $t\mapsto(-1)^{v_{\mathfrak{p}}(t)}$ on K is pliable. Hence, by Proposition 2.3.5, $(x,y)\mapsto(-1)^{v_{\mathfrak{p}}(P_v(x,y))}$ is a pliable function on A. Since $g_v(x,y)$ equals $\prod_{\mathfrak{p}|\mathfrak{d}}(-1)^{v_{\mathfrak{p}}(P_v(x,y))}$, which is a product of finitely many pliable functions, $g_v(x,y)$ is pliable.

It remains to show that $h_m(\mathfrak{a},x,y)$ depends only on $\mathfrak{a}$ and $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}$. For fixed $\mathfrak{a}$, the first factor $\lambda_K\left(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{d}^\infty)}\right)$ is a constant. Since

$$[-C_6(x,y),\mathfrak{a}]_{\mathfrak{d}} = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d}\\ \mathfrak{p}|\mathfrak{a}}}\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\mathfrak{a})},$$

it is enough to show that $\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)$ depends only on $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}$ for every prime $\mathfrak{p}$ with $\mathfrak{p}|\mathfrak{a}$, $\mathfrak{p} \nmid \mathfrak{d}$. For every $t \in \mathfrak{O}_K^*$,

$$\left(\frac{-C_6(rx,ry)}{\mathfrak{p}}\right) = \left(\frac{-r^{\deg C_6} C_6(x,y)}{\mathfrak{p}}\right) = \left(\frac{r}{\mathfrak{p}}\right)^{\deg C_6} \left(\frac{-C_6(x,y)}{\mathfrak{p}}\right).$$

Since $\deg C_6$ is even, it follows that

$$\left(\frac{-C_6(rx,ry)}{\mathfrak{p}}\right) = \left(\frac{-C_6(x,y)}{\mathfrak{p}}\right).$$

Hence $\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)$ depends only on $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}$. Therefore $h_m(\mathfrak{a}, x, y)$ depends only on $\mathfrak{a}$ and $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}$.

We have shown that g_v and h_v in (2.5.7) satisfy properties (1) and (2) in the statement. Properties (3) and (4) are immediate from (2.5.2). Since $V_{\mathfrak{d},v}(\mathcal{E})(x,y) = \lambda_K(P_v(x,y))[-C_6(x,y), P_v(x,y)]_{\mathfrak{d}}$, we are done.

Case 2: $\mathcal{E}$ has additive, potentially multiplicative reduction at v. We are given $e_{v,4} = 2$, $e_{v,6} = 3$, $e_{v,D} > 6$. Let $\mathfrak{p}$ be a prime ideal dividing $P_v(x,y)$ but not $\mathfrak{d}$. Then $v_{\mathfrak{p}}(C_4(x,y)) = 4k$, $v_{\mathfrak{p}}(C_6(x,y)) = 6k$, $v_{\mathfrak{p}}(D(x,y)) > 12k$ if $v_{\mathfrak{p}}(P_v(x,y)) = 2k$, $k > 0$, and $v_{\mathfrak{p}}(C_4(x,y)) = 4k+2$, $v_{\mathfrak{p}}(C_6(x,y)) = 6k+3$, $v_{\mathfrak{p}}(D(x,y)) > 12k+6$ if $v_{\mathfrak{p}}(P_v(x,y)) = 2k+1$, $k \geq 0$. Thus, $\mathcal{E}(y/x)$ has multiplicative reduction at $\mathfrak{p}$ if $v_{\mathfrak{p}}(P_v(x,y))$ is even and positive, but has additive, potentially multiplicative reduction if $v_{\mathfrak{p}}(P_v(x,y))$ is odd.

Hence, by Lemma 2.3.21,

$$\prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y) \\ v_{\mathfrak{p}}(P_v(x,y)) \text{ even}}} -\left(\frac{-C_6(x,y)\mathfrak{p}^{-v_{\mathfrak{p}}(C_6(x,y))}}{\mathfrak{p}}\right) \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y) \\ v_{\mathfrak{p}}(P_v(x,y)) \text{ odd}}} \left(\frac{-1}{\mathfrak{p}}\right)$$

$$= h_{pm}(\mathrm{sq}_K(P_v(x,y)), x, y) \cdot [-1, P_v(x,y)]_{\mathfrak{d}},$$

where $h_{pm}(\mathfrak{a}, x, y) = \prod_{\mathfrak{p}|\mathfrak{d}, \mathfrak{p}\nmid\mathfrak{a}} \left(-\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)\right)^{v_{\mathfrak{p}}(a)}$. It is clear that $h_{pm}(\mathfrak{a}, x, y)$ is multiplicative on $\mathfrak{a}$ and trivial for $\mathfrak{a}|\mathfrak{d}^\infty$. As shown above, $\left(\frac{-C_6(x,y)}{\mathfrak{p}}\right)$ depends only on $\mathfrak{p}$ and $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}$. Hence $h_{pm}(\mathfrak{a}, x, y)$ depends only on $\mathfrak{a}$ and $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}}$. Set $g_v(x, y) = 1$, Since $V_{\mathfrak{d},v}(\mathcal{E})(x, y) = [-1, P_v(x, y)]_{\mathfrak{d}}$,

$$\prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = g_v(x, y) \cdot h_{pm}(\mathrm{sq}_K(P_v(x, y)), x, y) \cdot V_{\mathfrak{d},v}(\mathcal{E})(x, y).$$

Case 3: $\mathcal{E}$ has half-bad reduction at v. We are given $e_{v,4} \geq 2$, $e_{v,6} \geq 3$, $e_{v,D} = 6$. Let $\mathfrak{p}$ be a prime ideal dividing $P_v(x, y)$ but not $\mathfrak{d}$. Then $v_{\mathfrak{p}}(C_4(x, y)) \geq 4k$, $v_{\mathfrak{p}}(C_6(x, y)) \geq 6k$, $v_{\mathfrak{p}}(D(x, y)) = 12k$ if $v_{\mathfrak{p}}(P_v(x, y)) = 2k$, $k > 0$, and $v_{\mathfrak{p}}(C_4(x, y)) \geq 4k + 2$, $v_{\mathfrak{p}}(C_6(x, y)) \geq 6k + 3$, $v_{\mathfrak{p}}(D(x, y)) = 12k + 6$ if $v_{\mathfrak{p}}(P_v(x, y)) = 2k + 1$, $k \geq 0$. Thus, $\mathcal{E}(y/x)$ has half-bad reduction at $\mathfrak{p}$ if $v_{\mathfrak{p}}(P_v(x, y))$ is odd, and good reduction if $v_{\mathfrak{p}}(P_v(x, y))$ is even. Hence, by Proposition 2.5.1,

$$W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \begin{cases} 1 & \text{if } v_{\mathfrak{p}}(P_v(x, y)) \text{ is even,} \\ \left(\frac{-1}{\mathfrak{p}}\right) & \text{if } v_{\mathfrak{p}}(P_v(x, y)) \text{ is odd.} \end{cases}$$

Thereby

$$\prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} \left(\frac{-1}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(P_v(x,y))} = [-1, P_v(x, y)]_{\mathfrak{d}} = V_{\mathfrak{d},v}(\mathcal{E})(x, y).$$

Set $g_v(x, y) = 1$.

Case 4: $\mathcal{E}$ has gp_2 reduction at v. We are given that the reduction is additive and $\gcd(e_{v,D}, 12) = 2$. Then the reduction of $\mathcal{E}(y/x)$ at $\mathfrak{p}$ is good if $6|v_{\mathfrak{p}}(P_v(x, y))$ and

additive and potentially good otherwise if $6 \nmid v_{\mathfrak{p}}(P_v(x,y))$. Hence

$$\gcd(v_{\mathfrak{p}}(D(x,y)),12) = \begin{cases} 2 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 1,5 \bmod 6, \\ 4 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 2,4 \bmod 6, \\ 6 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 3 \bmod 6. \end{cases}$$

So, by Proposition 2.5.1,

$$W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \begin{cases} 1 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 0 \bmod 6, \\ \left(\frac{-2}{\mathfrak{p}}\right) & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 3 \bmod 6, \\ \left(\frac{-1}{\mathfrak{p}}\right) & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \not\equiv 0 \bmod 3. \end{cases}$$

Let $H : I_K \to \{-1,1\}$ be the multiplicative function such that $H(\mathfrak{p}^n) = 1$ for $\mathfrak{p}|\mathfrak{d}$ and

$$H(\mathfrak{p}^n) = \begin{cases} 1 & \text{if } n \equiv 0,4,5 \bmod 6 \\ \left(\frac{-1}{\mathfrak{p}}\right) & \text{if } n \equiv 1,3 \bmod 6 \\ \left(\frac{2}{\mathfrak{p}}\right) & \text{if } n \equiv 2 \bmod 6 \end{cases}$$

for $\mathfrak{p} \nmid \mathfrak{d}$. Then

$$W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \begin{cases} \left(\frac{-1}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(P_v(x,y))} & \text{if } v_{\mathfrak{p}}(P_v(x,y)) = 1, \\ H(\mathfrak{p}^{v_{\mathfrak{p}}(P_v(x,y))-1}) \left(\frac{-1}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(P_v(x,y))} & \text{if } v_{\mathfrak{p}}(P_v(x,y)) > 1. \end{cases}$$

Hence

$$\begin{aligned} \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) &= \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}^2|P_v(x,y)}} H(\mathfrak{p}^{v_{\mathfrak{p}}(P_v(x,y))-1}) \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} \left(\frac{-1}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(P_v(x,y))} \\ &= H(\mathrm{sq}_K(P_v(x,y))) \cdot [-1, P_v(x,y)]_{\mathfrak{d}}. \end{aligned}$$

Set $g_v(x,y)=1$, $h_{gp_2}(\mathfrak{a},x,y)=H(\mathfrak{a})$ and we are done.

Case 5: $\mathcal{E}$ has gp_3 reduction at v. We are given that the reduction is additive and $\gcd(e_{v,D},12)=3$. Then

$$\gcd(v_{\mathfrak{p}}(D(x,y)),12)=\begin{cases}3 & \text{if } v_{\mathfrak{p}}(P_v(x,y))\equiv 1,3 \bmod 4,\\ 6 & \text{if } v_{\mathfrak{p}}(P_v(x,y))\equiv 2 \bmod 4,\\ 12 & \text{if } v_{\mathfrak{p}}(P_v(x,y))\equiv 0 \bmod 4.\end{cases}$$

So, by Proposition 2.5.1,

$$W_{\mathfrak{p}}(\mathcal{E}(y/x))=\begin{cases}1 & \text{if } v_{\mathfrak{p}}(P_v(x,y))\equiv 0 \bmod 4,\\ \left(\frac{-1}{\mathfrak{p}}\right) & \text{if } v_{\mathfrak{p}}(P_v(x,y))\equiv 2 \bmod 4,\\ \left(\frac{-2}{\mathfrak{p}}\right) & \text{if } v_{\mathfrak{p}}(P_v(x,y))\not\equiv 1 \bmod 2.\end{cases}$$

Let $H: I_K\to\{-1,1\}$ be the multiplicative function such that $H(\mathfrak{p}^n)=1$ for $\mathfrak{p}|\mathfrak{d}$ and

$$H(\mathfrak{p}^n)=\begin{cases}\left(\frac{2}{\mathfrak{p}}\right) & \text{if } n\equiv 1 \bmod 4\\ 1 & \text{if } n\not\equiv 1 \bmod 4\end{cases}$$

for $\mathfrak{p}\nmid\mathfrak{d}$. Then

$$\prod_{\substack{\mathfrak{p}\nmid\mathfrak{d}\\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x))=H(\mathrm{sq}_K(P_v(x,y)))\cdot[-2,P_v(x,y)]_{\mathfrak{d}}.$$

Set $g_v(x,y)=1$, $h_v(\mathfrak{a},x,y)=H(\mathfrak{a})$ and we are done.

Case 6: $\mathcal{E}$ has gp_4 reduction at v. We are given that the reduction is additive and

$\gcd(e_{v,D}, 12) = 4$. Then

$$\gcd(v_{\mathfrak{p}}(D(x,y)), 12) = \begin{cases} 4 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 1, 2 \bmod 3, \\ 12 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 0 \bmod 3. \end{cases}$$

So, by Proposition 2.5.1,

$$W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \begin{cases} 1 & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \equiv 0 \bmod 3, \\ \left(\frac{-3}{\mathfrak{p}}\right) & \text{if } v_{\mathfrak{p}}(P_v(x,y)) \not\equiv 0 \bmod 3. \end{cases}$$

Let $H : I_K \to \{-1, 1\}$ be the multiplicative function such that $H(\mathfrak{p}^n) = 1$ for $\mathfrak{p}|\mathfrak{d}$ and

$$H(\mathfrak{p}^n) = \begin{cases} \left(\frac{-3}{\mathfrak{p}}\right) & \text{if } n \equiv 1, 2, 3 \bmod 6 \\ 1 & \text{otherwise} \end{cases}$$

for $\mathfrak{p} \nmid \mathfrak{d}$. Then

$$\prod_{\substack{\mathfrak{p} \nmid \mathfrak{d} \\ \mathfrak{p} | P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = H(\mathrm{sq}_K(P_v(x,y))) \cdot [-3, P_v(x,y)]_{\mathfrak{d}}.$$

Set $g_v(x,y) = 1$, $h_v(\mathfrak{a}, x, y) = H(\mathfrak{a})$ and we are done. □

Proposition 2.5.4. *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let $\mathfrak{M} \in I_K$. Then there are $g : \mathbb{A}_{\mathcal{E}} \to \{-1, 1\}$, $h : I_K \times \mathbb{A}_{\mathcal{E}} \to \{-1, 1\}$ such that , for all $(x, y) \in \mathbb{A}_{\mathcal{E}}$,*

$$W(\mathcal{E}(y/x)) = g(x,y) \cdot h(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)), x, y) \cdot \lambda_K(M_{\mathcal{E}}(x,y)),$$

and, furthermore,

1. *g is pliable,*

2. *$h(\mathfrak{a}, x, y)$ depends only on $\mathfrak{a}$ and on $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$.*

3. *$h(\mathfrak{a}_1\mathfrak{a}_2, x, y) = h(\mathfrak{a}_1, x, y)h(\mathfrak{a}_2, x, y)$ for any $\mathfrak{a}_1, \mathfrak{a}_2 \in I_K$,*

4. *$h(\mathfrak{a}, x, y) = 1$ for $\mathfrak{a}|\mathfrak{M}^\infty$.*

Proof. For all $(x, y) \in \mathbb{A}_{\mathcal{E}}$, we can write

$$W(\mathcal{E}(y/x)) = W_\infty(\mathcal{E}(y/x)) \prod_{\mathfrak{p}} W_{\mathfrak{p}}(\mathcal{E}(y/x)).$$

It follows from the definition of local root numbers that $W_{\mathfrak{p}}(\mathcal{E}(y/x)) = 1$ when $\mathcal{E}(y/x)$ has good reduction at $\mathfrak{p}$ (see, e.g., [Ro], Sec. 19, Prop (i)). We also know that $W_\infty = -1$ (see, e.g., [Ro], Sec. 20). Let $\mathfrak{d} = \mathfrak{M} \cdot \mathfrak{d}_0$. Then

$$W(\mathcal{E}(y/x)) = -\prod_{\mathfrak{p}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \prod_{\mathfrak{p}|\mathfrak{d}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \cdot \prod_{\substack{\mathfrak{p}|\mathfrak{d} \\ \mathcal{E}(y/x) \text{ has bad red. at } \mathfrak{p}}} W_{\mathfrak{p}}(\mathcal{E}(y/x)).$$

Let $\mathfrak{p} \nmid \mathfrak{d}$ be a prime at which $\mathcal{E}(y/x)$ has bad reduction. Since

$$D(x, y) = D_0 \prod_v (P_v(x, y))^{e_{v,D}}$$

and $D_0|\mathfrak{d}$, we must have $\mathfrak{p}|P_v(x, y)$ for some place v with $e_{v,D} > 0$. By the definition (2.5.3) of $\mathfrak{d}$, it follows that $\mathfrak{p} \nmid P_u(x, y)$ for every place $u \neq v$ of $K(t)$. Thus

$$\begin{aligned} W(\mathcal{E}(y/x)) &= -\prod_{\mathfrak{p}|\mathfrak{d}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \prod_{\substack{v \\ e_{v,D}>0}} \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y) \\ \mathcal{E}(y/x) \text{ has bad. red. at } \mathfrak{p}}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \\ &= -\prod_{\mathfrak{p}|\mathfrak{d}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \prod_{\substack{v \\ e_{v,D}>0}} \prod_{\substack{\mathfrak{p}\nmid\mathfrak{d} \\ \mathfrak{p}|P_v(x,y)}} W_{\mathfrak{p}}(\mathcal{E}(y/x)). \end{aligned}$$

By Lemma 2.5.3,

$$\prod_{\substack{v \\ e_{v,D}>0}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \prod_{\substack{v \text{ half-bad} \\ e_{v,D}>0}} g_v(x,y) V_{\mathfrak{d},v}(\mathcal{E})(x,y)$$

$$\cdot \prod_{\substack{v \text{ quite bad} \\ e_{v,\mathfrak{d}}>0}} g_v(x,y) h(\mathrm{sq}_K(P_v(x,y)),x,y) V_{\mathfrak{d},v}(\mathcal{E})(x,y)$$

$$= \prod_{\substack{v \\ e_{v,D}>0}} g_{nu}(x,y) \prod_{\substack{v \text{ quite bad} \\ e_{v,D}>0}} h(\mathrm{sq}_K(P_v(x,y)),x,y) \prod_{\substack{v \\ e_{v,D}>0}} V_{\mathfrak{d},v}(\mathcal{E})(x,y).$$

For every two distinct places v, u of $K(t)$ with $e_{v,D} > 0$, $e_{u,D} > 0$, we know that

$$\gcd(P_v(x,y), P_u(x,y)) | \mathfrak{d}^\infty,$$

and thus $\gcd(\mathrm{sq}_K(P_v(x,y)), \mathrm{sq}_K(P_v(x,y))) | \mathfrak{d}^\infty$. By properties (3) and (4) in the statement of Lemma 2.5.3,

$$\prod_{\substack{v \text{ quite bad} \\ e_{v,D}>0}} h(\mathrm{sq}_K(P_v(x,y)),x,y) = h(\mathrm{sq}_K(B'(x,y)),x,y).$$

Since $V_{\mathfrak{d},v}(\mathcal{E}) = 1$ for v with $e_{v,D} = 0$,

$$\prod_{\substack{v \\ e_{v,D}>0}} V_{\mathfrak{d},v}(\mathcal{E})(x,y) = \prod_{v} V_{\mathfrak{d},v}(\mathcal{E})(x,y) = V(\mathcal{E})(x,y).$$

Hence

$$\prod_{\substack{v \\ e_{v,D}>0}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) = \left(\prod_{\substack{v \\ e_{v,D}>0}} g_v(x,y) \right) \cdot h(B'(x,y),x,y) \cdot V(\mathcal{E}(x,y))$$

and thus

$$W(\mathcal{E}(y/x)) = \left(-\prod_{\mathfrak{p}|\mathfrak{d}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \prod_{\substack{v \\ e_{v,D}>0}} g_v(x,y) \right) \cdot h(B'(x,y),x,y) \cdot V(\mathcal{E}(x,y))$$

By Lemma 2.5.2,

$$V(\mathcal{E})(x,y) = f(x,y) \cdot \lambda_K(M_{\mathcal{E}}(x,y)),$$

where f is a pliable function. Therefore,

$$W(\mathcal{E}(y/x)) = -f(x,y) \prod_{\mathfrak{p}|\mathfrak{d}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \prod_{\substack{v \\ e_{v,D}>0}} g_v(x,y) \cdot h(B'(x,y),x,y)\lambda_K(M_{\mathcal{E}}(x,y)).$$

By Proposition 2.3.25 and Lemma 2.3.7, the map

$$(x,y) \mapsto W_{\mathfrak{p}}(\mathcal{E}(y/x))$$

is pliable. Hence the map

$$g : (x,y) \mapsto \left(-f(x,y) \cdot \prod_{\mathfrak{p}|\mathfrak{d}} W_{\mathfrak{p}}(\mathcal{E}(y/x)) \prod_{\substack{v \\ e_{v,D}>0}} g_v(x,y) \right)$$

on $\mathbb{A}_{\mathcal{E}}$ is the product of finitely many pliable maps. Therefore, g is itself pliable. We have obtained

$$W(\mathcal{E}(y/x)) = g(x,y) \cdot h(B'(x,y),x,y) \cdot \lambda_K(M_{\mathcal{E}}(x,y)),$$

where g is pliable and h depends only on $\mathfrak{a}$ and on $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$. $\square$

2.5.3 Averages and correlations

In order to give explicit estimates for the average of $W(\mathcal{E}(y/x))$, we need quantitative versions of Hypotheses $\mathfrak{B}_1$ and $\mathfrak{B}_2$.

Hypothesis $\mathfrak{B}_1(K, P, \eta(N), \epsilon(N))$. *Let $\epsilon(N) \geq 0$, $\eta(N) \leq N$. The polynomial $P \in \mathfrak{O}_K$ obeys*

$$\sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m}} \lambda_K(P(x)) \ll \frac{\epsilon(N)N}{m}$$

for every $m \leq \eta(N)$.

Hypothesis $\mathfrak{B}_2(K, P, \eta(N), \epsilon(N))$. *Let $\epsilon(N) \geq 0$, $\eta(N) \leq N$. The homogeneous polynomial $P \in \mathfrak{O}_K[x, y]$ obeys*

$$\sum_{(x,y) \in S \cap [-N,N]^2 \cap L} \lambda_K(P(x, y)) \ll \frac{\epsilon(N)N^2}{[\mathbb{Z}^2 : L]}$$

for every sector S and every lattice coset L of index $[\mathbb{Z}^2 : L] \leq \eta(N)$.

We can now prove the results stated in the introduction.

Theorem 2.5.5 ($\mathfrak{A}_1(K, B'_{\mathcal{E}}(1, t), \delta(N))$, $\mathfrak{B}_1(K, M_{\mathcal{E}}(1, t), \eta(N), \epsilon(N))$). *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Suppose $M_{\mathcal{E}}(1, t)$ is non-constant. Then, for any integers a, m, $0 < m \leq \eta(N)$,*

$$\sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m}} W(\mathcal{E}(x)) \ll \left(\frac{\epsilon(N)}{m} + \frac{\epsilon'(N)}{\sqrt{m'}} \right) N + \delta(N), \tag{2.5.8}$$

where

$$\begin{aligned} \epsilon' &= \sqrt{\max((\log \eta(N))^c/\eta(N), N^{-1/2})} \log(-\max((\log \eta(N))^c/\eta(N), N^{-1/2})), \\ m' &= \min(m, \min(N^{1/2}, \eta(N)/(\log \eta(N))^c)), \end{aligned} \tag{2.5.9}$$

and both c and the implied constant in (2.5.8) depend only on $\mathcal{E}$ and the implied constants in hypotheses $\mathfrak{A}_1$ and $\mathfrak{B}_1$.

Proof. Let $\mathbb{A}_{\mathcal{E},\mathbb{Z}} = \{t \in \mathbb{Z} : (1,t) \in \mathbb{A}_{\mathcal{E}}\}$. Let $\mathfrak{M} = 1$. By Proposition 2.5.4,

$$W(\mathcal{E}(t)) = g(1,t) \cdot h(\mathrm{sq}_K(B'_{\mathcal{E}}(1,t)), 1, t) \cdot \lambda_K(M_{\mathcal{E}}(1,t)) \tag{2.5.10}$$

for all $t \in \mathbb{A}_{\mathcal{E},\mathbb{Z}}$, where $|g(x,y)| = 1$, $|h(\mathfrak{a}, x, y)| = 1$, g is pliable and $h(\mathfrak{a}, 1, t)$ depends only on $\mathfrak{a}$ and $t \bmod \mathrm{rad}(\mathfrak{a})$. Let $g_0(t) = g(1,t)$, $h_0(\mathfrak{a}, t) = h(\mathfrak{a}, 1, t)$. By Lemma 2.3.8, g_0 is affinely pliable.

By $\mathfrak{B}_1(K, M_{\mathcal{E}}(1,t), \eta(N), \epsilon(N))$ and Lemma 2.3.34,

$$\sum_{\substack{1 \le x \le N \\ x \equiv a \bmod m}} g_0(t)\lambda_K(M_{\mathcal{E}}(1,t)) \ll \left(\frac{\epsilon(N)}{m} + \frac{(\log \eta(N))^c}{\eta(N)}\right) N$$

for any $a, m \in \mathbb{Z}$, $0 < m \le N$. Then, by $\mathfrak{A}_1(K, B'_{\mathcal{E}}(1,t), \delta(N))$ and Proposition 2.4.1,

$$\sum_{\substack{1 \le x \le N \\ x \equiv a \bmod m}} h_0(\mathfrak{a}, t) g_0(t) \lambda_K(M_{\mathcal{E}}(1,t))$$

is at most a constant times

$$\left(\frac{\epsilon(N)}{m} + \frac{\epsilon'(N)}{\sqrt{m'}}\right) N + \delta(N),$$

where ϵ' and m' are as in (2.5.9). By (2.5.10),

$$W(\mathcal{E}(t)) = g_0(t) \cdot h(\mathrm{sq}_K(B'_{\mathcal{E}}(1,t)), t) \cdot \lambda_K(M_{\mathcal{E}}(1,t))$$

for all $t \in \mathbb{A}_{\mathcal{E},\mathbb{Z}}$. Since there are only finitely many integers not in $\mathbb{A}_{\mathcal{E},\mathbb{Z}}$, the statement follows. □

Theorem 2.5.6 **($\mathfrak{A}_1(K, B'_{\mathcal{E}}(1,t), \delta(N))$, $\mathfrak{B}_1(K, M_{\mathcal{E}}(1,t)M_{\mathcal{E}}(1,t+k), \eta(N), \epsilon(N))$).**

Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let k be a non-zero integer. Suppose $M_{\mathcal{E}}(1,t)$ is not constant. Then, for any integers a, m, $0 < m \leq \eta(N)$,

$$\sum_{\substack{1\leq x\leq N\\ x\equiv a \bmod m}} W(\mathcal{E}(x))W(\mathcal{E}(x+k)) \ll \left(\frac{\epsilon(N)}{m} + \frac{\epsilon'(N)}{\sqrt{m'}}\right) N + \delta(N), \tag{2.5.11}$$

where

$$\begin{aligned} \epsilon' &= \sqrt{\max((\log\eta(N))^c/\eta(N), N^{-1/2})}\log(-\max((\log\eta(N))^c/\eta(N), N^{-1/2})),\\ m' &= \min(m, \min(N^{1/2}, \eta(N)/(\log\eta(N))^c)), \end{aligned} \tag{2.5.12}$$

and both c and the implied constant in (2.5.11) depend only on $\mathcal{E}$ and the implied constants in hypotheses $\mathfrak{A}_1$ and $\mathfrak{B}_1$.

Proof. Let $\mathbb{A}_{\mathcal{E},\mathbb{Z}} = \{t \in \mathbb{Z} : (1,t) \in \mathbb{A}_{\mathcal{E}}\}$. Let $\mathfrak{M} = \mathfrak{m}_{B'_{\mathcal{E}}(1,t)B'_{\mathcal{E}}(1,t+k)}$, where $\mathfrak{m}$ is as in Corollary 2.4.10. By Proposition 2.5.4, $W(\mathcal{E}(t))$ equals

$$\begin{aligned} &g(1,t)\, h(\mathrm{sq}_K(B'_{\mathcal{E}}(1,t)),1,t)g(1,t+k)\\ &\qquad h(\mathrm{sq}_K(B'_{\mathcal{E}}(1,t+k)),1,t+k)\lambda_K(M_{\mathcal{E}}(1,t)M_{\mathcal{E}}(1,t+k)) \end{aligned}$$

for all $t \in \mathbb{A}_{\mathcal{E},\mathbb{Z}}$, where $|g(x,y)| = 1$, $|h(\mathfrak{a},x,y)| = 1$, g is pliable and $h(\mathfrak{a},1,t)$ depends only on $\mathfrak{a}$ and $t \bmod \mathrm{rad}(\mathfrak{a})$. Let $g_0(t) = g(1,t)g(1,t+k)$,

$$h_0(t) = h(\mathrm{sq}_K(B'_{\mathcal{E}}(1,t)),1,t)h(\mathrm{sq}_K(B'_{\mathcal{E}}(1,t+k)),1,t+k), \tag{2.5.13}$$

By Lemma 2.3.8, $g(1,t)$ and $g(1,t+k)$ are affinely pliable, and hence so is $g_0(t)$. By Lemma 2.4.10, (2.5.13) depends only on

$$\mathrm{sq}_K(\mathrm{Lcm}(B'_{\mathcal{E}}(1,t), B'_{\mathcal{E}}(1,t+k))(x))/\gcd(\mathrm{sq}_K(\mathrm{Lcm}(B'_{\mathcal{E}}(1,t), B'_{\mathcal{E}}(1,t+k))(x)), \mathfrak{M}^{\infty})$$

and on $x \bmod \mathfrak{p}$ for $\mathfrak{p} | \operatorname{sq}_K(\operatorname{Lcm}(B'_{\mathcal{E}}(1,t), B'_{\mathcal{E}}(1,t+k))(x))$, $\mathfrak{p} \nmid \mathfrak{M}$.

The remainder of the proof is as for Theorem 2.5.5. Notice that, by Lemma 2.4.5, $\mathfrak{A}_1(K, B'_{\mathcal{E}}(1,t), \delta(N))$ implies $\mathfrak{A}_1(K, B'_{\mathcal{E}}(1,t+k), \delta(N))$ and thus, by Lemma 2.4.7, it implies $\mathfrak{A}_1(K, B'_{\mathcal{E}}(1,t)B'_{\mathcal{E}}(1,t+k), \delta(N))$ as well. □

Theorem 2.5.7 ($\mathfrak{A}_1(K, B'_{\mathcal{E}}(1,t), \delta(N))$). *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Let c be an integer other than zero. Suppose $M_{\mathcal{E}}(1,t)$ is not constant. If*

$$\sum_{\substack{1 \le x \le N \\ x \equiv a \bmod m}} W(\mathcal{E}(x)) \ll \frac{\epsilon(N)N}{m}$$

for any integers a, m, $0 < m \le \eta(N)$, then

$$\sum_{\substack{1 \le x \le N \\ x \equiv a \bmod m}} \lambda_K(P(x)) \ll \left(\frac{\epsilon(N)}{m} + \frac{\epsilon'(N)}{\sqrt{m'}} \right) N + \delta(N) \tag{2.5.14}$$

for any integers a, m, $0 < m \le \eta(N)$, where

$$\begin{aligned} \epsilon' &= \sqrt{\max((\log \eta(N))^c/\eta(N), N^{-1/2})} \log(-\max((\log \eta(N))^c/\eta(N), N^{-1/2})), \\ m' &= \min(m, \min(N^{1/2}, \eta(N)/(\log \eta(N))^c)), \end{aligned} \tag{2.5.15}$$

and both c and the implied constant in (2.5.14) depend only on $\mathcal{E}$ and the implied constant in hypothesis $\mathfrak{A}_1$.

Proof. Since $|g(x,y)| = |h(\mathfrak{a}, x, y)| = 1$ for any $\mathfrak{a}$, x, y, we can rewrite (2.5.10) as

$$\lambda_K(M_{\mathcal{E}}(1,t)) = g(1,t) \cdot h(\operatorname{sq}_K(B'_{\mathcal{E}}(1,t)), 1, t) W(\mathcal{E}(t)).$$

The rest is as in the proof of Theorem 2.5.5. □

Theorem 2.5.8 ($\mathfrak{A}_2(K, B'_{\mathcal{E}}, \delta(N))$, $\mathfrak{B}_2(K, M_{\mathcal{E}}, \eta(N), \epsilon(N))$). *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Suppose $M_{\mathcal{E}}$ is non-constant. Then, for every*

sector S and every lattice coset L of index $[\mathbb{Z}^2 : L] \leq \eta(N)$,

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} W(\mathcal{E}(y/x)) \ll \left(\frac{\epsilon(N)}{[\mathbb{Z}^2 : L]} + \frac{\epsilon'(N)}{\sqrt{m'}}\right) N^2 + \delta(N), \tag{2.5.16}$$

where

$$\begin{aligned} \epsilon' &= \sqrt{\max((\log\eta(N))^c/\eta(N), N^{-1/2})}\log(-\max((\log\eta(N))^c/\eta(N), N^{-1/2})), \\ m' &= \min([\mathbb{Z}^2 : L], \min(N^{1/2}, \eta(N)/(\log\eta(N))^c)), \end{aligned} \tag{2.5.17}$$

and both c and the implied constant in (2.5.16) depend only on $\mathcal{E}$ and the implied constants in hypotheses $\mathfrak{A}_2$ and $\mathfrak{B}_2$.

Proof. By Proposition 2.5.4,

$$W(\mathcal{E}(y/x)) = g(x,y)\cdot h(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)), x, y)\cdot \lambda_K(M_{\mathcal{E}}(x,y)), \tag{2.5.18}$$

for all $(x,y) \in \mathbb{A}_{\mathcal{E}}$, where $g : \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$, $h : I_K \times \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$ are such that

- g is pliable,
- $h(\mathfrak{a}, x, y)$ depends only on $\mathfrak{a}$ and on $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$.

By $\mathfrak{B}_2(K, M_{\mathcal{E}}, \eta(N), \epsilon(N))$ and Lemma 2.4.4,

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} \lambda(P_K(x,y)) \ll \max\left(\epsilon(N), \frac{\sqrt{\log[\mathbb{Z}^2 : L]}}{\eta(N)}\right)\frac{N^2}{[\mathbb{Z}^2 : L]}$$

for every lattice L of index $[\mathbb{Z}^2 : L] \leq N$. We can now apply Proposition 2.3.40 with $\epsilon_N = \max(\epsilon(N), \sqrt{\log\eta(N)}/\eta(N))$, $\eta_N = \eta(N)$, obtaining

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} g(x,y)\lambda_K(M_{\mathcal{E}}(x,y)) = \left(\frac{\epsilon(N)}{\phi([\mathbb{Z}^2 : L])} + \frac{(\log\eta_N)^c}{\eta_N}\right) N^2$$

for any sector S and any lattice L. Then, by $\mathfrak{A}_2(K, B'_{\mathcal{E}}, \delta(N))$ and Proposition 2.4.2, the absolute value of

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} h(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)), x, y)g(x,y)\lambda_K(M_{\mathcal{E}}(x,y))$$

is at most a constant times

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} W(\mathcal{E}(y/x)) \ll \left(\frac{\epsilon(N)}{[\mathbb{Z}^2 : L]} + \frac{\epsilon'(N)}{\sqrt{m'}}\right) N^2 + \delta(N),$$

where ϵ' and m' are as in (2.5.17). Since the set $\{(x,y) \in \mathbb{Z}^2 : x,\ y \text{ coprime}\} - \mathbb{A}_{\mathcal{E}}$ is finite, the statement follows by (2.5.18). □

Theorem 2.5.9 ($\mathfrak{A}_2(K, B'_{\mathcal{E}}, \delta(N))$, $\mathfrak{B}_2(K, M_{\mathcal{E}}(t_0,t_1)M_{\mathcal{E}}(k_0x, k_0y+k_1x), \eta(N), \epsilon(N))$). *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Suppose $M_{\mathcal{E}}$ is non-constant. Let $k = k_1/k_0$ be anon-zero rational number, $\gcd(k_0, k_1) = 1$. Then, for every sector S and every lattice coset L of index $[\mathbb{Z}^2 : L] \le \eta(N)$,*

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} W(\mathcal{E}(y/x))W(\mathcal{E}(y/x+k)) \ll \left(\frac{\epsilon(N)}{[\mathbb{Z}^2 : L]} + \frac{\epsilon'(N)}{\sqrt{m'}}\right) N^2 + \delta(c'N), \tag{2.5.19}$$

where

$$\epsilon' = \sqrt{\max((\log\eta(N))^c/\eta(N), N^{-1/2})}\log(-\max((\log\eta(N))^c/\eta(N), N^{-1/2})),$$
$$m' = \min([\mathbb{Z}^2 : L], \min(N^{1/2}, \eta(N)/(\log\eta(N))^c)),$$

and c, c' and the implied constant in (2.5.19) depend only on $\mathcal{E}$ and the implied constants in hypotheses $\mathfrak{A}_2$ and $\mathfrak{B}_2$.

Proof. Let $\mathbb{A}_{\mathcal{E},k} = \{(x,y) \in \mathbb{A}_{\mathcal{E}} : \left(\frac{k_0x}{\gcd(k_0x,k_0y+k_1x)}, \frac{k_0y+k_1x}{\gcd(k_0x,k_0y+k_1x)}\right) \in A_{\mathcal{E}}\}$. Since

$\frac{k_0y+k_1x}{k_0x} = \frac{y}{x} + k$, we can write $\mathbb{A}_{\mathcal{E},k}$ in full as the set of all coprime $x, y \in \mathfrak{O}_K$ such that

$$x \neq 0,\ c_4(y/x) \neq \infty,\ c_6(y/x) \neq \infty,\ \Delta(y/x) \neq 0, \infty,\ q_0(y/x) \neq 0,$$
$$c_4(y/x+k) \neq \infty, c_6(y/x+k) \neq \infty, \Delta(y/x+k) \neq 0, \infty,\ q_0(y/x+k) \neq 0.$$

Hence $\mathbb{A} - \mathbb{A}_{\mathcal{E},k}$ is a finite set.

Let $F_1(x,y) = k_0x$, $F_2(x,y) = k_0y + k_1x$. For x, y coprime, $\gcd(k_0x, k_0y + k_1x)$ must divide k_0^2. Let

$$\mathfrak{M} = k_0\mathfrak{m}_{B'_{\mathcal{E}}, B'_{\mathcal{E}}(F_1(x,y), F_2(x,y))},$$

where $\mathfrak{m}_{\cdot}$ is as in Lemma 2.4.11. Let g, h be as in Proposition 2.5.4. Then

$$W(\mathcal{E}(y/x))W(\mathcal{E}(y/x+k))$$

equals

$$g_1(x,y) \cdot h_1(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)), x, y) \cdot \lambda_K(M_{\mathcal{E}}(x,y)M_{\mathcal{E}}(F_1(x,y), F_2(x,y))),$$

for $(x,y) \in \mathbb{A}_{\mathcal{E},k}$, where

$$g_0(x,y) = g\left(\frac{F_1(x,y)}{\gcd(F_1(x,y), F_2(x,y))}, \frac{F_2(x,y)}{\gcd(F_1(x,y), F_2(x,y))}\right),$$
$$g_1(x,y) = g(x,y) \cdot \lambda_K(\gcd(F_1(x,y), F_2(x,y)))^{\deg M_{\mathcal{E}}} g_0(x,y),$$
$$h_1(x,y) = h(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)), x, y) \cdot h_0(x,y),$$

and $h_0(x,y)$ equals

$$h\left(\mathrm{sq}_K\left(B'_{\mathcal{E}}\left(\frac{F_1(x,y)}{\gcd(F_1(x,y), F_2(x,y))}, \frac{F_2(x,y)}{\gcd(F_1(x,y), F_2(x,y))}\right)\right), F_1(x,y), F_2(x,y)\right).$$

By Lemma 2.3.10,

$$(x,y) \mapsto g\left(\frac{x}{\gcd(x,y,k_0^2)}, \frac{y}{\gcd(x,y,k_0^2)}\right)$$

is a pliable function on $S' = \{(x,y) \in \mathbb{Z}^2 : (x/\gcd(x,y,k_0^2), y/\gcd(x,y,k_0^2)) \in \mathbb{A}_{\mathcal{E}}\}$. Then, by Proposition 2.3.6, g_0 is a pliable function on

$$\{(x,y) \in \mathbb{Z}^2 : x,\ y \text{ coprime}, \left(\frac{F_1(x,y)}{\gcd(F_1(x,y),F_2(x,y))}, \frac{F_2(x,y)}{\gcd(F_1(x,y),F_2(x,y))}\right) \in \mathbb{A}_{\mathcal{E}}\},$$

which is a subset of $\mathbb{A}_{\mathcal{E},k}$. Since $\gcd(F_1(x,y),F_2(x,y))|k^\infty$ for x, y coprime, the map

$$(x,y) \to \lambda_K(\gcd(F_1(x,y),F_2(x,y)))$$

on $\mathbb{A}_{\mathcal{E},k}$ is pliable. Hence $g_1(x,y) = g(x,y) \cdot \lambda_K(\gcd(F_1(x,y),F_2(x,y)))^{\deg M_{\mathcal{E}}} g_0(x,y)$ is pliable.

By Proposition 2.5.4, (2), (3) and (4), $h(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)),x,y)$ depends only on

$$\mathrm{sq}_K(B'_{\mathcal{E}}(x,y))/\gcd(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)),\mathfrak{M}^\infty)$$

and on $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}$ for $\mathfrak{p}|\,\mathrm{sq}_K(B'_{\mathcal{E}}(x,y))$, $\mathfrak{p} \nmid \mathfrak{M}$. Hence $h_0(x,y)$ depends only on

$$\mathrm{sq}_K(B'_{\mathcal{E}}(F_1(x,y),F_2(x,y)))/\gcd(\mathrm{sq}_K(B'_{\mathcal{E}}(F_1(x,y),F_2(x,y))),\mathfrak{M}^\infty) \tag{2.5.20}$$

and on

$$\frac{F_1(x,y)/\gcd(F_1(x,y),F_2(x,y)) \bmod \mathfrak{p}}{F_2(x,y)/\gcd(F_1(x,y),F_2(x,y)) \bmod \mathfrak{p}}$$

for

$$\mathfrak{p}|\,\mathrm{sq}_K(B'_{\mathcal{E}}(F_1(x,y)/\gcd(F_1(x,y),F_2(x,y)),F_2(x,y)/\gcd(F_1(x,y),F_2(x,y)))).\ \ \mathfrak{p} \nmid \mathfrak{M}.$$

Since $\gcd(F_1(x,y), F_2(x,y)) | k_0^2$ and $k_0 | \mathfrak{M}$,

$$\frac{F_1(x,y)/\gcd(F_1(x,y), F_2(x,y)) \bmod \mathfrak{p}}{F_2(x,y)/\gcd(F_1(x,y), F_2(x,y)) \bmod \mathfrak{p}} = \frac{F_1(x,y) \bmod \mathfrak{p}}{F_2(x,y) \bmod \mathfrak{p}}$$

for all x, y coprime, $\mathfrak{p} \nmid \mathfrak{M}$. In turn, since $F_2(x,y)/F_1(x,y) = y/x + k_0/k_1 = y/x + k$,

$$\frac{F_1(x,y) \bmod \mathfrak{p}}{F_2(x,y) \bmod \mathfrak{p}} = \left(\frac{y}{x} + k\right)^{-1} \bmod \mathfrak{p}$$

for all x, y coprime, $\mathfrak{p} \nmid \mathfrak{M}$. Since k is fixed, $\left(\frac{y}{x} + k\right)^{-1} \bmod \mathfrak{p}$ depends only on $\frac{y \bmod \mathfrak{p}}{x \bmod \mathfrak{p}}$. Thus

$$h\left(\mathrm{sq}_K\left(B'_{\mathcal{E}}\left(\frac{F_1(x,y)}{\gcd(F_1(x,y), F_2(x,y))}, \frac{F_2(x,y)}{\gcd(F_1(x,y), F_2(x,y))}\right)\right), F_1(x,y), F_2(x,y)\right)$$

depends only on (2.5.20) and on $\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}$ for $\mathfrak{p} | \mathrm{sq}_K(B'_{\mathcal{E}}(F_1(x,y), F_2(x,y)))$, $\mathfrak{p} \nmid \mathfrak{M}$. By Lemma 2.4.11, it follows that h_1 depends only on

$$\frac{\mathrm{sq}_K(P(x,y))}{\gcd(\mathrm{sq}_K(P(x,y)), \mathfrak{M}^\infty)}, \quad \frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}} \text{ for } \mathfrak{p} | \mathrm{sq}_K(P(x,y)),$$

where $P = \mathrm{Lcm}(B'_{\mathcal{E}}(x,y), B'_{\mathcal{E}}(F_1(x,y), F_2(x,y))))$. It remains to show the fact that $\mathfrak{A}_2(K, P, \delta(c'N))$ holds for some c' depending only on the implied constant in $\mathfrak{A}_2$. This follows immediately from $\mathfrak{A}_2(K, B'_{\mathcal{E}}, \delta(N))$ and Lemmas 2.4.6 and 2.4.8. □

Theorem 2.5.10 ($\mathfrak{A}_2(K, B'_{\mathcal{E}}, \delta(N))$). *Let K be a number field. Let $\mathcal{E}$ be an elliptic curve over $K(t)$. Suppose $M_{\mathcal{E}}$ is non-constant. If for every sector S and every lattice coset L of index $[\mathbb{Z}^2 : L] \leq \eta(N)$,*

$$\sum_{(x,y) \in S \cap [-N,N]^2 \cap L} W(\mathcal{E}(y/x)) \ll \frac{\epsilon(N) N^2}{[\mathbb{Z}^2 : L]}$$

then, for every sector S and every lattice coset L of index $[\mathbb{Z}^2 : L] \leq \eta(N)$,

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1}} \lambda_K(P(x,y)) \ll \left(\frac{\epsilon(N)}{[\mathbb{Z}^2 : L]} + \frac{\epsilon'(N)}{\sqrt{m'}}\right) N^2 + \delta(N), \tag{2.5.21}$$

where

$$\epsilon' = \sqrt{\max((\log\eta(N))^c/\eta(N), N^{-1/2})}\log(-\max((\log\eta(N))^c/\eta(N), N^{-1/2})),$$
$$m' = \min([\mathbb{Z}^2 : L], \min(N^{1/2}, \eta(N)/(\log\eta(N))^c)),$$

and both c and the implied constant in (2.5.21) depend only on $\mathcal{E}$ and the implied constants in hypotheses $\mathfrak{A}_2$ and $\mathfrak{B}_2$.

Proof. By Proposition 2.5.4,

$$\lambda_K(M_{\mathcal{E}}(x,y)) = g(x,y)\cdot h(\mathrm{sq}_K(B'_{\mathcal{E}}(x,y)), x, y)\cdot W(\mathcal{E}(y/x)),$$

for all $(x,y) \in \mathbb{A}_{\mathcal{E}}$, where $g : \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$, $h : I_K \times \mathbb{A}_{\mathcal{E}} \to \{-1,1\}$ are such that

- g is pliable,
- $h(\mathfrak{a}, x, y)$ depends only on $\mathfrak{a}$ and on $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$.

Proceed as in the proof of Theorem 2.5.8. □

Theorems 1.1', 1.3' and 1.4' follow immediately from Theorems 2.5.5, 2.5.8 and 2.5.9, respectively, and from the known cases of $\mathfrak{A}_i$ and $\mathfrak{B}_i$ listed in Appendix A.1. In order to obtain Theorems 1.1–1.4 and Propositions 1.7.9, 1.7.10 from Theorems 2.5.5–2.5.10, it is enough to show that Conjecture $\mathfrak{A}_i(K,P)$ and Hypothesis $\mathfrak{B}_i(K,P)$, as stated in subsection 1.8, imply $\mathfrak{A}_i(K,P,\delta(N))$ and $\mathfrak{B}_i(K,P,\eta(N),\epsilon(N))$, respectively, for some $\delta(N)$, $\eta(N)$, $\epsilon(N)$ satisfying $\delta(N) = o(N)$, $\lim_{N\to\infty}\eta(N) = N$, $\epsilon(N) = o(N)$.

The case of $\mathfrak{A}_i$ is clear: since $\mathfrak{A}_1(K,P)$ states that

$$\lim_{N\to\infty}\frac{1}{N}\#\{1\le x\le N : \exists\mathfrak{p}\,\text{s.t.}\,\rho(\mathfrak{p})>N^{1/2},\mathfrak{p}^2|P(x)\}=0,$$

we can take

$$\delta(N)=\#\{1\le x\le N : \exists\mathfrak{p}\,\text{s.t.}\,\rho(\mathfrak{p})>N^{1/2},\mathfrak{p}^2|P(x)\}$$

and thus obtain $\mathfrak{A}_1(K,P,\delta(N))$; the same works for $\mathfrak{A}_2$. Now assume that $\mathfrak{B}_1(K,P)$ holds, i.e.,

$$\lim_{N\to\infty}\frac{1}{N}\sum_{\substack{1\le n\le N\\ n\equiv a \bmod m}}\lambda_K(P(n))=0$$

for any $a\ge 0$, $m>0$. For every $n\ge 1$, let $A(n)$ be the smallest positive integer such that, for every $1\le m\le n$, $0\le a<n$,

$$\frac{1}{N}\sum_{\substack{1\le n\le N\\ n\equiv a \bmod m}}\lambda_K(P(n))<\frac{1}{m\cdot n}$$

for all $N\ge A(n)$. Set $A(0)=0$. For $x\ge 1$, let $B(x)$ be the largest non-negative integer n such that $A(n)\le x$. For every $n>1$, $B(x)>n$ for all $x\ge A(n)$. Hence $\lim_{x\to\infty}B(x)=\infty$. Set $\eta(N)=B(N)$, $\epsilon(N)=\frac{1}{B(N)}$. Then $\mathfrak{B}_1(K,P,\eta(N),\epsilon(N))$ holds. The same argument is valid for $\mathfrak{B}_2$.

2.6 Examples

2.6.1 Specimens and how to find them

Let K be a number field. For any $j\in K(t)$ other than $j=0$, $j=1728$, the curve given by the equation

$$y^2=x^3-\frac{c_4}{48}x-\frac{c_6}{864},$$

$$c_4 := j(j-1728), \quad c_6 := j(j-1728)^2$$

is an elliptic curve over $K(t)$ with j-invariant equal to j. Any two elliptic curves $\mathcal{E}$, $\mathcal{E}'$ over $K(t)$ with the same j-invariant $j(\mathcal{E}) = j(\mathcal{E}') \neq 0, 1728$ must be quadratic twists of each other. Therefore, every elliptic curve $\mathcal{E}$ over $K(t)$ with j-invariant $j \neq 0, 1728$ is given by

$$c_4 = d^2 j(j-1728), \quad c_6 = d^3 j(j-1728)^2 \tag{2.6.1}$$

for some $d \in (K(t))^*$. Write $t = y/x$. Then the places of potentially multiplicative reduction of $\mathcal{E}$ are given by the factors in the denominator of $j(y/x)$, where $j(y/x)$ is written as a fraction whose numerator and denominator have no common factors. The set of places of multiplicative reduction of $\mathcal{E}$ is, of course, a subset of the set of places of potentially multiplicative reduction. We can choose which subset it is by adjusting d accordingly.

Thus we can easily find infinitely many elliptic curves $\mathcal{E}$ over $K(t)$ having $M_{\mathcal{E}}(x, y)$ equal to a given square-free homogeneous polynomial. (See (1.2.1) for the definition of $M_{\mathcal{E}}(x, y)$.) Say, for example, that you wish $M_{\mathcal{E}}(x, y)$ to be y. The set of potentially multiplicative places will have to include the place of $K(t)$ given by y. For simplicity's sake, let us require the set to have that place as its only element. Then j will have to be a non-constant polynomial on t^{-1}. In order for y to give a place of multiplicative reduction over $K(t)$, and not one of merely potential multiplicative reduction, $v_t(d)$ must be even if the degree of j as a polynomial on t^{-1} is even, and odd if the degree of j is odd. These conditions on d and j are sufficient. Thus, e.g., the families given

by

$$
\begin{aligned}
&j = t^{-1},\ d = t,\\
&c_4 = t^2 \cdot t^{-1}(t^{-1} - 1728) = 1 - 1728t,\ c_6 = t^3 \cdot t^{-1}(t^{-1} - 1728)^2 = (1 - 1728t)^2,\\
&j = t^{-2},\ d = 1,\\
&c_4 = t^{-2}(t^{-2} - 1728),\ c_6 = t^{-2}(t^{-2} - 1728)^2,\\
&j = t^{-4} - 3,\ d = (t+1),\\
&c_4 = (t+1)^2(t^{-4} - 3)(t^{-4} - 1731),\ c_6 = (t+1)^3(t^{-4} - 3)(t^{-4} - 1731)^2,
\end{aligned}
\tag{2.6.2}
$$

all have $M_{\mathcal{E}}(x, y) = y$. Note that $\deg_{\text{irr}} B'_{\mathcal{E}}(x, y) \leq 3$ for all three families in (2.6.2). Hence Theorems 1.1', 1.3' and 1.4' can be applied: for any of the families in (2.6.2), $W(\mathcal{E}(t))$ averages to zero over the integers and over the rationals; furthermore, $W(\mathcal{E}(t))$ is white noise over the rationals.

In detail, the general procedure for finding all curves $\mathcal{E}$ with $M_{\mathcal{E}}(x, y) = P(x, y)$, P square-free, is as follows. Let $P = P_1 \cdots P_2 \cdots P_n$, P_i irreducible, $P_i \neq P_j$. Suppose $P_i \neq x$ for all i. Let $Q_i(t)$ be the polynomial on t such that $P_i(y/x) = Q_i(y/x) \cdot x^{\deg Q_i}$. Choose any positive integers $k_1, \cdots, k_n$ and four polynomials $R_1(t)$, $R_2(t)$, $R_3(t)$, $R_4(t)$ coprime to $Q_1(t), \cdots, Q_n(t)$; assume that R_1 is square-free, that R_1, R_2, R_3 are pairwise coprime, that R_4 is prime to R_1 and R_2, and that $\deg R_3 \leq \sum_i k_i \deg Q_i$. Let R_5 be the product of the irreducible factors of R_2. Then

$$
j = \frac{R_3(t)}{R_1(t) R_2(t)^2 \prod_i Q_i(t)^{k_i}},\quad d = R_4(t) R_5(t) \prod_i Q_i(t)^{k_i} \tag{2.6.3}
$$

give us an elliptic curve with $\mathcal{E}$ with $M_{\mathcal{E}}(x, y) = P(x, y)$; furthermore, any such curve can be expressed as in (2.6.3). If $P = x \cdot P_1 \cdot P_2 \cdots P_n$, proceed as above, but require $\deg R > \sum_i k_i \deg Q_i$.

The degree $\deg_{\text{irr}} B'_{\mathcal{E}}(x, y)$ of the largest irr. factor of the polynomial $B'_{\mathcal{E}}(x, y)$

coming from (2.6.3) is equal to the largest of

$$\deg_{\mathrm{irr}} P, \deg_{\mathrm{irr}} R_1, \deg_{\mathrm{irr}} R_2, \deg_{\mathrm{irr}} R_3, \deg_{\mathrm{irr}}(R_3 - 1728 \cdot R_1 R_2^2 \prod_i Q_i^{k_i}) \tag{2.6.4}$$

or to 1, should all the expressions in (2.6.3) be zero. The degree $\deg_{\mathrm{irr}} B'_{\mathcal{E}}(1,t)$ is equal to (2.6.4). Since we need only know the degrees of $M_{\mathcal{E}}$ and $B_{\mathcal{E}}$ to know whether our results hold conditionally or unconditionally, we see that we have an explicit description of all families for which our results hold unconditionally. It only remains to see a few more examples that may not be quite trivial to find.

Take, for instance, the issue of semisimplicity. Constructing families with

$$\deg(M_{\mathcal{E}}(x,y)) \leq 3$$

and c_4, c_6 coprime is a cumbersome but feasible matter. The following are a few characteristic specimina:

$$\begin{array}{lll}
c_4 = 1 + \frac{8}{3}t + t^2, & c_6 = 1 + \frac{25}{6}t + 4t^2 + t^3, & M_{\mathcal{E}} = (12x+5y)(3x+8y)y, \\
c_4 = 2 + 4t + t^2, & c_6 = 1 + 9t + 6t^2 + t^3, & M_{\mathcal{E}} = (7x+2y)(x^2+4xy+y^2), \\
c_4 = 2 - 4t + t^2, & c_6 = 3 + 9t - 6t^2 + t^3, & M_{\mathcal{E}} = x^3 + 102x^2y - 63xy^2 + 10y^3, \\
c_4 = 4, & c_6 = 11 + t, & M_{\mathcal{E}} = x(3x+y)(19x+y), \\
c_4 = 3, & c_6 = 2 + 7t, & M_{\mathcal{E}} = x(-23x^2 + 28xy + 49y^2), \\
c_4 = 1 + t, & c_6 = -1 + 3t, & M_{\mathcal{E}} = xy(-3x+y), \\
c_4 = -2 + 6t + t^2, & c_6 = -\frac{45}{2} + \frac{21}{2}t + 9t^2 + t^3, & M_{\mathcal{E}} = -\frac{2057}{4}x^3 + \frac{1089}{2}x^2y + \frac{363}{4}xy^2, \\
c_4 = (t+1)(t+3), & c_6 = (13x^2 + 12xy + 3y^2), & M_{\mathcal{E}} = x(13x^2 + 12xy + 3y^2).
\end{array}$$

Note that none of these families is strictly speaking semistable, since they all have additive reduction at the place $\mathrm{den} - \mathrm{num}$ corresponding to x.

Thanks to (2.6.3), it is a simple matter to construct a family $\mathcal{E}$ such that $M_{\mathcal{E}}(x,y)$ equals the homogeneous polynomial of degree three for which the parity problem was

first treated [H-B]:

$$c_4 = 1 - 1728(t^3+1),\ c_6 = (1-1728(t^3+1))^2,\ M_{\mathcal{E}}(x,y) = x^3 + 2y^3.$$

We may conclude by seeing two families $\mathcal{E}$ over $K(t)$, K a number field other than $\mathbb{Q}$, for which our results are unconditional. (See Appendix A.2.)

$$K = \mathbb{Q}(\sqrt{5}),\ c_4 = (1-1728(t+\sqrt{5})),\ c_6 = (1-1728(t+\sqrt{5}))^2,\ M_{\mathcal{E}} = \sqrt{5}x + y,$$

$$K = \mathbb{Q}(2^{1/3}, \omega),\ c_4 = t^2(t^2 - 1728(t+\omega)),\ \ c_6 = t^2(t^2 - 1728(t+\omega))^2,\ M_{\mathcal{E}} = x(\omega x + y),$$

where ω is a third root of unity.

2.6.2 Pathologies

There are three kinds of families to which our results do not apply: (a) constant families, (b) non-constant families with $M_{\mathcal{E}} = 1$, and (c) families over $K(t)$, $K \neq \mathbb{Q}$, such that $\mathfrak{B}_i(K, M_{\mathcal{E}})$ fails to hold. The first kind is well understood; if K is Galois, the third kind behaves essentially like the second kind. (See Appendix A.2.) Consider, then, $\mathcal{E}$ over $\mathbb{Q}(t)$ with $M_{\mathcal{E}} = 1$. Choosing $\mathfrak{M}$ large enough in Proposition 2.5.4, applying Lemmas 2.3.12 and 2.3.13 and assuming $\mathfrak{A}_i(\mathbb{Q}, B'_{\mathcal{E}})$, we can see that there are intersections $S \cap L$ and arithmetic progressions $a + m\mathbb{Z}$ over which $W(\mathcal{E}(t))$ in fact does not average to 0. We may still have $\mathrm{av}_{\mathbb{Z}}\, W(\mathcal{E}(t)) = 0$ or $\mathrm{av}_{\mathbb{Q},\mathbb{Z}^2}\, W(\mathcal{E}(t)) = 0$ by cancellation of some sort. The following is an example where such cancellation does not occur.

Let

$$f(t) = \frac{t^5 - 1}{t - 1},\ g(t) = \frac{6(t^7 - 1)}{t - 1}.$$

Define $\mathcal{E}$ to be the elliptic curve over $\mathbb{Q}(t)$ given by the equation

$$y^2 = x^3 - 3f(f^3 - g^2)^2 x - 2g(f^3 - g^2)^3.$$

Bounding $\operatorname{av}_{\mathbb{Q}} \mathcal{E}(t)$ from below by a positive number is simply a matter of consulting Halberstadt's tables [Ha]. A short computer program yields that

$$\frac{1}{25^2} \sum_{\substack{x=1 \\ \gcd(x,y)=1}}^{100} \sum_{y=1}^{100} W(\mathcal{E}(y/x)) = 0.395,$$

$$\frac{1}{25^2} \sum_{\substack{x=1 \\ \gcd(x,y)=1}}^{100} \sum_{y=1}^{100} W(\mathcal{E}(-y/x)) = 0.35,$$

$$\frac{1}{100^2} \sum_{\substack{x=1 \\ \gcd(x,y)=1}}^{100} \sum_{y=1}^{100} W(\mathcal{E}(y/x)) = 0.351.$$

Finally, there is the curious matter of families $\mathcal{E}$ with $M_{\mathcal{E}}(x, y) = x$: the average of $W(\mathcal{E}(t))$ over the rationals is zero, but $M_{\mathcal{E}}(1, t) = 1$, and thus Theorem 1.1 does not apply. This is indeed the case for any $\mathcal{E}$ with j a polynomial, $v_t(d) \not\equiv \deg(j) \bmod 2$, c_4 and c_6 given by j and d as in (2.6.1). If j is a polynomial and $v_t(d) \equiv \deg(j) \bmod 2$, then $M_{\mathcal{E}}(x, y) = 1$. Thus, for any family $\mathcal{E}$ with polynomial j, there is an arithmetic progression $a + m\mathbb{Z}$ such that $\operatorname{av}_{a+m\mathbb{Z}} W(\mathcal{E}(t))$ is non-zero.

Chapter 3

The parity problem

3.1 Outline

Let $f \in \mathbb{Z}[x, y]$ be a non-constant homogeneous polynomial of degree at most 3. Let α be the Liouville function ($\alpha = \lambda$) or the Moebius function ($\alpha = \mu$). We show that $\alpha(f(x, y))$ averages to zero. (If $\alpha = \lambda$, we assume, of course, that f is not of the form $C \cdot g^2$, $C \in \mathbb{Z}$, $g \in \mathbb{Z}[x, y]$.)

The case $\deg f = 1$ is well-known. Our solution for the case $\deg f = 2$ can hardly be said to be novel, as the main ideas go back to de la Vallée-Poussin ([DVP1], [DVP2]) and Hecke ([Hec]). Nevertheless, there seems to be no treatment in the literature displaying both full generality and a strong bound in accordance with the current state of knowledge on zero-free regions. We will treat a completely general quadratic form, without assuming that the form is positive-definite or that its discriminant is a field discriminant. Our bounds will reflect the broadest known zero-free regions of Hecke L-functions. We will allow the variables to be confined to given lattice cosets or to sectors in the plane.

The case $\deg f = 3$ appeared to be completely out of reach until rather recently. We will succeed in breaking parity by an array of methods; in so far as there is an

overall common method, it may be said to consist in the varied usage of traditional sieve-methods in non-traditional ways. The strategy used for reducible polynomials is clearly different from that for irreducible polynomials. (The latter case has a parallel in the problem of capturing primes.) Nevertheless, there may be some deep similarities that have come only indirectly and partially to the fore. Note how there seems to be a uniform barrier for the error bound at $1/(\log N)$. Bilinear conditions lurk everywhere.

3.2 Preliminaries

3.2.1 The Liouville function

The Liouville function $\lambda(n)$ is defined on the set of non-zero rational integers as follows:

$$\lambda(n) = \prod_{p|n} (-1)^{v_p(n)}. \tag{3.2.1}$$

The following identities are elementary:

$$\lambda(n) = \mu(n) \quad \text{for } n \text{ square-free},$$

$$\sum_{d|n} |\mu(d)|\lambda(n/d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1, \end{cases}$$

$$\sum_{n} \lambda(n) n^{-s} = \prod_{p} \frac{1}{1 + p^{-s}} = \frac{\zeta(2s)}{\zeta(s)}.$$

We will find it convenient to choose a value for $\lambda(0)$; we adopt the convention that $\lambda(0) = 0$. We can easily extend the domain of λ further. We define λ on $\mathbb{Q}$ by

$$\lambda\left(\frac{n_0}{n_1}\right) = \frac{\lambda(n_0)}{\lambda(n_1)} \tag{3.2.2}$$

and on ideals in a Galois extension $K/\mathbb{Q}$ of degree n by

$$\lambda(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_k^{e_k}) = \prod_i \omega^{f(\mathfrak{p}_i)\cdot e_i}, \tag{3.2.3}$$

where ω is a fixed $(2n)$th root of unity and $f(\mathfrak{p}_i)$ is the degree of inertia of $\mathfrak{p}_i$ over $\mathfrak{p}_i \cap \mathbb{Q}$. Notice that (3.2.3) restricts to (3.2.2), which, in turn, restricts to (3.2.1). Notice also that the above *extension* is different from the natural *generalization* λ_K:

$$\lambda_K(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_k^{e_k}) = \prod_i (-1)^{e_i}. \tag{3.2.4}$$

We define, as usual,

$$\mu_K(\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_k^{e_k}) = \begin{cases} \prod_i (-1)^{e_i} & \text{if } e_i \leq 1 \text{ for all } i = 1, 2, \cdots, k \\ 0 & \text{otherwise.} \end{cases} \tag{3.2.5}$$

3.2.2 Ideal numbers and Grössencharakters

Let K be a number field. Write $\mathfrak{O}_K$ for its ring of integers. Let I_K be the semigroup of non-zero ideals of $\mathfrak{O}_K$; let J_K be the group of non-zero fractional ideals of $\mathfrak{O}_K$. For every $\mathfrak{d} \in I_K$, define $\mathfrak{O}_{K,\mathfrak{d}}$ to be the set of elements of $\mathfrak{O}_K$ prime to $\mathfrak{d}$. Define $I_{K,\mathfrak{d}}$ to be the semigroup of ideals of $\mathfrak{O}_K$ prime to $\mathfrak{d}$.

Since the class group of $\mathfrak{O}_K$ is finite, there are ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_{i_0} \in I_K$ and positive integers $h_1, h_2, \cdots, h_{i_0}$ such that every $\mathfrak{d} \in \mathfrak{O}_K$ can be expressed in a unique way in the form

$$\mathfrak{d} = \mathfrak{d}_p \mathfrak{a}_1^{d_1}\mathfrak{a}_2^{d_2}\cdots\mathfrak{a}_{i_0}^{d_{i_0}}, \quad \mathfrak{d}_p \text{ principal}, 0 \leq d_i < h_i. \tag{3.2.6}$$

Fix $\alpha_1, \ldots, \alpha_{i_0} \in \mathfrak{O}_K$ such that $(\alpha_i) = \mathfrak{a}_i^{h_i}$. Choose $\beta_1, \ldots, \beta_{i_0}$ in the algebraic completion of K such that $\beta_i^{h_i} = \alpha_i$ for every $i = 1, \cdots, i_0$. Define $L = K(\beta_1, \ldots, \beta_{i_0})$.

Let $\mathcal{I}(K)^\times$ be the subgroup of L^* generated by K^* and $\beta_1, \cdots, \beta_{i_0}$. We say that $\mathcal{I}(K) = \mathcal{I}(K)^\times \cap \{0\}$ is the set of *ideal numbers*. For $a = \alpha\beta_1^{d_1} \cdots \beta_{i_0}^{d_{i_0}} \in \mathcal{I}(K)^\times$, $\alpha \in K$, let $\mathfrak{I}(a) = (\alpha)\mathfrak{a}_1^{d_1} \cdots \mathfrak{a}_{i_0}^{d_{i_0}}$. Then $\mathfrak{I} : \mathcal{I}(K)^\times \to J_K$ is a surjective homomorphism with kernel $\mathfrak{O}_K^*$. We define $\mathcal{I}(\mathfrak{O}_K)^\times$ to be the preimage $\mathfrak{I}^{-1}(I_K)$.

For $a, b \in \mathcal{I}(\mathfrak{O}_K)^\times$, we say that $a|b$ (*a divides b*) if $b = ac$ for some $c \in \mathcal{I}(\mathfrak{O}_K)^\times$; we say that $\gcd(a, b) = 1$ (*a is prime to b*) if there is no non-unit $c \in \mathcal{I}(\mathfrak{O}_K)^\times$ such that $c|a$, $c|b$.

Let $\mathfrak{d} \in I_K$. Let $\hat{\mathfrak{d}}$ be an arbitrary element of $\mathfrak{I}^{-1}(\mathfrak{d})$. Define $\mathcal{I}(\mathfrak{O}_K)_\mathfrak{d}$ to be the semigroup of all $a \in \mathcal{I}(\mathfrak{O}_K)^\times$ prime to $\hat{\mathfrak{d}}$. For $a, b \in \mathcal{I}(\mathfrak{O}_K)_\mathfrak{d}$, $a = \alpha\beta_1^{a_1} \cdots \beta_{i_0}^{a_{i_0}}$, $b = \beta\beta_1^{b_1} \cdots \beta_{i_0}^{b_{i_0}}$, we say that $a \sim b$ if $a_i = b_i$ for every $i = 1, \ldots, i_0$ and $\hat{\mathfrak{d}}|(\alpha - \beta)\beta_1^{a_1} \cdots \beta_{i_0}^{a_{i_0}}$. Define $\mathcal{C}_\mathfrak{d}(K)$ to be the set of equivalence classes of $\mathcal{I}(\mathfrak{O}_K)_\mathfrak{d}$ under $\sim$.

For every embedding of K into $\mathbb{C}$, choose an embedding of L extending it; since $\mathcal{I}(K) \subset L$, we obtain an embedding of $\mathcal{I}(K)$ into $\mathbb{C}$. Let $\iota_1, \ldots, \iota_{\deg_K}$ be the embeddings of $\mathcal{I}(K)$ thus obtained; order them so that $\iota_1, \ldots, \iota_{r_1}$ come from the real embeddings of K and $\iota_{r_1+1}, \ldots, \iota_{r_1+2r_2}$ come from the complex embeddings of K. We can assume $\iota_{r_1+r_2+1} = \overline{\iota_{r_1+1}}, \ldots, \iota_{r_1+2r_2} = \overline{\iota_{r_1+r_2}}$.

For $a, b \in \mathcal{I}(\mathfrak{O}_K)_\mathfrak{d}$, we say that $a \sim_n b$ if $a \sim b$ and $\operatorname{sgn} \iota_i(a) = \operatorname{sgn} \iota_i(b)$ for every $i = 1, \ldots, \deg_K$. Define $\mathcal{C}_\mathfrak{d}^n(K)$ to be the set of equivalence classes of $\mathcal{I}(\mathfrak{O}_K)_\mathfrak{d}$ under $\sim_n$.

We denote the set of all characters χ of a finite group G by $\Xi(G)$. Let $\chi \in \Xi(\mathcal{C}_\mathfrak{d}^n(K))$. For $s_1, \ldots, s_{r_1+r_2} \in \mathbb{R}$, $n_1, \ldots, n_{r_2} \in \mathbb{Z}$, define $\gamma_{s,n} : \mathcal{I}(\mathfrak{O}_K)^\times \to S^1$ as follows:

$$\gamma_{s,n}(a) = \prod_{j=1}^{r_1+r_2} |\iota_j(a)|^{is_j} \prod_{j=1}^{r_2} \left(\frac{\iota_{r_1+j}(a)}{|\iota_{r_1+j}(a)|} \right)^{n_j}. \tag{3.2.7}$$

Assume $\gamma_{s,n}(u)\chi(u) = 1$ for every unit $u \in \mathfrak{O}_K^* \subset \mathcal{I}(\mathfrak{O}_K)^\times$. Then we can define the *Grössencharakter* $\psi_{\chi,s,n} : I_{K,\mathfrak{d}} \to S^1$ by $\psi(\mathfrak{a}) = \chi(a)\gamma_{s,n}(a)$, where a is any element of $\mathfrak{I}^{-1}(\mathfrak{a})$.

Consider now $K/\mathbb{Q}$ quadratic. We can describe the Grössencharakters of K as

follows. Let $K/\mathbb{Q}$ be imaginary. Write ι for the embedding ι_1 of $\mathcal{I}(\mathfrak{O}_K)$ in $\mathbb{C}$. Let $\chi \in \Xi(\mathcal{C}_{\mathfrak{d}}(K))$. If n is an integer such that $\chi(u)(\iota(u))^n = 1$ for every $u \in \mathfrak{O}_K^*$, then there is a Grössencharakter

$$\psi_n(\mathfrak{a}) = \chi(a)\left(\frac{\iota(s)}{|\iota(s)|}\right)^n. \tag{3.2.8}$$

Let $K/\mathbb{Q}$ now be real. In the definition of $\mathcal{I}(K)^\times$, we can choose $\alpha_1, \ldots, \alpha_{i_0}$ positive and $\beta_1, \ldots, \beta_{i_0}$ real. Thus we can assume that $\iota_1(a), \iota_2(a) \in \mathbb{R}$ for all $a \in \mathcal{I}(K)$. Let u_1 be the primitive unit of $\mathfrak{O}_K$ such that $\iota_1(u_1) > 1$. For every $\mathfrak{d} \in I_K$, let $k_{\mathfrak{d}}$ be the smallest positive integer such that $u_1^{k_{\mathfrak{d}}} \equiv 1 \bmod \mathfrak{d}$. Let

$$r_{\mathfrak{d}} = \begin{cases} 1 & \text{if } \frac{\iota_1(u_1)}{\iota_2(u_1)} > 0, \\ 2 & \text{if } \frac{\iota_1(u_1)}{\iota_2(u_1)} < 0. \end{cases}$$

Let $l_{\mathfrak{d}}$ be the positive real number $\left(\frac{\iota_1(u_1)}{\iota_2(u_1)}\right)^{r_{\mathfrak{d}} k_{\mathfrak{d}}}$. Let $\chi \in \Xi(\mathcal{C}_{\mathfrak{d}}(K))$. If $n \in \mathbb{Z}$, $n_0 \in \{0, 1\}$ are such that

$$\chi(u_1)\left(\operatorname{sgn}\left(\frac{\iota_1(u_1)}{\iota_2(u_1)}\right)\right)^{n_0}\left|\frac{\iota_1(u_1)}{\iota_2(u_1)}\right|^{2\pi i n/\log l_{\mathfrak{d}}} = 1,$$

then there is a Grössencharakter

$$\psi_n(\mathfrak{a}) = \chi(a)\left(\operatorname{sgn}\left(\frac{\iota_1(a)}{\iota_2(a)}\right)\right)^{n_0}\left|\frac{\iota_1(a)}{\iota_2(a)}\right|^{2\pi i n/\log l_{\mathfrak{d}}}. \tag{3.2.9}$$

We define the *size* $\mathcal{S}(\psi)$ of a Grössencharakter ψ to be

$$\sqrt{\sum_{j=1}^{r_1+r_2} s_j^2 + \sum_{j=r_1+r_2+1}^{r_1+2r_2} n_j^2}, \tag{3.2.10}$$

where s_j and n_j are as in (3.2.7). For $K/\mathbb{Q}$ quadratic and imaginary,

$$\mathcal{S}(\psi) = n,$$

where n is as in (3.2.8). For $K/\mathbb{Q}$ quadratic and real,

$$\mathcal{S}(\psi) = 2^{3/2}\pi n/\log l_{\mathfrak{d}},$$

where n is as in (3.2.9). Thus, if we take $K/\mathbb{Q}$ to be fixed,

$$\mathcal{S}(\psi) \ll N\mathfrak{d} \cdot n.$$

3.2.3 Quadratic forms

We will consider only quadratic forms $ax^2+bxy+cy^2$ with integer coefficients $a, b, c \in \mathbb{Z}$. A quadratic form $ax^2 + bxy + cy^2$ is *primitive* if $\gcd(a, b, c) = 1$.

Let n be a rational integer. We denote by $\mathrm{sq}(n)$ the largest positive integer whose square divides n. Define

$$d_n = \begin{cases} \mathrm{sq}(n) & \text{if } 4 \nmid n \\ \mathrm{sq}(n)/2 & \text{if } 4|n. \end{cases}$$

Lemma 3.2.1. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be a primitive, irreducible quadratic form. Let $K = \mathbb{Q}(\sqrt{b^2 - 4ac})$. Then there are algebraic integers $\alpha_1, \alpha_2 \in \mathfrak{O}_K$ linearly independent over $\mathbb{Q}$ such that*

$$Q(x, y) = \frac{N(x\alpha_1 + y\alpha_2)}{a}$$

for all $x, y \in \mathbb{Z}$. The subgroup $\mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2$ of $\mathfrak{O}_K$ has index $[\mathfrak{O}_K : \mathbb{Z}\alpha_1+\mathbb{Z}\alpha_2] = d_{b^2-4ac}$.

Proof. Set $\alpha_1 = a$, $\alpha_2 = \frac{b+\sqrt{b^2-4ac}}{2}$. □

3.2.4 Truth and convention

Following Iverson and Knuth [Kn], we define [true] to be 1 and [false] to be zero. Thus, for example, $x \to [x \in S]$ is the characteristic function of a set S.

3.2.5 Approximation of intervals

We denote by S^1 the unit circle in $\mathbb{R}^2$. An *interval* $I \subset S^1$ is a connected subset of S^1.

Lemma 3.2.2. *Let $I \subset S^1$ be an interval with endpoints x_0, x_1. Let $d(x,y) \in [0,\pi]$ denote the angle between two given points $x, y \in S^1$. Then, for any positive ϵ and any positive integer k, there are complex numbers $\{a_n\}_{n=-\infty}^{\infty}$ such that*

$$0 \leq \sum_{n=-\infty}^{\infty} a_n x^n \leq 1 \qquad \textit{for every } x \in S^1,$$

$$\sum_{n=-\infty}^{\infty} a_n x^n = [x \in I] \quad \textit{if } d(x,x_0), d(x,x_1) \geq \epsilon/2,$$

$$|a_n| \ll \left(\frac{k}{\epsilon}\right)^k |n|^{-(k+1)} \qquad \textit{for } n \neq 0,$$

$$|a_0| \ll 1.$$

The implied constant is absolute.

Proof. See [Vi], Ch. 1, Lemma 12. □

3.2.6 Lattices, convex sets and sectors

A *lattice* is a subgroup of $\mathbb{Z}^n$ of finite index; a *lattice coset* is a coset of such a subgroup. By the *index* of a lattice coset we mean the index of the lattice of which it is a coset. For any lattice cosets L_1, L_2 with $\gcd([\mathbb{Z}^n : L_1], [\mathbb{Z}^n : L_2]) = 1$, the

intersection $L_1 \cap L_2$ is a lattice coset with

$$[\mathbb{Z}^n : L_1 \cap L_2] = [\mathbb{Z}^n : L_1][\mathbb{Z}^n : L_2]. \tag{3.2.11}$$

In general, if L_1, L_2 are lattice cosets, then $L_1 \cap L_2$ is either the empty set or a lattice coset such that

$$\begin{aligned} \operatorname{lcm}([\mathbb{Z}^n : L_1], [\mathbb{Z}^n : L_2]) \mid [\mathbb{Z}^n : L_1 \cap L_2], \\ [\mathbb{Z}^n : L_1 \cap L_2] \mid [\mathbb{Z}^n : L_1][\mathbb{Z}^n : L_2]. \end{aligned} \tag{3.2.12}$$

For $S \subset [-N, N]^n$ a convex set and $L \subset \mathbb{Z}^n$ a lattice coset,

$$\#(S \cap L) = \frac{\operatorname{Area}(S)}{[\mathbb{Z}^n : L]} + O(N^{n-1}), \tag{3.2.13}$$

where the implied constant depends only on n.

By a *sector* we will mean a connected component of a set of the form $\mathbb{R}^n - (T_1 \cap T_2 \cap \cdots \cap T_n)$, where T_i is a hyperplane going through the origin. Every sector S is convex. Given a sector $S \subset \mathbb{R}^2$, we may speak of the *angle* $\alpha \in (0, 2\pi]$ spanned by S, or, for short, the *angle* α *of* S.

Call a sector S of $\mathbb{R}^2$ a *subquadrant* if its closure intersects the x- and y-axes only at the origin. By the *hyperbolic angle* $\theta \in (0, \infty]$ of a subquadrant $S \subset \mathbb{R}^2$ we mean

$$\sup_{(x,y)\in S} \log|x/y| - \inf_{(x,y)\in S} \log|x/y|.$$

Notice that the area of the region

$$\{(x, y) \in S : x^2 + y^2 \leq R\}$$

equals $\frac{1}{2}\alpha R$, where α is the angle of S, whereas the area of the region

$$\{(x, y) \in S : xy \leq R\}$$

equals $\frac{1}{2}\theta R$, where θ is the hyperbolic angle of S.

3.2.7 Classical bounds and their immediate consequences

By Siegel, Walfisz and Vinogradov (vd. [Wa], V §5 and V §7),

$$\left| \sum_{\substack{n \le x \\ n \equiv a \bmod m}} \lambda(n) \right| \ll x e^{-C(\log x)^{2/3}/(\log\log x)^{1/5}}, \tag{3.2.14}$$

$$\left| \sum_{\substack{n \le x \\ n \equiv a \bmod m}} \mu(n) \right| \ll x e^{-C(\log x)^{2/3}/(\log\log x)^{1/5}} \tag{3.2.15}$$

for $m \le (\log x)^A$, with C and the implied constant depending on A.

The following lemma is well-known in essence.

Lemma 3.2.3. *Let K be a finite extension of $\mathbb{Q}$. Let $\mathfrak{d}$ be an ideal of $\mathfrak{O}_K$. Let ψ be a Grössencharacter on $I_{K,\mathfrak{d}}$. Assume*

$$\mathcal{S}(\psi) \ll e^{(\log x)^{3/5}(\log\log x)^{1/5}}. \tag{3.2.16}$$

If

$$N\mathfrak{d} \ll e^{(\log x)^{2/5}(\log\log x)^{1/5}} \tag{3.2.17}$$

and ψ is not a real Dedekind character, or

$$N\mathfrak{d} \ll (\log N)^A \tag{3.2.18}$$

and ψ is a real Dedekind character, then

$$\sum_{\substack{\mathfrak{m} \in I_{K,\mathfrak{d}} \\ N\mathfrak{m} \le x}} \psi(\mathfrak{m})\mu_K(\mathfrak{m}) \ll x e^{-C\frac{(\log x)^{2/3}}{(\log\log x)^{1/5}}}, \tag{3.2.19}$$

where C and the implied constant in (3.2.19) depend only on K, A, and the implied constants in (3.2.16), (3.2.17) and (3.2.18).

Proof. Clearly

$$\sum_{\mathfrak{m}\in I_{K,\mathfrak{d}}} \mu_K(\mathfrak{m})(N\mathfrak{m})^{-s} = \prod_{\mathfrak{p}}(1-(N\mathfrak{p})^{-s}) = \frac{1}{L(\psi,s)}.$$

Given the zero-free region in [Col] and the Siegel-type bound in [Fo] for the exceptional zero, the result follows in the standard fashion (see e.g. [Dav], Ch. 20–22, or [Col], §6). □

Lemma 3.2.4. *Let K be a quadratic extension of $\mathbb{Q}$. Let $\mathfrak{d}$ be an ideal of $\mathfrak{O}_K$. Let ψ be a Grössencharacter on $I_{K,\mathfrak{d}}$. Suppose*

$$\mathcal{S}(\psi) \ll e^{(\log x)^{3/5}(\log\log x)^{1/5}}, \quad N\mathfrak{d} \ll (\log N)^A. \tag{3.2.20}$$

Then

$$\sum_{\substack{\mathfrak{m}\in I_{K,\mathfrak{d}}\\ N\mathfrak{m}\le x}} \psi(\mathfrak{m})\lambda(N\mathfrak{m}) \ll xe^{-C\frac{(\log x)^{2/3}}{(\log\log x)^{1/5}}}, \tag{3.2.21}$$

where C and the implied constant in (3.2.21) depend only on K, A and the implied constant in (3.2.20).

Proof. Define

$$\phi(\psi,s) = \sum_{\mathfrak{m}\in I_{K,\mathfrak{d}}} \psi(\mathfrak{m})\lambda(N\mathfrak{m})(N\mathfrak{m})^{-s}$$

for $\Re s > 1$. We can express ϕ as an Euler product:

$$\phi(\psi,s) = \prod_{\substack{\mathfrak{p}\in I_{K,\mathfrak{d}}\\ \mathfrak{p}\cap\mathbb{Q} \text{ splits in } K}} \frac{1}{1+\psi(\mathfrak{p})(N\mathfrak{p})^{-s}} \prod_{\substack{\mathfrak{p}\in I_{K,\mathfrak{d}}\\ \mathfrak{p}\cap\mathbb{Q} \text{ does not split in } K}} \frac{1}{1-\psi(\mathfrak{p})(N\mathfrak{p})^{-s}}.$$

Write

$$R(\psi, s) = \prod_{\substack{\mathfrak{p} \in I_{K,\mathfrak{d}} \\ \mathfrak{p} \cap \mathbb{Q} \text{ ramifies}}} \frac{1 + \psi(\mathfrak{p})(N\mathfrak{p})^{-s}}{1 - \psi(\mathfrak{p})(N\mathfrak{p})^{-s}}.$$

Then

$$\begin{aligned}
\phi(\psi, s) &= R(\psi, s) \prod_{\substack{\mathfrak{p} \in I_{K,\mathfrak{d}} \\ \mathfrak{p} \cap \mathbb{Q} \text{ unsplit \& unram.}}} \frac{1 + \psi(\mathfrak{p})(N\mathfrak{p})^{-s}}{1 - \psi(\mathfrak{p})(N\mathfrak{p})^{-s}} \prod_{\mathfrak{p} \in I_{K,\mathfrak{d}}} \frac{1}{1 + \psi(\mathfrak{p})(N\mathfrak{p})^{-s}} \\
&= R(\psi, s) \prod_{\substack{p \nmid d \\ p \text{ unsplit \& unram. in } K}} \frac{1 + \chi(p)p^{-2s}}{1 - \chi(p)p^{-2s}} \prod_{\mathfrak{p} \in I_{K,\mathfrak{d}}} \frac{1 - \psi(\mathfrak{p})(N\mathfrak{p})^{-s}}{1 - \psi^2(\mathfrak{p})(N\mathfrak{p})^{-2s}},
\end{aligned}$$

where $d = N\mathfrak{d}$ and χ is the restriction of ψ to $\mathbb{Z}^+$. We denote

$$\chi'(p) = \begin{cases} 0 & \text{if } p \text{ ramifies} \\ 1 & \text{if } p \text{ splits} \\ -1 & \text{if } p \text{ neither splits nor ramifies,} \end{cases}$$

$$L(\psi, s) = \prod_{\mathfrak{p} \in I_{K,\mathfrak{d}}} \frac{1}{1 - \psi(\mathfrak{p})(N\mathfrak{p})^{-s}}$$

and obtain

$$\phi(\chi, s) = R(\psi, s) \prod_{p \text{ ram. in } K} (1 - \chi(p)p^{-2s}) \frac{L(\chi, 2s)}{L(\chi \cdot \chi', 2s)} \frac{L(\psi^2, 2s)}{L(\psi, s)}.$$

Proceed as in Lemma 3.2.3. □

3.2.8 Bilinear bounds

We shall need bilinear bounds for the Liouville function. For section 3.4, the following lemma will suffice. It is simply a linear bound in disguise.

Lemma 3.2.5. *Let S be a convex subset of $[-N, N]^2$. Let $L \subset \mathbb{Z}^2$ be a lattice coset*

of index

$$[\mathbb{Z}^2 : L] \ll (\log N)^A. \tag{3.2.22}$$

Let $f : \mathbb{Z} \to \mathbb{C}$ *be a function with* $\max_y |f(y)| \leq 1$*. Then, for every* $\epsilon > 0$*,*

$$\left| \sum_{(x,y)\in S\cap L} \lambda(x) f(y) \right| \ll \mathrm{Area}(S) \cdot e^{-C(\log N)^{2/3}/(\log\log N)^{1/5}} + N^{1+\epsilon}, \tag{3.2.23}$$

where C *and the implied constant in (3.2.23) depend only on* K*,* ϵ*,* A *and the implied constant in (3.2.22).*

Proof. For every $y \in \mathbb{Z}\cap[-N, N]$, the set $\{x : (x, y) \in L\}$ is either the empty set or an arithmetic progression $m\mathbb{Z} + a_y$, where $m|[\mathbb{Z}^2 : L]$. Let y_0 and y_1 be the least and the greatest $y \in \mathbb{Z} \cap [-N, N]$ such that $\{x : (x, y) \in S\}$ is non-empty. Let $y \in \mathbb{Z} \cap [y_0, y_1]$. Since S is convex and a subset of $[-N, N]^2$, the set $\{x : (x, y) \in S\}$ is an interval $[N_{y,0}, N_{y,1}]$ contained in $[-N, N]$. Hence

$$\begin{aligned}
\left| \sum_{(x,y)\in S\cap L} \lambda(x) f(y) \right| &= \left| \sum_{\substack{y_0 \leq y \leq y_1 \\ \{x:(x,y)\in L\}\neq\emptyset}} \sum_{\substack{-N_{y,0} \leq x \leq N_{y,1} \\ x \equiv a_y \bmod m_y}} \lambda(x) f(y) \right| \\
&\leq \sum_{\substack{y_0 \leq y \leq y_1 \\ \{x:(x,y)\in L\}\neq\emptyset}} \left| \sum_{\substack{-N_{y,0} \leq x \leq N_{y,1} \\ x \equiv a_y \bmod m}} \lambda(x) \right|.
\end{aligned}$$

By (3.2.14),

$$\sum_{\substack{y_0\le y\le y_1\\ \{x:(x,y)\in L\}\neq\emptyset}}\left|\sum_{\substack{-N_{y,0}\le x\le N_{y,1}\\ x\equiv a_y \bmod m}}\lambda(x)\right| = \sum_{\substack{y_0\le y\le y_1\\ \{x:(x,y)\in L\}\neq\emptyset\\ N_{y,1}-N_{y,0}>N^{\epsilon}}}\left|\sum_{\substack{-N_{y,0}\le x\le N_{y,1}\\ x\equiv a_y \bmod m}}\lambda(x)\right|$$

$$+\sum_{\substack{y_0\le y\le y_1\\ \{x:(x,y)\in L\}\neq\emptyset\\ N_{y,1}-N_{y,0}\le N^{\epsilon}}}\left|\sum_{\substack{-N_{y,0}\le x\le N_{y,1}\\ x\equiv a_y \bmod m}}\lambda(x)\right|$$

$$\ll \sum_{y_0\le y\le y_1}(N_{y_1}-N_{y_0})e^{-C(\log N^{\epsilon})^{2/3}/(\log\log N)^{1/5}}+N^{1+\epsilon}.$$

Clearly

$$\mathrm{Area}(S)=\sum_{y=y_0}^{y_1}(N_{y,1}-N_{y,0})+O(N).$$

Therefore

$$\left|\sum_{(x,y)\in S\cap L}\lambda(x)f(y)\right| \ll \mathrm{Area}(S)\cdot e^{-C(\log N^{\epsilon})^{2/3}/(\log\log N)^{1/5}}+N^{1+\epsilon}.$$

□

As a special case of, say, Theorem 1 in [Le], we have the following analogue of Bombieri-Vinogradov:

$$\sum_{m\le\frac{N^{1/2}}{(\log N)^{2A+4}}}\max_{\substack{a\\(a,m)=1}}\max_{x\le N}\left|\sum_{\substack{n\le x\\ n\equiv a \bmod m}}\lambda(n)-\frac{1}{\phi(m)}\sum_{\substack{n\le x\\ \gcd(n,m)=1}}\lambda(n)\right|\ll\frac{N}{(\log N)^A},\quad (3.2.24)$$

where the implied constant depends only on A.

A simpler statement is true.

Lemma 3.2.6. *For any $A > 0$,*

$$\sum_{m \le \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_a \max_{x \le N} \left| \sum_{\substack{n \le x \\ n \equiv a \bmod m}} \lambda(n) \right| \ll \frac{N}{(\log N)^A},$$

where the implied constant depends only on A.

Proof. Write $\operatorname{rad}(m) = \prod_{p|m} p$. Then

$$\sum_{d | \gcd(\operatorname{rad}(m), n)} \lambda(n/d) = \begin{cases} \lambda(n) & \text{if } \gcd(m,n) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned}
\sum_{m \le N^{1/2}} \frac{1}{\phi(m)} \max_{x \le N} \left| \sum_{\substack{n \le x \\ \gcd(n,m)=1}} \lambda(n) \right| &= \sum_{m \le N^{1/2}} \frac{1}{\phi(m)} \max_{x \le N} \left| \sum_{d | \operatorname{rad}(m)} \sum_{\substack{n \le x \\ d | n}} \lambda(n/d) \right| \\
&\le \sum_{m \le N^{1/2}} \frac{1}{\phi(m)} \sum_{d | \operatorname{rad}(m)} \max_{x \le N/d} \left| \sum_{n \le x} \lambda(n) \right| \\
&\ll \sum_{m \le N^{1/2}} \frac{1}{\phi(m)} \sum_{d | \operatorname{rad}(m)} N/d \cdot e^{-C\sqrt{\log N/d}} \quad \text{by 3.2.14} \\
&\le N e^{-C\sqrt{\log N^{1/2}}} \sum_{m \le N^{1/2}} \frac{1}{\phi(m)} \sum_{d | \operatorname{rad}(m)} \frac{1}{d} \\
&\ll \frac{N}{(\log N)^A}.
\end{aligned}$$

By (3.2.24) this implies

$$\sum_{m \le \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_{\substack{a \\ \gcd(a,m)=1}} \max_{x \le N} \left| \sum_{\substack{n \le x \\ n \equiv a \bmod m}} \lambda(n) \right| \ll \frac{N}{(\log N)^A}.$$

Now

$$\sum_{m\le \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_a \max_{x\le N} \left| \sum_{\substack{n\le x\\ n\equiv a \bmod m}} \lambda(n)\right| = \sum_{m\le \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_{r|m} \max_{(a,m)=1} \max_{x\le N} \left| \sum_{\substack{n\le x\\ n\equiv ar \bmod m}} \lambda(n)\right|$$

$$= \sum_{m\le \frac{N^{1/2}}{(\log N)^{2A+6}}} \max_{r|m} \max_{(a,m)=1} \max_{x\le \frac{N}{r}} \left| \sum_{\substack{n\le x\\ n\equiv a \bmod m/r}} \lambda(n)\right|$$

$$< \sum_{r\le N^{1/2}} \sum_{s\le \frac{(N/r)^{1/2}}{(\log(N/r))^{2A+6}}} \max_{(a,s)=1} \max_{x\le \frac{N}{r}} \left| \sum_{\substack{n\le x\\ n\equiv a \bmod s}} \lambda(n)\right|$$

$$\ll \sum_{r\le N^{1/2}} \frac{N/r}{(\log N/r)^{A+1}} \ll \frac{N}{(\log N)^A}.$$

□

The following lemma is to Lemma 3.2.5 what Bombieri-Vinogradov is to (3.2.14).

Lemma 3.2.7. *Let A, K and N be positive integers such that $K \le N^{1/2}/(\log N)^{2A+6}$. For $j = 1, 2, \ldots, K$, let S_j be a convex subset of $[-N, N]^2$ and let $L_j \subset \mathbb{Z}^2$ be a lattice coset of index j. Let $f : \mathbb{Z} \to \mathbb{C}$ be a function with $\max_y |f(x, y)| \le 1$. Then*

$$\sum_{j=1}^{K} \left| \sum_{(x,y)\in S_j\cap L_j} \lambda(x) f(y)\right| \ll \frac{N^2}{(\log N)^A},$$

where the implicit constant depends only on A.

Proof. We start with

$$\sum_{j=1}^{K}\left|\sum_{(x,y)\in S_j\cap L_j}\lambda(x)f(y)\right| \le \sum_{j=1}^{K}\sum_{y}\left|\sum_{\substack{x\\(x,y)\in S_j\cap L_j}}\lambda(x)\right|$$
$$= \sum_{j=1}^{K}\sum_{k=0}^{\lceil N/j\rceil}\sum_{y=kj}^{(k+1)j-1}\left|\sum_{\substack{x\\(x,y)\in S_j\cap L_j}}\lambda(x)\right|.$$

For any $y \in \mathbb{Z}$, the set

$$\{x : (x,y) \in L_j\}$$

is either the empty set or an arithmetic progression of modulus $m_j|j$ independent of y. Thus the set

$$A_j = \{(x,y) \in L_j : kj \le y \le (k+1)j - 1\}$$

is the union of m_j sets of the form

$$B_{y_0,a} = \{(x,y) \in \mathbb{Z}^2 : x \equiv a \bmod m_j,\ y = y_0\}$$

with $kj \le y_0 \le (k+1)j - 1$. Since an arithmetic progression of modulus d is the union of j/d arithmetic progressions of modulus j, the set A_j is the union of j sets of the form

$$C_{x_0,a} = \{(x,y) \in \mathbb{Z}^2 : x \equiv a \bmod j,\ y = y_0\}.$$

Therefore

$$\begin{aligned}
\sum_{j=1}^{K}\sum_{k=0}^{\lceil N/j\rceil}\sum_{y=kj}^{(k+1)j-1}\left|\sum_{\substack{x\\(x,y)\in S_j\cap L_j}}\lambda(x)\right| &\le \sum_{j=1}^{K}\sum_{k=0}^{\lceil N/j\rceil}\sum_{l=1}^{j}\left|\sum_{\substack{x\\(x,y_0(k,l))\in S_j\cap C_{y_0(k,l),a(k,l)}}}\lambda(x)\right| \\
&\le \sum_{j=1}^{K}(N+j)\max_{y_0}\max_{a}\left|\sum_{\substack{x\\(x,y_0)\in S\cap C_{y_0,a}}}\lambda(x)\right| \\
&\le \sum_{j=1}^{K}(N+j)\max_{-N\le b\le c\le N}\max_{a}\left|\sum_{\substack{b\le x\le c\\x\equiv a \bmod j}}\lambda(x)\right| \\
&\le \sum_{j=1}^{K}4(N+j)\max_{0<c\le N}\max_{a}\left|\sum_{\substack{0<x\le c\\x\equiv a \bmod j}}\lambda(x)\right|.
\end{aligned}$$

We apply Lemma 3.2.8 and are done. □

Corollary 3.2.8. *Let A, K, N, d_0 and d_1 be positive integers such that $Kd_1 \le N^{1/2}/(\log N)^{2A+6}$. For $k = 1, 2, \ldots, K$, let S_k be a convex subset of $[-N, N]^2$ and let $L_k \subset \mathbb{Z}^2$ be a lattice coset of index $\frac{r_k}{d_0}k$ for some r_k dividing d_0d_1. Then*

$$\sum_{k\le K}\left|\sum_{(x,y)\in S_k\cap L_k}\lambda(x)\lambda(y)\right| \ll \tau(d_0d_1)\cdot\frac{N^2}{(\log N)^A},$$

where the implicit constant depends only on A.

Proof. For every $j \le Kd_1$, there are at most $\tau(d_0d_1)$ lattice cosets L_k of index j. There are no lattice cosets R_k of index greater than Kd_1. The statement then follows from Lemma 3.2.7. □

3.2.9 Anti-sieving

In the next two lemmas we use an upper-bound sieve not to find almost-primes, but to split the integers multiplicatively, with the almost-primes as an error term. A treatment by means of a cognate of Vaughan's identity would also be possible, but much more cumbersome. The error term would be the same.

Lemma 3.2.9. *For any given $M_2 > M_1 > 1$, there are $\sigma_d \in \mathbb{R}$ with $|\sigma_d| \leq 1$ and support on*

$$\{M_1 \leq d < M_2 : p < M_1 \Rightarrow p \nmid d\}$$

such that for any a, m, N_1 and N_2 with $0 \leq m < M_1$ and $0 \leq (N_2 - N_1)/m < M_2$,

$$\sum_{\substack{N_1 \leq n < N_2 \\ n \equiv a \bmod m}} \left| 1 - \sum_{d|n} \sigma_d \right| \ll \frac{\log M_1}{\log M_2} \frac{N_2 - N_1}{m} + M_2^2,$$

where the implied constant is absolute.

Proof. Set λ_d as in the Rosser-Iwaniec sieve with sieving set $\mathfrak{P} = \{p \text{ prime} : p \geq M_1, p \nmid m\}$ and upper cut $z = M_2$. Set $\sigma_1 = 0$, $\sigma_d = -\lambda_d$ for $d \neq 1$. Since

$$\sum_{\substack{N_1 \leq n < N_2 \\ n \equiv a \bmod m}} \left| \sum_{d|n} \lambda_d \right| \ll \frac{\log M_1}{\log M_2} \frac{N_2 - N_1}{m},$$

the statement follows. □

Note that some of the older combinatorial sieves would be enough for Lemma 3.2.9, provided that M_2 were kept greater than a given power of M_1.

Lemma 3.2.10. *Let $K/\mathbb{Q}$ be a number field. Let $M_2 > M_1 > 1$. Let $\jmath : K \to \mathbb{R}^{\deg(K/\mathbb{Q})}$ be a bijective $\mathbb{Q}$-linear map taking $\mathfrak{O}_K$ to $\mathbb{Z}^{\deg(K/\mathbb{Q})}$. Then there are $\sigma_{\mathfrak{d}} \in \mathbb{R}$*

with $|\sigma_{\mathfrak{d}}| \leq 1$ *and support on*

$$\{\mathfrak{d} : M_1 \leq N\mathfrak{d} < M_2,\ \gcd(\mathfrak{d}, [\mathbb{Z}^2 : L]) = 1,\ (N\mathfrak{p} < M_1 \Rightarrow \mathfrak{p} \nmid \mathfrak{d})\} \tag{3.2.25}$$

such that for any positive integer $N > M_2$*, any lattice coset* $L \subset \mathbb{Z}^{\deg(K/\mathbb{Q})}$ *with index* $[\mathbb{Z}^2 : L] < M_1$ *and any convex set* $S \subset [-N, N]^{\deg(K/\mathbb{Q})}$*,*

$$\sum_{\jmath(x) \in S \cap L} \left| 1 - \sum_{\substack{\mathfrak{d} \\ x \in \mathfrak{d}}} \sigma_{\mathfrak{d}} \right| \ll \frac{\log M_1}{\log M_2} \frac{\mathrm{Area}(S)}{[\mathfrak{O}_K : L]} + N^{\deg(K/\mathbb{Q})-1} M_2^2,$$

where the implied constant depends only on K*.*

Proof. Set $\lambda_{\mathfrak{d}}$ as in the generalized lower–bound Rosser–Iwaniec sieve ([Col2]) with sieving set $\{\mathfrak{p} \text{ prime} : N\mathfrak{p} \geq M_1, (N\mathfrak{p}, [\mathfrak{O}_K : L]) = 1\}$ and upper cut $z = M_2$. Set $\sigma_{\mathfrak{O}_K} = 0$, $\sigma_{\mathfrak{d}} = -\lambda_{\mathfrak{d}}$ for $\mathfrak{d} \neq \mathfrak{O}_K$. □

3.3 The average of λ on integers represented by a quadratic form

We say that a subset S of $\mathbb{C}$ is a *sector* if it is a sector of $\mathbb{R}^2$ under the natural isomorphism $(x + iy) \mapsto (x, y)$ from $\mathbb{C}$ to $\mathbb{R}^2$.

Lemma 3.3.1. *Let* K *be an imaginary quadratic extension of* $\mathbb{Q}$*. Let* $\mathfrak{d} \in I_K$*,* $\chi \in \Xi(C_{\mathfrak{d}}(K))$*. Let* S *be a sector of* $\mathbb{C}$*. Define the function* $\sigma_{S,\chi} : I_{K,\mathfrak{d}} \to \mathbb{Z}$ *by*

$$\sigma_{S,\chi}(\mathfrak{s}) = \sum_{\substack{s \in \mathfrak{I}^{-1}(\mathfrak{s}) \\ \iota(s) \in S}} \chi(s).$$

Then for any positive ϵ and any positive integer k there are Grössencharakters

$$\{\psi_n\}_{-\infty<n<\infty}$$

on $I_{K,\mathfrak{d}}$, sectors S_1, S_2 of angle ϵ, and complex numbers $\{c_n\}_{-\infty<n<\infty}$ such that

$$\begin{aligned} \sigma_{S,\chi}(\mathfrak{s}) &= \sum_{n=-\infty}^{\infty} c_n\psi_n(\mathfrak{s}) \quad \textit{for every } \mathfrak{s} \in I_{K,\mathfrak{d}} \textit{ with } \iota(\mathcal{I}^{-1}(\mathfrak{s})) \cap S_i = \emptyset, \\ \left|\sum_{n=-\infty}^{\infty} c_n\psi_n(\mathfrak{s})\right| &\ll 1 \quad \textit{for every } \mathfrak{s} \in I_{K,\mathfrak{d}}, \\ |c_0| \ll 1, \quad |c_n| \ll (k/\epsilon)^k|n|^{-(k+1)} &\quad \textit{for } n \neq 0. \end{aligned} \tag{3.3.1}$$

The implied constants are absolute.

Proof. For every $s \in \mathcal{I}(\mathfrak{O}_K)_{\mathfrak{d}}$,

$$\sigma_{S,\chi}(\mathfrak{I}(s)) = \sum_{u\in\mathfrak{O}_K^*} [\iota(us) \in S]\chi(us).$$

Since S is a sector, $\iota(us) \in S$ if and only if $\iota(u)\frac{\iota(s)}{|\iota(s)|} \in S$. Now $S \cap S^1$ is an interval. By Lemma 3.2.2 there are $\{a_n\}_{n=-\infty}^{\infty}$ such that

$$\begin{aligned} 0 \leq \sum_{n=-\infty}^{\infty} a_n x^n \leq 1 &\quad \text{for every } x \in S^1, \\ \sum_{n=-\infty}^{\infty} a_n x^n = [x \in S \cap S^1] &\quad \text{if } x \in S^1,\ x \notin S_1, S_2, \\ |a_n| \ll (k/\epsilon)^k|n|^{-(k+1)} &\quad \text{for } n \neq 0,\ \ |a_0| \ll 1, \end{aligned}$$

where S_1, S_2 are sectors of angle ϵ. Hence

$$\sum_{u\in\mathfrak{O}_K^*} [\iota(us) \in S]\chi(us) = \sum_{u\in\mathfrak{O}_K^*} \sum_{n=-\infty}^{\infty} a_n \left(\iota(u)\frac{\iota(s)}{|\iota(s)|}\right)^n \chi(us)$$

if $s \notin uS_1, uS_2$ for every $u \in \mathfrak{O}_K^*$. Changing the order of summation,

$$\sum_{u\in\mathfrak{O}_K^*}\sum_{n=-\infty}^{\infty} a_n \left(\iota(u)\frac{\iota(s)}{|\iota(s)|}\right)^n \chi(us) = \sum_{n=-\infty}^{\infty} a_n \sum_{u\in\mathfrak{O}_K^*} \iota(u)^n\chi(u)\left(\frac{\iota(s)}{|\iota(s)|}\right)^n \chi(s).$$

We will have $\sum_{u\in\mathfrak{O}_K^*} u^n\chi(u) \neq 0$ only when $u^n\chi(u) = 1$ for all $u \in \mathfrak{O}_K^*$. Then there is a Grössencharakter ψ_n such that

$$\psi_n(\mathfrak{s}) = \left(\frac{\iota(s)}{|\iota(s)|}\right)^n \chi(s)$$

for every $s \in \mathcal{I}^{-1}(\mathfrak{s})$. Hence

$$\sum_{n=-\infty}^{\infty} a_n \sum_{u\in\mathfrak{O}_K^*} \iota(u)^n\chi(u)\left(\frac{\iota(s)}{|\iota(s)|}\right)^n \chi(s) = \sum_{\substack{-\infty<n<\infty \\ \iota(u)^n\chi(u)=1}} (\#\mathfrak{O}_K^*)a_n\psi_n(\mathfrak{s}).$$

Set

$$c_n = \begin{cases} (\#\mathfrak{O}_K^*)a_n & \text{if } \iota(u)^n\chi(u) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

□

Let the sector $S \subset \mathbb{R}^2$ be a subquadrant. Define

$$\rho(x,y) = x/y$$

$$\gamma_-(S) = \inf_{(x,y)\in S} x/y,$$

$$\gamma_+(S) = \sup_{(x,y)\in S} x/y.$$

If S is a subquadrant, $\gamma_-(S)$ and $\gamma_+(S)$ are finite non-zero real numbers of the same sign. Moreover, $(x,y) \in S$ if and only if $\rho(x,y) \in (\gamma_-(S), \gamma_+(S))$. The sign $\operatorname{sgn}(x)$ is

the same for all $x \in S$. We call it $\operatorname{sgn}(S)$ and define

$$H_S = \{(x, y) \in \mathbb{R}^2 : \operatorname{sgn}(x) = \operatorname{sgn}(S)\}.$$

For $K/\mathbb{Q}$ a real quadratic extension, let $\iota : \mathcal{I}(K) \to \mathbb{R}^2$ be the embedding given by $\iota(a) = (\iota_1(a), \iota_2(a))$.

Lemma 3.3.2. *Let K be a real quadratic extension of $\mathbb{Q}$. Let $\mathfrak{d} \in I_K$, $\chi \in \Xi(C_{\mathfrak{d}}(K))$. Let S be a subquadrant of $\mathbb{R}^2$. Define the function $\sigma_{S,\chi} : I_{K,\mathfrak{d}} \to \mathbb{Z}$ by*

$$\sigma_{S,\chi}(\mathfrak{s}) = \sum_{\substack{s \in \mathcal{J}^{-1}(\mathfrak{s}) \\ \iota(s) \in S}} \chi(s).$$

Then for any positive ϵ and any positive integer k there are Grössencharakters

$$\{\psi_n\}_{-\infty<n<\infty}$$

on $I_{K,\mathfrak{d}}$, sectors S_1, S_2 of hyperbolic angle at most ϵ, and complex numbers $\{c_n\}_{-\infty<n<\infty}$ such that

$$\begin{aligned}
\sigma_{S,\chi}(\mathfrak{s}) &= \sum_{n=-\infty}^{\infty} c_n \psi_n(\mathfrak{s}) \quad \textit{for every } \mathfrak{s} \in I_{K,\mathfrak{d}} \textit{ with } \iota(\mathcal{I}^{-1}(\mathfrak{s})) \cap S_i = \emptyset, \\
\left| \sum_{n=-\infty}^{\infty} c_n \psi_n(\mathfrak{s}) \right| &\ll \frac{|\log(\gamma_+(\iota(S))/\gamma_-(\iota(S)))|}{|\log(\iota_1(u_1)/\iota_2(u_1))|} + k_{\mathfrak{d}} \quad \textit{for every } \mathfrak{s} \in I_{K,\mathfrak{d}}, \\
|c_0|, |c_1| &\ll \frac{|\log(\gamma_+(\iota(S))/\gamma_-(\iota(S)))|}{|\log(\iota_1(u_1)/\iota_2(u_1))|} \\
|c_n| &\ll (k k_{\mathfrak{d}}/\epsilon)^k |n|^{-(k+1)} \quad \textit{for } n \neq 0, 1,
\end{aligned}$$

where u_1, ι_1 and ι_2 are as in subsection 3.2.2. The implied constants are absolute.

Proof. For every $s \in \mathcal{I}(\mathfrak{O}_K)_{\mathfrak{d}}$ with $\iota(s) \in H_S$,

$$\sigma_{S,\chi}(\mathfrak{I}(s)) = \sum_{u \in \mathfrak{O}_K^*} [\iota(us) \in S]\chi(us).$$

Since $\iota_1(u_1)$ is positive, $\iota(s) \in H_S$ implies $\iota(u_1^k s) \in H_S$, $\iota(-u_1^k s) \notin H_S$ for every $k \in \mathbb{Z}$. Hence

$$\begin{aligned}
\sigma_{S,\chi}(\mathfrak{I}(s)) &= \sum_{k=-\infty}^{\infty} [\iota(u_1^k s) \in S]\chi(u^k s) \\
&= \sum_{k=-\infty}^{\infty} [\iota(u_1^k s) \in (S \cap (-S))]\chi(u_1^k s) \\
&= \sum_{k=-\infty}^{\infty} [\rho(\iota(u_1^k s)) \in (\gamma_-(S), \gamma_+(S))]\chi(u_1^k s).
\end{aligned}$$

Let $k_{\mathfrak{d}}$, $l_{\mathfrak{d}}$, $r_{\mathfrak{d}}$ be as in section 3.2.2. Let C_0 is the largest integer smaller than $\frac{|\log(\gamma_+(\iota(S))/\gamma_-(\iota(S)))|}{\log l_{\mathfrak{d}}}$. Let $\gamma_0 = \gamma_-(S) l_{\mathfrak{d}}^{C_0}$. Then

$$\sigma_{S,\chi}(\mathfrak{I}(s)) = \chi(s)\left(C_0 k_{\mathfrak{d}}[\chi(u_1) = 1] + \sum_{k=-\infty}^{\infty} [\rho(\iota(u_1^k s)) \in (\gamma_0, \gamma_+(S))]\chi(u_1^k)\right).$$

Assume $\operatorname{sgn}(\rho(\iota(s))) = \operatorname{sgn}(\gamma_0)$. Then there is exactly one integer n such that $l_{\mathfrak{d}}^n s \in (\gamma_0, l_{\mathfrak{d}}\gamma_0]$. Let $\phi : \mathbb{R}^* \to S^1$ be given by

$$\phi(r) = e^{2\pi i \frac{\log|r|}{\log l_{\mathfrak{d}}}}.$$

Define $\Phi = \phi \circ \rho \circ \iota : K \mapsto S^1$. Then

$$\sum_{k=-\infty}^{\infty} [\rho(\iota(u_1^k s)) \in (\gamma_0, \gamma_+(S))]\chi(u_1^k) = \sum_{k=0}^{k_{\mathfrak{d}}-1} [\Phi(u_1^{r_{\mathfrak{d}} k} s) \in (\phi(\gamma_0), \phi(\gamma_+(S)))]\chi(u_1^{r_{\mathfrak{d}} k}).$$

By Lemma 3.2.2 there are $\{a_n\}_{n=-\infty}^{\infty}$ such that

$$0 \leq \sum_{n=-\infty}^{\infty} a_n x^n \leq 1 \quad \text{for every } x \in S^1,$$

$$\sum_{n=-\infty}^{\infty} a_n x^n = [x \in S \cap S^1] \quad \text{if } d(x, \gamma_0), d(x, \gamma_+(S)) \geq \epsilon/2k_{\mathfrak{d}},$$

$$|a_n| \ll (kk_{\mathfrak{d}}/\epsilon)^k |n|^{-(k+1)} \quad \text{for } n \neq 0, \quad |a_0| \ll 1.$$

Hence

$$\sigma_{S,\chi}(\mathfrak{I}(s)) = \chi(s) \left(C_0 k_{\mathfrak{d}} [\chi(u_1) = 1] + \sum_{n=-\infty}^{\infty} a_n \left(\sum_{k=0}^{k_{\mathfrak{d}}-1} \Phi(u_1^{r_{\mathfrak{d}} k})^n \chi(u_1^{r_{\mathfrak{d}} k}) \right) \Phi(s)^n \right),$$

provided that $d(\Phi(u_1^{r_{\mathfrak{d}} k} s), \gamma_0) \geq \epsilon/2$, $d(\Phi(u_1^{r_{\mathfrak{d}} k} s), \gamma_+(S)) \geq \epsilon/2$ for every non-negative k less than $k_{\mathfrak{d}}$. We will have

$$\sum_{k=0}^{k_{\mathfrak{d}}-1} \Phi(u_1^{r_{\mathfrak{d}} k})^n \chi(u_1^{r_{\mathfrak{d}} k}) \neq 0 \tag{3.3.2}$$

only when $\Phi(u_1^{r_{\mathfrak{d}}})^n \chi(u_1^{r_{\mathfrak{d}}}) = 1$.

Suppose $\frac{\iota_1(u_1)}{\iota_2(u_1)} < 0$. Then there is a Grössencharakter

$$\psi_n(\mathfrak{s}) = \chi(s) \operatorname{sgn}(\rho(\iota(s)))^{n_0} \Phi(s)^n,$$

where

$$n_0(n) = \begin{cases} 1 & \text{if } \chi(u_1)\Phi(u_1)^n = 1 \\ -1 & \text{if } \chi(u_1)\Phi(u_1)^n = -1. \end{cases}$$

Let

$$c_n = a_n k_{\mathfrak{d}} [\Phi(u_1^2)^n \chi(u_1^2) = 1] \operatorname{sgn}(\gamma_0)^{n_0(n)} + C_0 k_{\mathfrak{d}} [\chi(u_1) = 1][n = 0].$$

Thus

$$\sigma_{S,\chi}(\mathfrak{I}(s)) = \sum_{n=-\infty}^{\infty} c_n \psi_n(\mathfrak{I}(s))$$

for every $s \in \mathcal{I}(\mathfrak{O}_K)_{\mathfrak{d}}$ with $\iota(s) \in H_S$, $\operatorname{sgn}(\rho(\iota(s))) = \operatorname{sgn}(\gamma_0)$ and

$$d(\Phi(u_1^{r_{\mathfrak{d}} k} s), \gamma_0) \geq \epsilon/2k_{\mathfrak{d}}, \quad d(\Phi(u_1^{r_{\mathfrak{d}} k} s), \gamma_+(S)) \geq \epsilon/2k_{\mathfrak{d}}$$

for every $0 \leq k < k_{\mathfrak{d}}$. Since $\frac{\iota_1(u_1)}{\iota_2(u_1)} < 0$, for every $s \in \mathcal{I}(\mathfrak{O}_K)_{\mathfrak{d}}$ there is a $u \in \mathfrak{O}_K^*$ such that $\iota(us) \in H_S$, $\operatorname{sgn}(\rho(\iota(us))) = \operatorname{sgn}(\gamma_0)$. Hence

$$\sigma_{S,\chi}(\mathfrak{s}) = \sum_{n=-\infty}^{\infty} c_n \psi_n(\mathfrak{s})$$

provided that $d(\Phi(s), \gamma_0) \geq \epsilon/2k_{\mathfrak{d}}$, $d(\Phi(s), \gamma_+(S)) \geq \epsilon/2k_{\mathfrak{d}}$ for every $s \in \mathcal{I}^{-1}(\mathfrak{s})$.

Suppose now $\frac{\iota_1(u_1)}{\iota_2(u_1)} > 0$. We have (3.3.2) only when $\Phi(u_1)\chi(u_1) = 1$. Then there are Grössencharakters

$$\begin{aligned} \psi_{n+}(\mathfrak{s}) &= \chi(s)\Phi(s)^n, \\ \psi_{n-}(\mathfrak{s}) &= \chi(s)\operatorname{sgn}(\rho(\iota(s)))\Phi(s)^n \end{aligned}.$$

Let

$$\begin{aligned} c_{n+} &= a_n k_{\mathfrak{d}}[\Phi(u_1)^n \chi(u_1) = 1] + C_0 k_{\mathfrak{d}}[\chi(u_1) = 1][n = 0] \\ c_{n-} &= (a_n k_{\mathfrak{d}}[\Phi(u_1)^n \chi(u_1) = 1] + C_0 k_{\mathfrak{d}}[\chi(u_1) = 1][n = 0]) \operatorname{sgn}(\gamma_0). \end{aligned}$$

Then

$$\sigma_{S,\chi}(\mathfrak{I}(s)) = \sum_{n=-\infty}^{\infty} \frac{1}{2}(c_{n+}\psi_{n+}(\mathfrak{I}(s)) + c_{n-}\psi_{n-}(\mathfrak{I}(s))) \tag{3.3.3}$$

for every $s \in \mathcal{I}_{K,\mathfrak{d}}$ with $\iota(s) \in H_S$ and

$$d(\Phi(u_1^{r_{\mathfrak{d}} k} s), \gamma_0) \geq \epsilon/2k_{\mathfrak{d}}, \quad d(\Phi(u_1^{r_{\mathfrak{d}} k} s), \gamma_+(S)) \geq \epsilon/2k_{\mathfrak{d}}$$

for every $0 \leq k < k_{\mathfrak{d}}$. If $\operatorname{sgn}(\rho(\iota(s))) \neq \operatorname{sgn}(\gamma_0)$, both sides of (3.3.3) are equal to zero.

Hence, for every $\mathfrak{s} \in I_{K,\mathfrak{d}}$,

$$\sigma_{S,\chi}(\mathfrak{s}) = \sum_{n=-\infty}^{\infty} \frac{1}{2}(c_{n+}\psi_{n+}(\mathfrak{s}) + c_{n-}\psi_{n-}(\mathfrak{s}))$$

provided that $d(\Phi(s), \gamma_0) \geq \epsilon/2k_{\mathfrak{d}}$, $d(\Phi(s), \gamma_+(S)) \geq \epsilon/2k_{\mathfrak{d}}$ for every $s \in \mathcal{I}^{-1}(\mathfrak{s})$.

Now let $s \in \mathcal{I}(\mathfrak{O}_K)_{\mathfrak{d}}$ be given with

$$d(\Phi(s), \gamma_0) < \epsilon/2k_{\mathfrak{d}}.$$

Then

$$\left| \frac{\log|\rho(s)|}{\log l_{\mathfrak{d}}} - x \right| < \epsilon/2k_{\mathfrak{d}}$$

for some $x \in \phi^{-1}(\gamma_0)$. Let us be given $\mathfrak{s} \in I_{K,\mathfrak{d}}$. Then

$$d(\Phi(s), \gamma_0) < \epsilon/2k_{\mathfrak{d}} \quad \text{for some } s \in \mathcal{I}^{-1}(s)$$

if and only if

$$\left| \frac{\log|\rho(s)|}{\log l_{\mathfrak{d}}} - x_0 \right| < \epsilon/2k_{\mathfrak{d}} \quad \text{for some } s \in \mathcal{I}^{-1}(\mathfrak{s}), \tag{3.3.4}$$

where x_0 is any fixed element of $\phi^{-1}(\gamma_0)$. Clearly (3.3.4) is equivalent to

$$(x_0 - \epsilon/2k_{\mathfrak{d}}) \log l_{\mathfrak{d}} < \log|\rho(s)| < (x_0 + \epsilon/2k_{\mathfrak{d}}) \log l_{\mathfrak{d}},$$

that is,

$$x_0 \log l_{\mathfrak{d}} - \frac{\epsilon r_{\mathfrak{d}}}{2} \log\left(\frac{\iota_1(u_1)}{\iota_2(u_1)}\right) < \log|\rho(s)| < x_0 \log l_{\mathfrak{d}} + \frac{\epsilon r_{\mathfrak{d}}}{2} \log\left(\frac{\iota_1(u_1)}{\iota_2(u_1)}\right).$$

Thus S is constrained to a section of hyperbolic angle $\frac{\epsilon r_{\mathfrak{d}}}{2} \log\left(\frac{\iota_1(u_1)}{\iota_2(u_1)}\right)$. The statement follows. $\square$

Let $Q(x,y)$ be a primitive, irreducible quadratic form. Let $K = \mathbb{Q}(\sqrt{b^2-4ac})$. We define $\phi_Q : \mathbb{Q}^2 \to K$ to be the map given by

$$\phi_Q(x,y) = \alpha_1 x + \alpha_2 y,$$

where α_1, α_2 are as in Lemma 3.2.1. As before, we define

$$\iota(s) = \begin{cases} (\iota_1(s), \iota_2(s)) \in \mathbb{R}^2 & \text{if } K \text{ is real} \\ \iota_1(s) \in \mathbb{C} \sim \mathbb{R}^2 & \text{if } K \text{ is imaginary.} \end{cases}$$

for $s \in \mathcal{I}(K)$. The map $\iota \circ \phi_Q : \mathbb{Q}^2 \to \mathbb{R}^2$ is linear. For any sector S of $\mathbb{R}^2$, there is a sector S_Q of $\mathbb{R}^2$ such that $(\iota \circ \phi_Q)(S \cap \mathbb{Q}^2) = S_Q \cap \iota(K)$.

We recall the definition of $\sigma_{S,\chi} : I_{K,\mathfrak{d}} \to \mathbb{Z}$ in the statements of Lemmas 3.3.1 and 3.3.2.

Lemma 3.3.3. *Let $Q(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a primitive, irreducible quadratic form. Let $K = \mathbb{Q}(\sqrt{b^2-4ac})$. Let $L \subset \mathbb{Z}^2$ be a lattice coset, $S \subset \mathbb{R}^2$ a sector. If K is real, assume S_Q is a subquadrant. Let $d = a \cdot d_{\mathrm{sq}(b^2-4ac)}[\mathbb{Z}^2 : L]$. Then there are sectors $\{S_\mathfrak{r}\}_{\mathfrak{r}|d^\infty}$, $S_\mathfrak{r} \subset \mathbb{R}^2$, and complex numbers $\{a_{\mathfrak{r}\chi}\}_{r|d^\infty, \chi \in \Xi(C_d(K))}$, $|a_{\mathfrak{r}\chi}| \leq \frac{d}{\#C_d(K)}$, such that*

$$\#\{x,y \in S \cap L : |Q(x,y)| = m\} = \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r} = \gcd(am, d^\infty)}} \sum_{\chi \in \Xi(C_d(K))} a_{\mathfrak{r}\chi} \sum_{\substack{\mathfrak{s} \\ N\mathfrak{s} = \frac{|am|}{\gcd(am, d^\infty)}}} \sigma_{S_\tau, \chi}(\mathfrak{s})$$

for every positive integer m. If K is real, then, for every $\mathfrak{r}|d^\infty$, $S_\mathfrak{r}$ is a subquadrant satisfying

$$|\log(\gamma_+(S_\mathfrak{r})/\gamma_-(S_\mathfrak{r}))| = |\log(\gamma_+(S_Q)/\gamma_-(S_Q))|.$$

Proof. By Lemma 3.2.1,

$$\#\{x, y \in S \cap L : |Q(x, y)| = m\} = \sum_{\substack{s \in \phi_Q(L) \\ \iota(s) \in S_Q \\ |Ns| = |am|}} 1.$$

For every $s \in \mathfrak{O}_K$ of norm $Ns = \pm am$, there is exactly one ideal of norm $\gcd(am, d^\infty)$ containing x. Hence

$$\sum_{\substack{s \in \phi_Q(L) \\ \iota(s) \in S_Q \\ |Ns| = |am|}} 1 = \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r} = \gcd(am, d^\infty)}} \sum_{\substack{s \in \phi_Q(L) \cap \mathfrak{r} \\ \iota(s) \in S_Q \\ |Ns| = |am|}} 1.$$

Since, by Lemma 3.2.1, $\phi_Q(L)$ is an additive subgroup of $\mathfrak{O}_K$ of index $d = [\mathfrak{O}_K : \phi_Q(L)] = a \cdot d_{sq(b^2-4ac)}[\mathbb{Z}^2 : L]$, $\phi_Q(L) \cap \mathfrak{r}$ is an additive subgroup of $\mathfrak{r}$ of index dividing d. Therefore, whether or not a given $s \in \mathfrak{r}$ is an element of $\phi_Q(L) \cap \mathfrak{r}$ depends only on $s \bmod d\mathfrak{r}$. If $N\mathfrak{r} = \gcd(am, d^\infty)$ and $Ns = am$, then $N\mathfrak{r} = \gcd(Ns, d^\infty)$, and so, given that $s \in \mathfrak{r}$, Ns/Nr is prime to d. Choose $r \in \mathfrak{I}^{-1}(\mathfrak{r})$. Then $s/r \in \mathcal{I}(\mathfrak{O}_K)_d$. Moreover, whether or not s is an element of $\phi_Q(L) \cap \mathfrak{r}$ depends only on the equivalence class $\langle s/r \rangle$ of s/r in $C_d(K)$. In other words, there is a subset $C_\mathfrak{r}$ of $C_d(K)$ such that $x/r \in \phi_Q(L) \cap \mathfrak{r}$ if and only if $\langle x/r \rangle \in C_\mathfrak{r}$. Then

$$\#\{x, y \in S \cap L : |Q(x, y)| = m\} = \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r} = \gcd(am, d^\infty)}} \sum_{\substack{s \in \mathcal{I}(\mathfrak{O}_K)_d \\ \langle s \rangle \in C_\mathfrak{r} \\ \iota(rs) \in S_Q \\ |N(\mathcal{I}(s))| = am/\gcd(am, r^\infty)}} 1.$$

For $\chi \in \Xi(C_d(K))$, let $a_{\mathfrak{r}\chi} = \frac{1}{\#C_d(K)} \sum_{c \in C_\mathfrak{r}} \overline{\chi(c)}$. Then

$$[\langle s \rangle \in C_\mathfrak{r}] = \sum_{\chi \in \Xi(C_d(K))} a_{\mathfrak{r}\chi} \chi(s).$$

Hence $\#\{x, y \in S \cap L : |Q(x,y)| = m\}$ equals

$$\sum_{\substack{\mathfrak{r} \\ N\mathfrak{r}=\gcd(am,d^\infty)}} \sum_{\chi \in \Xi(C_d(K))} a_{\mathfrak{r}\chi} \sum_{\substack{s \in \mathcal{I}(\mathfrak{O}_K)_d \\ \iota(rs) \in S \\ N(\mathcal{I}(s))=|am|/\gcd(|am|,d^\infty)}} \chi(s)$$

$$= \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r}=\gcd(am,d^\infty)}} \sum_{\chi \in \Xi(C_d(K))} a_{\mathfrak{r}\chi} \sum_{\substack{\mathfrak{s} \\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)}}} \sigma_{S_\tau,\chi}(\mathfrak{s}),$$

where

$$S_{\mathfrak{r}} = \begin{cases} \iota(r)^{-1} S_Q & \text{if } K \text{ is imaginary,} \\ \{(x,y) \in \mathbb{R}^2 : (\iota_i(r)x, \iota_2(r)y) \in S_Q\} & \text{if } K \text{ is real.} \end{cases}$$

□

Lemma 3.3.4. *Let K be a quadratic extension of $\mathbb{Q}$. Let a be a non-zero rational integer. Then, for any rational integer r dividing a, any ideal $\mathfrak{d} \in I_{K,r}$ of norm*

$$N\mathfrak{d} \ll (\log N)^A \tag{3.3.5}$$

and any Grössencharakter ψ on $I_{K,\mathfrak{d}}$ of size $\mathcal{S}(\psi) \ll e^{(\log x)^{3/5}(\log\log x)^{1/5}}$, we have

$$\sum_{\substack{\mathfrak{s} \in I_{K,\mathfrak{d}} \\ N\mathfrak{s} \le x \\ r | N\mathfrak{s}}} \psi(\mathfrak{s})\lambda(N\mathfrak{s}) \ll x e^{-C\frac{(\log x)^{2/3}}{(\log\log x)^{1/5}}}, \tag{3.3.6}$$

where C and the implied constant in (3.3.6) depend only on K, A, r, and the implied constant in (3.3.5).

Proof. For any $\mathfrak{s} \in I_{K,\mathfrak{d}}$,

$$\begin{aligned}
[r|N\mathfrak{s}] = [r|N(\gcd(\mathfrak{s}, r^\infty))] &= 1 - \sum_{\substack{\mathfrak{r}|r^\infty \\ r\nmid N\mathfrak{r}}} [\mathfrak{r} = \gcd(\mathfrak{s}, r^\infty)] \\
&= 1 - \sum_{\substack{\mathfrak{r}|r^\infty \\ r\nmid N\mathfrak{r}}} \sum_{\mathfrak{m}|\operatorname{rad}(r)} \mu_K(\mathfrak{m})[\mathfrak{r}\mathfrak{m}|\gcd(\mathfrak{s}, r^\infty)] \\
&= 1 - \sum_{\substack{\mathfrak{r}|r^\infty \\ r\nmid N\mathfrak{r}}} \sum_{\mathfrak{m}|\operatorname{rad}(r)} \mu_K(\mathfrak{m})[\mathfrak{r}\mathfrak{m}|\mathfrak{s}].
\end{aligned}$$

Hence

$$\sum_{\substack{\mathfrak{s}\in I_{K,\mathfrak{d}} \\ N\mathfrak{s}\le x \\ r|N\mathfrak{s}}} \psi(\mathfrak{s})\lambda(N\mathfrak{s}) = \sum_{\substack{\mathfrak{s}\in I_{K,\mathfrak{d}} \\ N\mathfrak{s}\le x}} \psi(\mathfrak{s})\lambda(N\mathfrak{s}) - \sum_{\substack{\mathfrak{r}|r^\infty \\ r\nmid N\mathfrak{r}}} \sum_{\mathfrak{m}|\operatorname{rad}(r)} \mu_K(\mathfrak{m}) \sum_{\substack{\mathfrak{s}\in I_{K,\mathfrak{d}} \\ N\mathfrak{s}\le x \\ \mathfrak{r}\mathfrak{m}|\mathfrak{s}}} \psi(\mathfrak{s})\lambda(N\mathfrak{s}). \tag{3.3.7}$$

We can rewrite the second term on the right side of (3.3.7) as

$$\sum_{\substack{\mathfrak{r}|r^\infty \\ r\nmid N\mathfrak{r}}} \sum_{\mathfrak{m}|\operatorname{rad}(r)} \mu_K(\mathfrak{m})\psi(\mathfrak{r}\mathfrak{m})\lambda(N(\mathfrak{r}\mathfrak{m})) \sum_{\substack{\mathfrak{s}\in I_{K,\mathfrak{d}} \\ N\mathfrak{s}\le x/N(\mathfrak{r}\mathfrak{m})}} \psi(\mathfrak{s})\lambda(N\mathfrak{s}).$$

The statement now follows from Lemma 3.2.4. □

Lemma 3.3.5. *Let K be a finite extension of $\mathbb{Q}$. Let d be a non-zero rational integer. Then*

$$\sum_{\substack{\mathfrak{r}\in I_K \\ \mathfrak{r}|d^\infty \\ X^{1/2}<N\mathfrak{r}\le X}} \frac{1}{N\mathfrak{r}} \ll \frac{(\log X)^C}{X^{1/2}},$$

where C and the implied constant depend only on K and d.

Proof. Let $\mathfrak{p}$ be the divisor of d of largest norm. Every $\mathfrak{r} \in I_K$ with $\mathfrak{r}|d^\infty$ and $N\mathfrak{r} >$

$X^{1/2}$ has a divisor $\mathfrak{d}|\mathfrak{r}$ of norm $X^{1/2} < N\mathfrak{d} \leq X^{1/2}N\mathfrak{p}$. Hence

$$\sum_{\substack{\mathfrak{r}\in I_K \\ \mathfrak{r}|d^\infty \\ X^{1/2}<N\mathfrak{r}\leq X}} \frac{1}{N\mathfrak{r}} \leq \sum_{\substack{\mathfrak{d}\in I_K \\ \mathfrak{d}|d^\infty \\ X^{1/2}<N\mathfrak{d}\leq X^{1/2}N\mathfrak{p}}} \frac{1}{N\mathfrak{d}} \sum_{\substack{\mathfrak{a}\in I_K \\ N\mathfrak{a}\leq X^{1/2}}} \frac{1}{N\mathfrak{a}}$$
$$\ll (\log X)^{c_1} \frac{1}{X^{1/2}} \sum_{\substack{\mathfrak{d}\in I_K \\ \mathfrak{d}|d^\infty \\ N\mathfrak{d}\leq X^{1/2}N\mathfrak{p}}} 1 \ll (\log X)^{c_1} \frac{1}{X^{1/2}} (\log X)^{c_2}.$$

□

Lemma 3.3.6. *Let $Q(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a primitive, irreducible quadratic form. Let $K = \mathbb{Q}(\sqrt{b^2-4ac})$. Let $L \subset \mathbb{Z}^2$ be a lattice coset, $S \subset \mathbb{R}^2$ a sector. Assume*

$$[\mathbb{Z}^2 : L] \ll (\log X)^A. \tag{3.3.8}$$

If K is real, assume S_Q is a subquadrant satisfying

$$|\log(\gamma_+(S_Q)/\gamma_-(S_Q))| \ll (\log X)^A. \tag{3.3.9}$$

Then

$$\sum_{\substack{x,y\in S\cap L \\ |Q(x,y)|\leq X}} \lambda(Q(x,y)) \ll X e^{-C\frac{(\log X)^{2/3}}{(\log\log X)^{1/5}}}, \tag{3.3.10}$$

where C and the implied constant depend on a, b, c, A and the implied constants in (3.3.8) and (3.3.9).

Proof. By Lemma 3.3.3,

$$\sum_{\substack{x,y\in S\cap L \\ |Q(x,y)|\leq X}} \lambda(Q(x,y)) = \sum_{m\leq X} \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r}=\gcd(am,d^\infty)}} \sum_{\chi\in\Xi(C_d(K))} a_{\mathfrak{r}\chi} \sum_{\substack{\mathfrak{s} \\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)}}} \sigma_{S_\mathfrak{r},\chi}(\mathfrak{s})\lambda(m),$$

where $d = a \cdot d_{\mathrm{sq}(b^2-4ac)}[\mathbb{Z}^2 : L]$. Since $a_{\mathfrak{r}\chi} \leq \frac{d}{\#C_d(K)}$, it will be enough to bound

$$\sum_{m \leq X} \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r} = \gcd(am, d^\infty)}} \sum_{\substack{\mathfrak{s} \\ N\mathfrak{s} = \frac{|am|}{\gcd(am, d^\infty)}}} \sigma_{S_\tau, \chi}(\mathfrak{s}) \lambda(m). \tag{3.3.11}$$

We will take ϵ to be a positive number whose value we shall set later. By Lemmas 3.3.1 and 3.3.2 with $k = 1$,

$$\sigma_{S,\chi}(\mathfrak{s}) = \sum_{n=-\infty}^{\infty} c_n \psi_n(\mathfrak{s}) \quad \text{for every } \mathfrak{s} \in I_{K,\mathfrak{d}} \text{ with } \iota(\mathcal{I}^{-1}(\mathfrak{s})) \cap S_i = \emptyset,$$

$$\left| \sum_{n=-\infty}^{\infty} c_n \psi_n(\mathfrak{s}) \right| \ll \frac{|\log(\gamma_+(\iota(S))/\gamma_-(\iota(S)))|}{|\log(\iota_1(u_1)/\iota_2(u_1))|} + k_{\mathfrak{d}} \quad \text{for every } \mathfrak{s} \in I_{K,\mathfrak{d}},$$

where S_1, S_2 are sectors of angle at most ϵ (if $K/\mathbb{Q}$ is imaginary) or of hyperbolic angle at most ϵ (if $K/\mathbb{R}$ is real), and

$$|c_n| \ll \frac{|n|^{-2}}{\epsilon} \quad \text{for } K/\mathbb{Q} \text{ imaginary},$$

$$|c_n| \ll \frac{k_{\mathfrak{d}}}{\epsilon} |n|^{-2} \quad \text{for } K/\mathbb{Q} \text{ real}, n \neq 0, 1,$$

$$|c_0|, |c_1| \ll \max\left(1, \frac{|\log(\gamma_+(\iota(S))/\gamma_-(\iota(S)))|}{|\log(\iota_1(u_1)/\iota_2(u_1))|}\right) \quad \text{for } K/\mathbb{Q} \text{ real}.$$

Let B be a large number whose value will be set later. Since $|\psi_n(\mathfrak{s})| = 1$, $d \ll (\log N)^A$ and $C_0 \ll (\log N)^A$, the absolute value of the difference between (3.3.11) and

$$\sum_{m \leq X} \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r} = \gcd(am, d^\infty)}} \sum_{\substack{\mathfrak{s} \\ N\mathfrak{s} = \frac{|am|}{\gcd(am, d^\infty)}}} \sum_{|n| \leq B} c_n \psi_n(\mathfrak{s}) \lambda(m) \tag{3.3.12}$$

is at most a constant times

$$\sum_{m\le X}\sum_{\substack{\mathfrak{r}\\ N\mathfrak{r}=\gcd(am,d^\infty)}}\sum_{\substack{\mathfrak{s}\\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)}}}\frac{k_{\mathfrak{d}}}{B\epsilon}\ll\sum_{m\le X}\frac{k_{\mathfrak{d}}\tau(m)}{B\epsilon}\ll\frac{k_{\mathfrak{d}}X\log X}{B\epsilon}.$$

By (3.3.8), the absolute value of

$$\sum_{m\le X}\sum_{\substack{\mathfrak{r}\\ N\mathfrak{r}=\gcd(am,d^\infty)}}\sum_{\substack{\mathfrak{s}\\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)}}}\sum_{n=-B}^{B}c_n\psi_n(\mathfrak{s})\lambda(m)$$

is at most a constant times

$$\max((\log X)^{3A},(\log X)^{2A}/\epsilon)\max_{-B\le n\le B}\left|\sum_{m\le X}\sum_{\substack{\mathfrak{r}\\ N\mathfrak{r}=\gcd(am,d^\infty)}}\sum_{\substack{\mathfrak{s}\\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)}}}\psi_n(N\mathfrak{s})\right|.$$

Clearly

$$\sum_{m\le X}\sum_{\substack{\mathfrak{r}\\ N\mathfrak{r}=\gcd(am,d^\infty)}}\sum_{\substack{\mathfrak{s}\\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)}}}\psi_n(\mathfrak{s})\lambda(m)=\lambda(a)\sum_{\substack{\mathfrak{r}\\ \mathfrak{r}|d^\infty}}\lambda(N\mathfrak{r})\sum_{\substack{\mathfrak{s}\\ \frac{a}{\gcd(a,d^\infty)}|N\mathfrak{s}\\ N\mathfrak{s}\le\frac{aX}{N\mathfrak{r}}}}\psi_n(\mathfrak{s})\lambda(N\mathfrak{s}).$$

Now

$$\sum_{\substack{\mathfrak{r}\\ \mathfrak{r}|d^\infty}}\left|\sum_{\substack{\mathfrak{s}\\ \frac{a}{\gcd(a,d^\infty)}|N\mathfrak{s}\\ N\mathfrak{s}\le\frac{aX}{N\mathfrak{r}}}}\psi_n(\mathfrak{s})\lambda(N\mathfrak{s})\right|\le\sum_{\substack{\mathfrak{r}\\ \mathfrak{r}|d^\infty\\ X^{1/2}<N\mathfrak{r}\le aX}}\frac{aX}{N\mathfrak{r}}\log\left(\frac{aX}{N\mathfrak{r}}\right)$$

$$+\sum_{\substack{\mathfrak{r}\\ \mathfrak{r}|d^\infty\\ N\mathfrak{r}\le X^{1/2}}}\left|\sum_{\substack{\mathfrak{s}\\ \frac{a}{\gcd(a,d^\infty)}|N\mathfrak{s}\\ N\mathfrak{s}\le\frac{aX}{N\mathfrak{r}}}}\psi_n(\mathfrak{s})\lambda(N\mathfrak{s})\right|.$$

Set $B = e^{(\log x)^{3/5}(\log\log x)^{1/5}}/(\log x)^A$. We bound the first term on the right by Lemma 3.3.5 and the second term by Lemma 3.3.4, obtaining

$$\sum_{\substack{\mathfrak{r} \\ \mathfrak{r}|d^\infty}} \left| \sum_{\substack{\mathfrak{s} \\ \frac{a}{\gcd(a,d^\infty)}|N\mathfrak{s} \\ N\mathfrak{s}\le \frac{aX}{N\mathfrak{r}}}} \psi_n(\mathfrak{s})\lambda(N\mathfrak{s}) \right| \ll \frac{aX}{X^{1/2}}(\log X)^C + \sum_{\substack{\mathfrak{r} \\ \mathfrak{r}|d^\infty \\ N\mathfrak{r}\le X^{1/2}}} \frac{aX}{N\mathfrak{r}} e^{-C\frac{(\log X)^{2/3}}{(\log\log X)^{1/5}}}$$

$$\ll Xe^{-C'\frac{(\log X)^{2/3}}{(\log\log X)^{1/5}}}.$$

It remains to estimate

$$\sum_{m\le X} \sum_{\substack{\mathfrak{r} \\ N\mathfrak{r}=\gcd(am,d^\infty)}} \sum_{\substack{\mathfrak{s} \\ N\mathfrak{s}=\frac{|am|}{\gcd(am,d^\infty)} \\ iota(\mathcal{I}^{-1}(\mathfrak{s}))\cap(S_1\cup S_2)\neq 0}} 1.$$

It is enough to bound

$$\sum_{\substack{\mathfrak{a} \\ N\mathfrak{a}\le X \\ \iota(\mathcal{I}^{-1}(\mathfrak{a}))\cap S_i=\emptyset}} 1 = \sum_{\substack{\iota(s)\in S_i \\ NS\le X}} 1$$

for $i = 1, 2$. If $K/\mathbb{Q}$ is imaginary, the angle of S_i is at most ϵ; if $K/\mathbb{Q}$ is real, the hyperbolic angle of S_i is at most ϵ. Since

$$\#\{s \in \iota^{-1}(S) : Ns \le X\}$$

is invariant when S is multiplied by a unit $u \in \mathfrak{O}_K^*$, we can assume without loss of generality that $\log x/y$ is bounded above and below by constants depending only on K. Then the boundary of

$$\{s \in \iota^{-1}(S) : Ns \le X\}$$

has length equal to at most a constant times $\sqrt{X}$. Hence

$$\sum_{\substack{\iota(s)\in S_i \\ NS\leq X}} 1 \ll \epsilon X + \sqrt{X}.$$

Set $\epsilon = \sqrt{B}$. Then

$$\sum_{\substack{x,y\in S\cap L \\ |Q(x,y)|\leq X}} \lambda(Q(x,y)) \ll Xe^{-C''\frac{(\log X)^{2/3}}{(\log\log X)^{1/5}}},$$

as was desired. □

Proposition 3.3.7. *Let $Q(x,y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x,y]$ be a quadratic form. Assume $b^2 - 4ac \neq 0$. Let $L \subset \mathbb{Z}^2$ be a lattice coset, $S \subset \mathbb{R}^2$ a sector. Assume*

$$[\mathbb{Z}^2 : L] \ll (\log X)^A. \tag{3.3.13}$$

Then

$$\sum_{(x,y)\in S\cap L\cap[-N,N]^2} \lambda(Q(x,y)) \ll N^2 e^{-C\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}},$$

where C and the implied constant depend only on a, b, c, A and the implied constant in (3.3.13).

Proof. If Q is reducible, the statement follows immediately from (3.2.14). Assume Q is irreducible. Let $K = \mathbb{Q}(\sqrt{b^2 - 4ac})$.

Suppose $K/\mathbb{Q}$ is imaginary. Then $|Q(x,y)| = 1$ describes an ellipse in $\mathbb{R}^2$ centered at the origin. Let $S \subset \mathbb{R}^2$ be a subquadrant. Write the ellipse in polar coordinates:

$$\theta \in [0, 2\pi],\ r = r_1(\theta),$$

where $r_1 : [0, 2\pi] \to \mathbb{R}^+$ is C^∞. Let

$$c_{10} = \min_{0 \le \theta \le 2\pi} r_1(\theta),\ c_{11} = \max_{0 \le \theta \le 2\pi} |r_1'(\theta)|.$$

Now consider the ellipse

$$\theta \in [0, 2\pi],\ r = \sqrt{X} r_1(\theta).$$

Any arc

$$\theta \in (\theta_1, \theta_2),\ r = \sqrt{X} r_1(\theta)$$

will lie within the region $R_{\theta_1,\theta_2}(\sqrt{X})$ bounded by the two arcs

$$\begin{aligned} &\theta \in (\theta_1, \theta_2),\ r = \sqrt{X}(r_1(\theta_1) - c_{11}(\theta_2 - \theta_1)), \\ &\theta \in (\theta_1, \theta_2),\ r = \sqrt{X}(r_1(\theta_1) + c_{11}(\theta_2 - \theta_1)), \end{aligned} \tag{3.3.14}$$

and the two lines $\theta = \theta_1$, $\theta = \theta_2$. It is easy to show that

$$\#(R_{\theta_1,\theta_2}(\sqrt{X}) \cap \mathbb{Z}^2) \ll c_{11}(\theta_1 - \theta_2)^2 X + (c_{11} + 1)(\theta_2 - \theta_1)\sqrt{X}. \tag{3.3.15}$$

Write the boundary of the square $[-1, 1]^2$ in polar coordinates:

$$\theta \in [0, 2\pi],\ r = r_2(\theta).$$

Let

$$c_{20} = \min_{0 \le \theta \le 2\pi} r_2(\theta),\ c_{21} = \max_{0 \le \theta \le 2\pi} r_2(\theta),\ c_{22} = \max_{0 \le \theta \le 2\pi} |r_2'(\theta)|.$$

For any positive real number N, path

$$\theta \in (\theta_1, \theta_2),\ r = N \cdot r_2(\theta)$$

lies in the region $R'_{\theta_1,\theta_2}(N)$ bounded by the arcs

$$\begin{aligned} &\theta \in (\theta_1, \theta_2),\ r = N(r_2(\theta_1) - c_{21}(\theta_2 - \theta_1)), \\ &\theta \in (\theta_1, \theta_2),\ r = N(r_2(\theta_1) + c_{21}(\theta_2 - \theta_1)) \end{aligned} \tag{3.3.16}$$

and the lines $\theta = \theta_1$, $\theta = \theta_2$. Clearly

$$\#(R_{\theta_1,\theta_2}(N) \cap \mathbb{Z}^2) \ll c_{21}(\theta_2 - \theta_1)^2 N^2 + (c_{21} + 1)(\theta_2 - \theta_1)N. \tag{3.3.17}$$

As can be seem from (3.3.14) and (3.3.16), the region

$$\theta \in (\theta_1, \theta_2), r \leq N r_2(\theta)$$

contains the region

$$\theta \in (\theta_1, \theta_2), r \leq \sqrt{X} r_1(\theta)$$

for

$$X = \left(\frac{N(r_2(\theta_1) - c_{21}(\theta_2 - \theta_1))}{r_1(\theta_1) + c_{11}(\theta_2 - \theta_1)} \right)^2.$$

If $\theta_2 - \theta_1 < \frac{r_{20}}{2c_{21}}$, we have $N^2 \ll X \ll N^2$. By (3.3.15) and (3.3.17), the area between the two regions contains

$$O(c_{11}(\theta_2-\theta_1)^2 X + (c_{11}+1)(\theta_2-\theta_1)\sqrt{X} + c_{21}(\theta_2-\theta_1)^2 N^2 + (c_{21}+1)(\theta_2-\theta_1)N) \tag{3.3.18}$$

points with integral coordinates. We can rewrite (3.3.18) as

$$O((\theta_2 - \theta_1)^2 N^2 + (\theta_2 - \theta_1)N),$$

where the implied constant depends on r_i and c_{ij}. By Lemma 3.3.6,

$$\sum_{\substack{(x,y)\in L\\ \theta_1<\theta(x,y)<\theta_2\\ |Q(x,y)|\le X}} \lambda(Q(x,y)) \ll Xe^{-C\frac{(\log X)^{2/3}}{(\log\log X)^{1/5}}},$$

where $\theta(x,y)$ is the angle $0 \le \theta < 2\pi$ between the x-axis and the vector from $(0,0)$ to (x,y). Hence

$$\sum_{\substack{(x,y)\in L\cap[-N,N]\\ \theta_1<\theta(x,y)<\theta_2}} \lambda(Q(x,y)) \ll N^2 e^{-C\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}} + (\theta_2-\theta_1)^2N^2 + (\theta_2-\theta_1)N. \quad (3.3.19)$$

Let S be a sector. We can assume that S is given by

$$\theta < \theta(x,y) < \theta'$$

for some $\theta, \theta' \in [0, 2\pi]$. Let

$$\theta_0 = \theta,\ \theta_1 = \frac{\theta'-\theta}{n} + \theta,\ \theta_2 = \frac{2(\theta'-\theta)}{n} + \theta,\ \ldots,\ \theta_n = \theta'.$$

Then $\theta_{i+1} - \theta_i = \frac{\theta'-\theta}{n} \le \frac{2\pi}{n}$. Assume $n \ge \frac{4\pi c_{21}}{r_{20}}$. Hence, by (3.3.19),

$$\begin{aligned}\sum_{(x,y)\in S\cap L\cap[-N,N]^2} \lambda(Q(x,y)) &= \sum_{i=0}^{n-1} \sum_{\substack{(x,y)\in L\cap[-N,N]^2\\ \theta_i<\theta(x,y)<\theta_{i+1}}} \lambda(Q(x,y))\\ &\ll ne^{-C\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}}N^2 + \frac{1}{n}N^2 + N.\end{aligned}$$

Choose $n = \min(e^{\frac{C}{2}\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}}, \frac{4\pi c_{21}}{r_{20}})$. Then

$$\sum_{(x,y)\in S\cap L\cap[-N,N]^2} \lambda(Q(x,y)) \ll e^{-\frac{C}{2}\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}}N^2.$$

Now suppose that $K/\mathbb{Q}$ is real. Then $|Q(x,y)| = 1$ describes two hyperbolas sharing two axes going through the origin. We can write the union of the two hyperbolas in polar coordinates:

$$\theta \in D,\ r = r_1(\theta),$$

where $\theta = \theta_a$, $\theta = \theta_b$ are the axes and

$$D = [0, 2\pi] - \{\theta_a, \theta_b, \theta_a + \pi, \theta_b + \pi\}.$$

For $\theta \in [0, 2\pi]$, define

$$d(\theta) = \min(|\theta - \theta_a|, |\theta - \theta_b|, |\theta - (\theta_a + \pi)|, |\theta - (\theta_b + \pi)|).$$

The function $r_1 : D \to \mathbb{R}^+$ has a positive minimum c_{10}. While $r_1(\theta)$ and $r_1'(\theta)$ are unbounded, $r_1(\theta)d(\theta)^{1/2}$ and $r_1'(\theta)d(\theta)^{3/2}$ are bounded; let

$$c_{11} = \max_{\theta} |r_1(\theta)| \cdot d(\theta)^{1/2},\ \ c_{12} = |r_1'(\theta)| \cdot d(\theta)^{3/2}.$$

We can define r_2, c_{20}, c_{21} and c_{22} as before. Let $(\theta_1, \theta_2) \in D$. The region

$$\theta \in (\theta_1, \theta_2),\ r \leq N r_2(\theta) \tag{3.3.20}$$

contains the region

$$\theta \in (\theta_1, \theta_2),\ r \leq \sqrt{X} r_2(\theta) \tag{3.3.21}$$

for

$$X = \left(\frac{N(r_2(\theta_1) - c_2(\theta_2 - \theta_1))}{r_1(\theta_1) + c_{11} \frac{\theta_2 - \theta_1}{\min(d(\theta_1), d(\theta_2))^{3/2}}} \right)^2.$$

Assume

$$\theta_2 - \theta_1 < \min\left(\frac{r_{20}}{2c_{21}}, d(\theta_1), d(\theta_2)\right), \quad \min(d(\theta_1), d(\theta_2)) \ll N^{-\epsilon}.$$

Then

$$N^{2-3\epsilon} \ll X \ll N^2. \tag{3.3.22}$$

It follows that the area between (3.3.20) and (3.3.21) contains

$$O((\theta_2 - \theta_1)^2 N^2 / \min(d(\theta_1), d(\theta_2))^2 + (\theta_2 - \theta_1) N / \min(d(\theta_1), d(\theta_2))^{3/2}.$$

By Lemma 3.3.6 and (3.3.22) we get

$$\sum_{\substack{(x,y)\in L \\ \theta_1 < \theta(x,y) < \theta_2 \\ |Q(x,y)| \le X}} \lambda(Q(x,y)) \ll N^2 e^{-C\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}}.$$

As in the case of $K/\mathbb{Q}$ imaginary, we can divide any sector S into slices (θ_1, θ_2) with

$$\theta_2 - \theta_1 \sim e^{-\frac{C}{2}\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}}.$$

We leave out angles of size

$$e^{-\frac{C}{4}\frac{(\log N)^{2/3}}{(\log\log N)^{1/5}}}$$

around θ_a, θ_b, $\theta_a + \pi$ and $\theta_b + \pi$. The statement follows. $\square$

3.4 The average of λ on the product of three linear factors

Lemma 3.4.1. *For any $M_2 > M_1 > 1$, there are $\sigma_d \in \mathbb{R}$ with $|\sigma_d| \leq 1$ and support on*

$$\{M_1 \leq d < M_2 : p < M_1 \Rightarrow p \nmid d\}$$

such that

$$\sum_{(x,y)\in S\cap L} g(x)f(x,y) = \sum_{a}\sum_{b}\sum_{\substack{c\\(ab,c)\in S\cap L}} \sigma_a\, g(a)g(b)f(ab,c) + O\left(\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + NM_2\right)$$

for any positive integer $N > M_2$, any convex set $S \subset [-N,N]^{\deg(K/\mathbb{Q})}$, any lattice coset $L \subset \mathbb{Z}^{\deg(K/\mathbb{Q})}$ with index $[\mathbb{Z}^2 : L] < M_1$, any function $f : \mathbb{Z}^2 \to \mathbb{C}$ and any completely multiplicative function $g : \mathbb{Z}^2 \to \mathbb{C}$ with

$$\max_{x,y} |f(x,y)| \leq 1, \quad \max_{y} |g(y)| \leq 1.$$

The implied constant is absolute.

Proof. Let $y_1 = \min(\{y \in \mathbb{Z} : \exists x\, s.t.\, (x,y) \in S\cap L\})$. There is an $l|[\mathbb{Z}^2 : L]$ such that, for any $y \in \mathbb{Z}$,

$$(\exists x\, s.t.\, (x,y) \in L) \Leftrightarrow (l|y - y_1).$$

Let

$$N_{j,0} = \min(\{x : (x, y_1 + jl) \in S\cap L\})$$

$$N_{j,1} = \max(\{x : (x, y_1 + jl) \in S\cap L\}) + 1.$$

Now take σ_d as in Lemma 3.2.9. If $N_{j,1} - N_{j,0} > M_2$, then

$$\sum_{x:(x,y_1+jl)\in S\cap L} \left|1 - \sum_{d|x}\sigma_d\right| \ll \frac{\log M_1}{\log M_2}\frac{N_{j,1} - N_{j,0}}{[\mathbb{Z}^2 : L]/l}$$

Summing this over all j we obtain

$$\sum_{(x,y)\in S\cap L}\left|1-\sum_{d|x}\sigma_d\right| \ll \frac{\log M_1}{\log M_2}\frac{(\mathrm{Area}(S))/l}{[\mathbb{Z}^2:L]}M_2N$$
$$\ll \frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+M_2N.$$

Since

$$\left|\sum_{(x,y)\in S\cap L} g(y)f(x,y)-\sum_{(x,y)\in S\cap L}\sum_{d|x}\sigma_d g(x)f(x,y)\right|$$

is at most

$$\sum_{(x,y)\in S\cap L}\left|g(y)f(x,y)-\sum_{d|x}\sigma_d g(y)f(x,y)\right| \le \sum_{(x,y)\in S\cap L}\left|1-\sum_{d|x}\sigma_d\right|$$

and

$$\sum_{\substack{a\\(ab,c)\in S\cap L}}\sum_{b}\sum_{c}\sigma_a\, g(a)g(b)f(ab,c)=\sum_{(x,y)\in S\cap L}\sum_{d|x}\sigma_d g(x)f(x,y).$$

we are done. □

Lemma 3.4.2. *Let c_1, c_2 be integers. Let $L\subset\mathbb{Z}^2$ be a lattice. Then the set $\{(a,b)\in\mathbb{Z}^2:(a,bc_1),(a,bc_2)\in L\}$ is either the empty set or a lattice coset $L'\subset\mathbb{Z}^2$ of index dividing $[\mathbb{Z}^2:L]^2$.*

Proof. The set of all elements of L of the form (a,bc_1) is the intersection of a lattice coset of index $[\mathbb{Z}^2:L]$ and a lattice of index c_1. By (3.2.12) it is either the empty set or a lattice coset of index dividing $c_1[\mathbb{Z}^2:L]$. Therefore the set of all (a,b) such that (a,bc_1) is in L is either the empty set or a lattice coset L_1 of index dividing $\frac{1}{c_1}c_1[\mathbb{Z}^2:L]=[\mathbb{Z}^2:L]$. Similarly, the set of all (a,b) such that $(a,bc_2)\in L$ is either the empty set or a lattice coset L_2 of index dividing $[\mathbb{Z}^2:L]$. Therefore $L'=L_1\cap L_2$ is either the empty set or a lattice coset of index dividing $[\mathbb{Z}^2:L]^2$. □

Definition 7. *For* $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$ *we denote*

$$A_{12} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad A_{13} = \begin{pmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{pmatrix} \quad A_{23} = \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Proposition 3.4.3. *Let* S *be a convex subset of* $[-N, N]^2$, $N > 1$. *Let* $L \subset \mathbb{Z}^2$ *be a lattice coset. Let* a_{11}, a_{12}, a_{21}, a_{22}, a_{31}, a_{32} *be rational integers. Then*

$$\sum_{(x,y)\in S\cap L} \lambda((a_{11}x + a_{12}y)(a_{21}x + a_{22}y)(a_{31}x + a_{32}y)) \ll \frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + \frac{N^2}{(\log N)^\alpha}$$

for any $\alpha > 0$. *The implied constant depends only on* (a_{ij}) *and* α.

Proof. We can assume that A_{12} is non-singular, as otherwise the statement follows immediately from Lemma 3.2.5. Changing variables we obtain

$$\begin{aligned} \sum_{\substack{(x,y)\in S\cap L \\ \gcd(a_{11}x+a_{12}y, a_{21}x+a_{22}y)=1}} & \lambda(a_{11}x + a_{12}y)\lambda(a_{21}x + a_{22}y)\lambda(a_{31}x + a_{32}y) \\ &= \sum_{\substack{(x,y)\in A_{12}S\cap A_{12}L \\ \gcd(x,y)=1}} \lambda(x)\lambda(y)\lambda\left((a_{31}\, a_{32})A_{12}^{-1}\begin{pmatrix} x \\ y \end{pmatrix}\right) \\ &= \sum_{\substack{(x,y)\in A_{12}S\cap A_{12}L \\ \gcd(x,y)=1}} \lambda(x)\lambda(y)\lambda(q_1x + q_2y), \end{aligned}$$

where $q_1 = -\frac{\det(A_{23})}{\det(A_{12})}$ and $q_2 = \frac{\det(A_{13})}{\det(A_{12})}$. Note that $q_1x + q_2y$ is an integer for all (x, y) in $A_{12}L$. We can assume that neither q_1 nor q_2 is zero. Write $S' = A_{12}S$, $L' = A_{12}L$. Clearly $S' \subset [-N', N']^2$ for $N' = \max(|a_{11}| + |a_{12}|, |a_{21}| + |a_{22}|)N$.

Now set

$$M_1 = (\log N')^{2\alpha+2},\ M_2 = \frac{(N')^{1/2}}{(\log N')^{\alpha}}.$$

Clearly $M_2 > M_1$ for $N > N_0$, N_0 depending only on (a_{ij}) and α.

By Lemma 3.4.1,

$$\sum_{(x,y)\in S'\cap L'} \lambda(x)\lambda(y)\lambda(q_1x+q_2y) = \sum_{\substack{a\\(ab,c)\in S'\cap L'}}\sum_{b}\sum_{c} \sigma_a\,\lambda(a)\lambda(b)\lambda(c)\lambda(q_1ab+q_2c)$$
$$+ O\left(\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S')}{[\mathbb{Z}^2:L']} + N'M_2\right).$$

We need to split the domain:

$$\sum_{\substack{a\\(ab,c)\in S'\cap L'}}\sum_{b}\sum_{c} \sigma_a\,\lambda(a)\lambda(b)\lambda(c)\lambda(q_1ab+q_2c) = \sum_{s=1}^{\lceil M_2/M_1\rceil} T_s,$$

where

$$T_s = \sum_{a=sM_1}^{(s+1)M_1-1}\ \sum_{\substack{|b|\le N'/sM_1\\(ab,c)\in S'\cap L'}}\ \sum_{c} \sigma_a\,\lambda(a)\lambda(b)\lambda(c)\lambda(q_1ab+q_2c).$$

By Cauchy's inequality,

$$T_s^2 \le \frac{(N')^2}{sM_1}\sum_{c}\ \sum_{|b|\le N'/sM_1}\left(\sum_{\substack{sM_1\le a<(s+1)M_1\\(ab,c)\in S'\cap L'}} \sigma_a\lambda(a)\lambda(q_1ab+q_2c)\right)^2.$$

Expanding the square and changing the order of summation, we get

$$\frac{(N')^2}{sM_1}\sum_{a_1=sM_1}^{(s+1)M_1-1}\ \sum_{a_2=sM_1}^{(s+1)M_1-1} \sigma_{a_1}\sigma_{a_2}\lambda(a_1)\lambda(a_2)\sum_{\substack{c\\(a_ib,c)\in S'\cap L'}}\ \sum_{|b|\le N'/sM_1} \lambda(q_1a_1b+q_2c)\lambda(q_1a_2b+q_2c).$$

There are at most $M_1\cdot 2N'\frac{N'}{sM_1}$ terms with $c_1=c_2$. They contribute at most $\frac{2(N')^4}{s^2M_1}$ to T_s^2, and thus no more than $((N')^2/\sqrt{M_1})\log M_2$ to the sum $\sum_{s=1}^{\lceil M_2/M_1\rceil} T_s$. It remains

to bound

$$\sum_{\substack{a_1=sM_1 \\ a_1\neq a_2}}^{(s+1)M_1-1} \sum_{a_2=sM_1}^{(s+1)M_1-1} \sigma_{a_1}\sigma_{a_2}\lambda(a_1)\lambda(a_2) \sum_{\substack{c \\ (a_ib,c)\in S'\cap L'}} \sum_{|b|\leq N'/sM_1} \lambda(q_1a_1b+q_2c)\lambda(q_1a_2b+q_2c).$$

Since $|\sigma_a| \leq 1$ for all a, the absolute value of this is at most

$$\sum_{\substack{a_1=sM_1 \\ a_1\neq a_2}}^{(s+1)M_1-1} \sum_{a_2=sM_1}^{(s+1)M_1-1} \left| \sum_{\substack{c \\ (a_ib,c)\in S'\cap L'}} \sum_{b} \lambda(q_1a_1b+q_2c)\lambda(q_1a_2b+q_2c) \right|.$$

By Lemma 3.4.2 we can write $\{(b,c) \in \mathbb{Z}^2 : (a_1b,c),(a_2b,c) \in S' \cap L'\}$ as $S'' \cap L''$ with S'' a convex subset of $[-N'/\max(a_1,a_2), N'/\max(a_1,a_2)] \times [-N', N']$ and $L'' \subset \mathbb{Z}^2$ a lattice coset of index dividing $[\mathbb{Z}^2 : L']^2$. Hence we have the sum

$$\sum_{\substack{a_1=sM_1 \\ a_1\neq a_2}}^{(s+1)M_1-1} \sum_{a_2=sM_1}^{(s+1)M_1-1} \left| \sum_{(b,c)\in S''\cap L''} \lambda(q_1a_1b+q_2c)\lambda(q_1a_2b+q_2c) \right|.$$

Set $S_{a_1,a_2} = \begin{pmatrix} q_1a_1 & q_2 \\ q_1a_2 & q_2 \end{pmatrix} S''$, $L_{a_1,a_2} = \begin{pmatrix} q_1a_1 & q_2 \\ q_1a_2 & q_2 \end{pmatrix} L''$, $N'' = (|q_1|+|q_2|)N'$. Clearly S_{a_1,a_2} is a convex subset of $[-N'', N'']^2$ with

$$\text{Area}(S_{a_1,a_2}) = |q_1q_2(a_1-a_2)|\,\text{Area}(S'') \leq |q_1q_2|M_1\frac{4(N')^2}{sM_1} \ll \frac{N^2}{s},$$

whereas $L_{a_1,a_2} \subset \mathbb{Z}^2$ is a lattice coset of index $|q_1q_2(a_1-a_2)|[L'' : \mathbb{Z}^2]$. (That L_{a_1,a_2} is inside $\mathbb{Z}^2$ follows from our earlier remark that q_1x+q_2y is an integer for all (x,y) in $A_{12}L'$.) Now we have

$$\sum_{\substack{a_1=sM_1 \\ a_1\neq a_2}}^{(s+1)M_1-1} \sum_{a_2=sM_1}^{(s+1)M_1-1} \left| \sum_{(v,w)\in S_{a_1,a_2}\cap L_{a_1,a_2}} \lambda(v)\lambda(w) \right|.$$

This is at most

$$M_1^2 \max_{sM_1 \le a < (s+1)M_1} \max_{\substack{-M_1 \le d \le M_1 \\ d \ne 0}} \left| \sum_{(v,w) \in S_{a,a+d} \cap L_{a,a+d}} \lambda(v)\lambda(w) \right|.$$

We can assume that $[\mathbb{Z}^2 : L] < (\log N)^\alpha$, as otherwise the bound we are attempting to prove is trivial. Hence $[\mathbb{Z}^2 : L''] \ll (\log N)^{2\alpha}$. By Lemma 3.2.5,

$$\left| \sum_{(v,w) \in S_{a,a+d} \cap L_{a,a+d}} \lambda(v)\lambda(w) \right| \ll \frac{N^2}{s} \cdot e^{-C(\log N'')^{3/5}/(\log\log N'')^{1/5}} + N^{1+1/3}.$$

It is time to collect all terms. The total is at most a constant times

$$\begin{aligned} \frac{\log M_1}{\log M_2} \frac{\mathrm{Area}(S')}{[\mathbb{Z}^2 : L']} + N' M_2^2 + \frac{(N')^2}{\sqrt{M_1}} \log M_2 \\ + (N')^2 \sqrt{M_1} \log M_2 \cdot e^{-C(\log N'')^{3/5}/(\log\log N'')^{1/5}} \\ + N^{5/3} \sqrt{M_2}, \end{aligned}$$

where the constant depends only on (a_{ij}) and α. Simplifying we obtain

$$O\left(\frac{\log\log N}{\log N} \frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + \frac{N^2}{(\log N)^\alpha} \right).$$

□

3.5 The average of λ on the product of a linear and a quadratic factor

We will be working with quadratic extensions $K/\mathbb{Q}$. It will be convenient to use embeddings $\jmath : K \to \mathbb{R}^2$ as in Lemma 3.2.10 instead of embeddings $\iota : K \to \mathbb{R}^2$ of the kind employed in section 3.3. (In Lemma 3.2.10, $\jmath : K \to \mathbb{R}^2$ takes $\mathfrak{O}_K$ to $\mathbb{Z}^2$,

whereas $\iota : K \to \mathbb{R}^2$ does not.) We define

$$\jmath(x + y\sqrt{d}) = (x, y) \text{ if } d \equiv 1 \bmod 4,$$
$$\jmath(x + y\sqrt{d}) = (x - y, 2y) \text{ if } d \not\equiv 1 \bmod 4,$$

where $x, y \in \mathbb{Q}$.

For every $z \in \jmath^{-1}([-N, N]^2)$,

$$|N_{K/\mathbb{Q}} z| \ll N^2, \tag{3.5.1}$$

where the implied constant depends only on K. In general there is no implication in the opposite sense, as the norm need not be positive definite. For $K = \mathbb{Q}(\sqrt{d})$, $d < 0$,

$$\#\{z \in \mathfrak{O}_K : N_{K/\mathbb{Q}}(z) \leq A\} \ll A. \tag{3.5.2}$$

For $K = \mathbb{Q}(\sqrt{d})$, $d > 1$, $A \leq N^2$,

$$\#\{z \in \jmath^{-1}([-N, N]^2) : N_{K/\mathbb{Q}}(z) \leq A\} \ll A\left(1 + \log \frac{N}{\sqrt{A}}\right) + N. \tag{3.5.3}$$

In either case the implied constant depends only on d.

Lemma 3.5.1. *Let $\mathfrak{a}$ be an ideal in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ divisible by no rational integer $n > 1$. Then for any positive N, $y_0 \in [-N, N]$,*

$$\#\{(x, y_0) \in [-N, N]^2 : \jmath^{-1}(x, y_0) \in \mathfrak{a}\} \leq \lceil N/N_{K/\mathbb{Q}}(\mathfrak{a}) \rceil.$$

Proof. For every rational integer $r \in \mathfrak{a}$, $N\mathfrak{a} | r$. Hence

$$\{x : \jmath^{-1}(x, y_0) \in \mathfrak{a}\}$$

is an arithmetic progression of modulus $N\mathfrak{a}$. $\square$

Proposition 3.5.2. *Let S be a convex subset of $[-N,N]^2$, $N>1$. Let $L\subset\mathbb{Z}^2$ be a lattice coset. Let a_1, a_2, a_3, a_4, a_5 be rational integers such that $a_1x^2+a_2xy+a_3y^2$ is irreducible. Then*

$$\sum_{(x,y)\in S\cap L}\lambda((a_1x^2+a_2xy+a_3y^2)(a_4x+a_5y))\ll\frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]}+\frac{N^2}{(\log N)^\alpha}$$

for any $\alpha>0$. The implied constant depends only on (a_{ij}) and α.

Proof. Write d for $a_1^2-4a_0a_2$, $K/\mathbb{Q}$ for $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, $\mathfrak{N}x$ for $N_{K/\mathbb{Q}}x$ and $\overline{r+s\sqrt{d}}$ for $r-s\sqrt{d}$. By Lemma 3.2.1 there are $\alpha_1,\alpha_2\in\mathfrak{O}_K$ linearly independent over $\mathbb{Q}$ and a non-zero rational number k such that

$$a_1x^2+a_2xy+a_3y^2=k\mathfrak{N}(x\alpha_1+y\alpha_2)=k(x\alpha_1+y\alpha_2)\overline{(x\alpha_1+y\alpha_2)}.$$

Hence

$$\sum_{(x,y)\in S\cap L}\lambda((a_1x^2+a_2xy+a_3y^2)(a_4x+a_5y))$$

equals

$$\lambda(k)\sum_{(x,y)\in S\cap L}\lambda((x\alpha_1+y\alpha_2)\overline{(x\alpha_1+y\alpha_2)}(a_4x+a_5y)).$$

By abuse of language we write $\Re(r+s\sqrt{d})$ for r, $\Im(r+s\sqrt{d})$ for s. Let $C=\begin{pmatrix}\Re\alpha_1 & \Re\alpha_2\\ \Im\alpha_1 & \Im\alpha_2\end{pmatrix}^{-1}$. Then $a_4x+a_5y=qz+\overline{qz}$ for $z=x\alpha_1+y\alpha_2$,

$$q=\frac{1}{2}(a_4c_{11}+a_5c_{21}+\frac{1}{\sqrt{d}}(a_4c_{12}+a_5c_{22})).$$

Define $\phi_Q:\mathbb{Z}^2\to\mathfrak{O}_K$ to be the mapping $(x,y)\mapsto(x\alpha_1+y\alpha_2)$. Let $L'=(\iota\circ\phi_Q)(L)$.

Let S' be the sector of $\mathbb{R}^2$ such that $(\iota \circ \phi)(S \cap \mathbb{Q}^2) = S' \cap \mathbb{Q}^2$. Then

$$\sum_{(x,y)\in S\cap L} \lambda((x\alpha_1 + y\alpha_2)\overline{(x\alpha_1 + y\alpha_2)}(a_4 x + a_5 y)) = \sum_{\jmath(z)\in S'\cap L'} \lambda(z\overline{z}(qz + \overline{qz})).$$

Note that $qz + \overline{qz}$ is an integer for all $z \in L'$.

Let N' be the smallest integer greater than one such that $j(S') \subset [-N', N']^2$. (Note that $N' \leq c_1 N$, where c_1 is a constant depending only on $\mathbb{Q}$.) Suppose $K/\mathbb{Q}$ is real. Then, by (3.5.3),

$$\begin{aligned}\#\{x \in \jmath^{-1}(S') : \mathfrak{N}x \leq \frac{(N')^2}{(\log N)^{\alpha+1}}\} &\leq \frac{(N')^2}{(\log N')^{\alpha+1}}(1 + \log(\log N')^{\alpha+1}) + N \\ &\leq \frac{N^2}{(\log N)^{\alpha}}.\end{aligned}$$

The set

$$\{x \in [-N, N]^2 : \mathfrak{N}(\jmath^{-1}(x)) > \frac{(N')^2}{(\log N)^{\alpha+1}}\}$$

is the region within a square and outside two hyperbolas. As such it is the disjoint union of at most four convex sets. Hence the set

$$S'' = S \cap \{x \in [-N, N]^2 : \mathfrak{N}(\jmath^{-1}(x)) > (N')^2/(\log N)^{\alpha+1}\}$$

is the disjoint union of at most four convex sets:

$$S'' = S_1 \cup S_2 \cup S_3 \cup S_4.$$

In the following, S^* will be S_1, S_2, S_3 or S_4, and as such a convex set contained in S''.

Suppose now that $K/\mathbb{Q}$ is imaginary. Then the set

$$\{x \in [-N, N]^2 : \mathfrak{N}(\jmath^{-1}(x)) > (N')^2/(\log N)^{\alpha+1}\}$$

is the region within a square and outside the circle given by

$$\{x : \mathfrak{N}(\jmath^{-1}(x)) = (N')^2/(\log N)^{\alpha+1}\}. \tag{3.5.4}$$

We can circumscribe about (3.5.4) a rhombus containing no more than

$$O((N')^2/(\log N)^{\alpha+1})$$

integer points, where the implied constant depends only on Q. We then quarter the region inside the square $[-N, N]$ and outside the rhombus, obtaining four convex sets V_1, V_2, V_3, V_4 inside S. We let S^* be $S \cap V_1$, $S \cap V_2$, $S \cap V_3$ or $S \cap V_4$.

For K either real or imaginary, we now have a convex set $S^* \subset [-N, N]$ such that, for any $\jmath \in \mathfrak{O}_K$,

$$\jmath(z) \in S^* \Rightarrow \mathfrak{N}z > N^2/(\log N)^\alpha.$$

Our task is to bound

$$\sum_{\substack{z \in \mathfrak{O}_K \\ \jmath(z) \in S^* \cap L'}} \lambda(z\overline{z}(qz + \overline{qz})).$$

Set

$$M_1 = (\log N)^{20(\alpha+1)}, \quad M_2 = \frac{N^{1/2}}{4d\,\mathrm{num}(\mathfrak{N}q)[\mathfrak{O}_K : L']^2(\log N)^{16\alpha+22}}.$$

By Lemma 3.2.10,

$$\begin{aligned}\sum_{\substack{z \in \mathfrak{O}_K \\ \jmath(z) \in S^* \cap L'}} \lambda(z\overline{z}(qz + \overline{qz})) = &\sum_{z \in S'' \cap L'} \sum_{\substack{\mathfrak{d} \\ z \in \mathfrak{d}}} \sigma_{\mathfrak{d}} \lambda(z\overline{z}(qz + \overline{qz})) \\ &+ O\left(\frac{\log M_1}{\log M_2} \frac{\mathrm{Area}(S')}{[\mathfrak{O}_K : L']}\right) + N'M_2.\end{aligned} \tag{3.5.5}$$

Let $N'' = (9/4 + |d|)(N')^2$. Then $\jmath(z) \in [-N', N']$ implies $|\mathfrak{N}z| \leq N''$. Since $\sigma_{\mathfrak{d}} = 0$

when $N\mathfrak{d} < M_1$, the first term on the right of (3.5.5) equals

$$\sum_{\substack{\mathfrak{b} \\ \mathfrak{N}\mathfrak{b} \le N''/M_1}} \lambda(\mathfrak{b}\overline{\mathfrak{b}}) \sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}} \lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ z \in S'' \cap L'}} \lambda(qz + \overline{qz}).$$

We need to split the domain:

$$\sum_{\substack{\mathfrak{b} \\ \mathfrak{N}\mathfrak{b} \le N''/M_1}} \lambda(\mathfrak{b}\overline{\mathfrak{b}}) \sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}} \lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ \jmath(z) \in S^* \cap L'}} \lambda(qz + \overline{qz}) = \sum_{s=1}^{\lceil \log_2(N''/M_1) \rceil} T_s,$$

where

$$T_s = \sum_{\substack{\mathfrak{b} \\ 2^{s-1} \le \mathfrak{N}\mathfrak{b} \le 2^s}} \lambda(\mathfrak{b}\overline{\mathfrak{b}}) \sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}} \lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ \jmath(z) \in S^* \cap L'}} \lambda(qz + \overline{qz}).$$

Notice that $\lambda(\mathfrak{b}\overline{\mathfrak{b}})$, $\sigma_{\mathfrak{a}}$, $\lambda(\mathfrak{a}\overline{\mathfrak{a}})$ and $\lambda(qz + \overline{qz})$ are all real. By Cauchy's inequality,

$$\begin{aligned} T_s^2 &\le 2^{s-1} \sum_{\substack{\mathfrak{b} \\ 2^{s-1} \le \mathfrak{N}\mathfrak{b} \le 2^s}} \left(\sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal}}} \sigma_{\mathfrak{a}} \lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ \jmath(z) \in S^* \cap L'}} \lambda(qz + \overline{qz}) \right)^2 \\ &\le 2^{s-1} \sum_{\mathfrak{b}} \left(\sum_{\substack{\mathfrak{a} \\ \mathfrak{a}\mathfrak{b} \text{ principal} \\ n_{s0} < \mathfrak{N}\mathfrak{a} \le n_{s1}}} \sigma_{\mathfrak{a}} \lambda(\mathfrak{a}\overline{\mathfrak{a}}) \sum_{\substack{(z)=\mathfrak{a}\mathfrak{b} \\ \jmath(z) \in S^* \cap L'}} \lambda(qz + \overline{qz}) \right)^2, \end{aligned}$$

where $n_{s0} = \frac{(N')^2}{2^s (\log N)^{\alpha+1}}$ and $n_{s1} = \min(\frac{N''}{2^{s-1}}, M_2)$. Expanding the square and changing the order of summation, we get

$$\begin{aligned} 2^{s-1} \sum_{\substack{\mathfrak{a}_1 \\ n_{s0} < \mathfrak{N}\mathfrak{a}_1 \le n_{s1}}} \sum_{\substack{\mathfrak{a}_2 \\ n_{s0} < \mathfrak{N}\mathfrak{a}_2 \le n_{s1}}} & \sigma_{\mathfrak{a}_1} \sigma_{\mathfrak{a}_2} \lambda(\mathfrak{a}_1 \overline{\mathfrak{a}_1}) \lambda(\mathfrak{a}_2 \overline{\mathfrak{a}_2}) \\ & \sum_{\substack{\mathfrak{b} \\ \mathfrak{a}_1\mathfrak{b},\, \mathfrak{a}_2\mathfrak{b} \text{ principal}}} \sum_{\substack{(z_1)=\mathfrak{a}_1\mathfrak{b} \\ \jmath(z_1) \in S^* \cap L'}} \sum_{\substack{(z_2)=\mathfrak{a}_2\mathfrak{b} \\ \jmath(z_2) \in S^* \cap L'}} \lambda(qz_1 + \overline{qz_1}) \lambda(qz_2 + \overline{qz_2}). \end{aligned}$$

Write $\mathcal{S}(x+y\sqrt{d})$ for $\max(|x|,|y|)$. Let $r=(z_2/z_1)\cdot\mathfrak{N}\mathfrak{a}$. We have $r\in\overline{\mathfrak{a}_1}$ because

$$(r)=((z_2)/(z_1))\cdot\mathfrak{N}\mathfrak{a}_1=(\mathfrak{a}_2/\mathfrak{a}_1)\cdot\mathfrak{N}\mathfrak{a}_1=\mathfrak{a}_2\cdot\overline{\mathfrak{a}_1}.$$

Since $\mathfrak{N}z_1>\frac{(N')^2}{(\log N)^{\alpha+1}}$ and $\mathcal{S}(z_2\overline{z_1})\ll(N')^2$, where the implied constant depends only on $\mathbb{Q}$,

$$\mathcal{S}(r)=\mathcal{S}\left(\frac{z_2}{z_1}\mathfrak{N}\mathfrak{a}_1\right)=\mathcal{S}\left(\frac{z_2\overline{z_1}}{\mathfrak{N}z_1}\mathfrak{N}\mathfrak{a}_1\right)=\mathcal{S}(z_2\overline{z_1})\frac{\mathfrak{N}\mathfrak{a}}{\mathfrak{N}z_1}\ll n_{s1}(\log N)^{\alpha+1}. \tag{3.5.6}$$

Set

$$R_s=\jmath^{-1}\left(\left[-kn_{s1}(\log N)^{\alpha+1},kn_{s1}(\log N)^{\alpha+1}\right]^2\right),$$

where k is the implied constant in (3.5.6) and as such depends only on K. Changing variables we obtain

$$2^{s-1}\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}_1\le n_{s1}}}\sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s\\ n_{s0}<\mathfrak{N}\left(\frac{(r)}{\mathfrak{a}}\right)\le n_{s1}}}\sigma_{\mathfrak{a}}\sigma_{(r)/\mathfrak{a}}\lambda(\mathfrak{a}\overline{\mathfrak{a}})\lambda\left(\frac{(r)}{\mathfrak{a}}\frac{\overline{(r)}}{\mathfrak{a}}\right)$$
$$\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L'\\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}}\lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{N\mathfrak{a}}+\frac{\overline{qrz}}{N\mathfrak{a}}\right),$$

that is, 2^{s-1} times

$$\sum_{\substack{\mathfrak{a}\\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1}}}\sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s\\ n_{s0}<\mathfrak{N}\left(\frac{(r)}{\mathfrak{a}}\right)\le n_{s1}}}\sigma_{\mathfrak{a}}\sigma_{(r)/\mathfrak{a}}\lambda(r\overline{r})\sum_{\substack{z\\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L'\\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S^*\cap L'}}\lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{\mathfrak{N}\mathfrak{a}}+\frac{\overline{qrz}}{\mathfrak{N}\mathfrak{a}}\right). \tag{3.5.7}$$

For any non-zero rational integer n,

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1} \\ n|\mathfrak{a}}} \sum_{r\in\overline{\mathfrak{a}}\cap R_s} \sum_{\substack{\jmath(z)\in\mathfrak{a}\cap S^* \\ 2^{s-1}\le\mathfrak{N}((z)/\mathfrak{a})<2^s}} 1 \ll \sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1} \\ n|\mathfrak{a}}} \frac{(2kn_{s1}(\log N)^{\alpha+1})^2}{\mathfrak{N}\mathfrak{a}} 2^s \log 2^s$$
$$\ll \frac{1}{n^2}\frac{N^4(\log N)^{2\alpha+5}}{2^s}.$$

Since the support of $\sigma_{\mathfrak{d}}$ is a subset of

$$\{\mathfrak{d} : M_1 \le \mathfrak{N}\mathfrak{d} < M_2, \mathfrak{N}\mathfrak{p} < M_1 \Rightarrow \mathfrak{N}\mathfrak{p} \nmid \mathfrak{d}\},$$

we have that $n|\mathfrak{a}$ and $\sigma_{\mathfrak{a}} \neq 0$ imply $n \ge \sqrt{M_1}$. Therefore (3.5.7) equals

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1} \\ n>1\Rightarrow n\nmid\mathfrak{a}}} \sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s \\ n_{s0}<\mathfrak{N}\left(\frac{(r)}{\mathfrak{a}}\right)\le n_{s1}}} \sigma_{\mathfrak{a}}\sigma_{(r)/\mathfrak{a}}\lambda(r\overline{r}) \sum_{\substack{z \\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L' \\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S''\cap L'}} \lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{N\mathfrak{a}}+\frac{\overline{qrz}}{N\mathfrak{a}}\right) \quad (3.5.8)$$

plus $O(N^4(\log N)^{2\alpha+5}/(2^s\sqrt{M_1}))$. The absolute value of (3.5.8) is at most

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1} \\ n>1\Rightarrow n\nmid\mathfrak{a}}} \sum_{r\in\overline{\mathfrak{a}}\cap R_s} \left| \sum_{\substack{z \\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L' \\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S''\cap L'}} \lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{N\mathfrak{a}}+\frac{\overline{qrz}}{N\mathfrak{a}}\right)\right|. \quad (3.5.9)$$

By Lemma 3.5.1,

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1}}} \sum_{r\in\overline{\mathfrak{a}}\cap R_s\cap\mathbb{Z}} \sum_{z\in\mathfrak{a}\cap S^*} 1 \ll \sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\le n_{s1}}} \left(\frac{N'}{\mathfrak{N}\mathfrak{a}}+1\right)\left(\frac{(N')^2}{\mathfrak{N}\mathfrak{a}}+N'\right)$$
$$\ll \frac{N^3\log M_1}{n_{s0}} + Nn_{s1}.$$

Thus we are left with

$$\sum_{\substack{\mathfrak{a} \\ n_{s0}<\mathfrak{N}\mathfrak{a}\leq n_{s1} \\ n>1\Rightarrow n\nmid\mathfrak{a}}} \sum_{\substack{r\in\overline{\mathfrak{a}}\cap R_s \\ \Im r\neq 0}} \left| \sum_{\substack{z \\ \jmath(z)\in\jmath(\mathfrak{a})\cap S^*\cap L' \\ \jmath(rz/\mathfrak{N}\mathfrak{a})\in S''\cap L'}} \lambda(qz+\overline{qz})\lambda\left(\frac{qrz}{N\mathfrak{a}}+\frac{\overline{qrz}}{N\mathfrak{a}}\right)\right|. \tag{3.5.10}$$

Notice that $r \in \overline{\mathfrak{a}}$ and $z \in \mathfrak{a}$ imply $(rz/\mathfrak{N}\mathfrak{a}) \in \mathfrak{O}_K$. Hence $(r/\mathfrak{N}\mathfrak{a})^{-1}\mathfrak{O}_K \supset \mathfrak{a}$. Therefore $(r/\mathfrak{N}\mathfrak{a})^{-1}\jmath^{-1}(L') \cap \mathfrak{a}$ is either the empty set or a sublattice of $\mathfrak{a}$ of index dividing $[\mathfrak{O}_K : L']$. This means that

$$L_{\mathfrak{a},r} = \{z \in \mathfrak{a} \cap \jmath^{-1}(L') : (rz/\mathfrak{N}\mathfrak{a}) \in \jmath^{-1}(L')\}$$

is either the empty set or a sublattice of $\mathfrak{a}$ of index $[\mathfrak{a} : L_{\mathfrak{a},r}]$ dividing $[\mathfrak{O}_K : L']^2$, whereas

$$S_{\mathfrak{a},r} = \{z \in S^* : (rz/\mathfrak{N}\mathfrak{a}) \in S''\}$$

is a convex subset of $[-N', N']^2$. The map

$$\kappa : (x,y) \mapsto (q\cdot\phi_Q(x,y) + \overline{q\cdot\phi_Q(x,y)}, \frac{qr\cdot\phi_Q(x,y)}{\mathfrak{N}\mathfrak{a}} + \frac{\overline{qr\cdot\phi_Q(x,y)}}{\mathfrak{N}\mathfrak{a}})$$

is given by the matrix

$$\begin{pmatrix} 2 & 0 \\ 2\frac{\Re r}{\mathfrak{N}\mathfrak{a}} & 2d\frac{\Im r}{\mathfrak{N}\mathfrak{a}} \end{pmatrix} \cdot \begin{pmatrix} \Re q & d\,\Im q \\ \Im q & \Re q \end{pmatrix} \quad \text{if } d \not\equiv 1 \bmod 4,$$

$$\begin{pmatrix} 2 & 0 \\ 2\frac{\Re r}{\mathfrak{N}\mathfrak{a}} & 2d\frac{\Im r}{\mathfrak{N}\mathfrak{a}} \end{pmatrix} \cdot \begin{pmatrix} \Re q & d\,\Im q \\ \Im q & \Re q \end{pmatrix} \cdot \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{pmatrix} \quad \text{if } d \equiv 1 \bmod 4.$$

Hence $\kappa(L_{\mathfrak{a},r})$ either the empty set or a lattice $L'_{\mathfrak{a},r}$ of index

$$[\mathbb{Z}^2 : L'_{\mathfrak{a},r}] = \begin{cases} 4d\,\Im r N q[\mathfrak{a} : L_{\mathfrak{a},r}] & \text{if } d \not\equiv 1 \bmod 4, \\ 2d\,\Im r N q[\mathfrak{a} : L_{\mathfrak{a},r}] & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

and $\kappa(S_{\mathfrak{a},r})$ is a convex set $S'_{\mathfrak{a},r}$ contained in

$$[-3|d|\frac{\mathcal{S}(r)}{\mathfrak{N}\mathfrak{a}}\mathcal{S}(q)N', 3|d|\frac{\mathcal{S}(r)}{\mathfrak{N}\mathfrak{a}}\mathcal{S}(q)N']^2,$$

which is contained in

$$[-3|d|S(q)\frac{n_{s1}(\log N)^{\alpha+1}}{n_{s0}}, 3|d|S(q)\frac{n_{s1}(\log N)^{\alpha+1}}{n_{s0}}],$$

which is in turn contained in

$$[-k'(\log N)^{2\alpha+2}N, k'(\log N)^{2\alpha+2}N],$$

where k' depends only on d and q. Write (3.5.10) as

$$\sum_{\substack{\mathfrak{a} \\ n_{s0} < N\mathfrak{a} \le n_{s1} \\ n>1 \Rightarrow n \nmid \mathfrak{a}}} \sum_{\substack{r \in \overline{\mathfrak{a}} \cap R_s \\ \Im r \neq 0}} \left| \sum_{(v,w) \in L'_{\mathfrak{a},r} \cap S'_{\mathfrak{a},r}} \lambda(v)\lambda(w) \right| \tag{3.5.11}$$

□

Since r is in R_s, $\Im r$ takes values between $-kn_{s1}(\log N)^{\alpha+1}$ and $kn_{s1}(\log N)^{\alpha+1}$. By Lemma 3.5.1, $\Im r$ takes each of these values at most

$$\lceil (kn_{s1}(\log N)^{\alpha+1})/n_{s0} \rceil \ll (\log N)^{2\alpha+2}$$

times. Thus (3.5.11) is bounded by a constant times

$$\frac{N''}{2^{s-1}}(\log N)^{2\alpha+2} \sum_{0<y\le kM_2(\log n)^{\alpha+1}} \max_{\mathfrak{a}} \max_{r:\Im r=y} \left| \sum_{(v,w)\in L'_{\mathfrak{a},r}\cap S'_{\mathfrak{a},y}} \lambda(v)\lambda(w) \right|.$$

By Corollary 3.2.8,

$$\sum_{0<y\le kM_2(\log n)^{\alpha+1}} \max_{\mathfrak{a}} \max_{r:\Im r=y} \left| \sum_{(v,w)\in L'_{\mathfrak{a},r}\cap S'_{\mathfrak{a},y}} \lambda(v)\lambda(w) \right|$$

is

$$O\left(\tau(4d\,\mathrm{num}(Nq)\det(Nq)[\mathfrak{O}_K : L']^2)\frac{((\log N)^{2\alpha+2}N)^2}{(\log N)^{8(\alpha+1)}}\right).$$

It is time to collect all terms. The total is at most

$$\frac{\log M_1}{\log M_2}\frac{\mathrm{Area}(S')}{[\mathfrak{O}_K : L']} + N'M_2^2 + \frac{N^2(\log N)^{\alpha+\frac{7}{2}}}{\sqrt{M_1}} + \sqrt{N}M_2(\log N)^{(\alpha+1)/2} + \sqrt{N}M_2 + N^2(\log N)^{\alpha}$$

times a constant depending only on (a_{ij}) and α. This simplifies to

$$O\left(\frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2 : L]} + \frac{N^2}{(\log N)^{\alpha}}\right).$$

3.6 The average of λ on irreducible cubics

In the present section we shall prove that $\mu(P(x,y))$ averages to zero for any irreducible homogeneous polynomial P of degree 3. There are two main stages in the proof: one is the reduction of the problem to a bilinear condition, and the other is the demonstration of the bilinear condition. The second stage resembles its analogue in Heath-Brown's proof that $x^3 + 2y^3$ captures its primes ([H-B]); although it is too early to speak of the general features of a strategy that was first carried out in [FI1]

and is still developing, one may venture that the bilinear conditions involved in the strategy carry over between related problems with relative ease. (See Appendix B.1.) The first stage, namely, the reduction to the bilinear condition, must be attempted with much closer regard to the specifics of the problem at hand. The reader may remark that there are few resemblances between subsection 3.6.4 and the corresponding sections in [H-B], [HBM], [HBM2]. We do follow the example of [H-B] in giving a fictively rational outline before undertaking the actual procedure over a cubic field. This explanatory device is appropiate in our case because of the inherent complications of what is essentially an extension of an approach similar to that in [FI2] to a density below the natural range of the method. For the sake of familiarity, we will adopt certain notational conventions used in [FI2].

3.6.1 Sketch

Let $\{a_n\}_{n=1}^{\infty}$ be a bounded sequence of non-negative real numbers. Write

$$A(x) = \sum_{1 \le n \le x} a_n, \quad A_d(x) = \sum_{\substack{1 \le n \le x \\ d|n}} a_n.$$

Our linear axiom will be

$$A_d = \frac{A(x)}{d} + \text{error} \qquad \text{for } d \ll D(x), \tag{3.6.1}$$

where the error term is small enough to be irrelevant for our purposes. We also take the bilinear axiom

$$\sum_{\substack{1 \le rs \le x \\ V \le s \le 2V}} f(r)g(s)a_{rs} \ll A(x)(\log x)^{-c_1}, \tag{3.6.2}$$

valid for any V, f, g satisfying

$$x^{1/2}t(x) \le V \le x/v(x),$$

$$f(n), g(n) \ll \tau_{c_2}(n),$$

$$\sum_{\substack{s \equiv a \bmod m \\ s \le S}} g(s) \ll Se^{-\kappa\sqrt{\log S}} \text{ for all } m \ll (\log x)^{c_4},$$

where the constants c_i will be as large as needed, and κ denotes an exponent of no importance. We will assume $v(x) > \sqrt{D(x)}$, as therein lies the origin of certain difficulties that we must learn to resolve. Set $z(x) = v(x)/\sqrt{D(x)}$. We assume

$$\log z(x) \ll (\log x)^{1/c_5},$$

$$z(x) \gg (\log x)^{c_6}$$

$$v(x)D(x) \gg x \cdot (z(x))^{-\kappa'},$$

Set

$$u(x) = (z(x))^{\kappa'} v(x), \quad y(x) = (z(x))^{-\kappa'-2} v(x),$$

$$w(x) = \frac{u(x)}{z(x)} 2^{[\log_2 x^{1/2}/(u(x)t(x))]}.$$

We write t, u, v, w, y, z instead of $t(x)$, $u(x)$, $\ldots$, $z(x)$, for the sake of brevity.

We adopt the symbols in [FI2]:

$$f(n \le a) = f(n) \cdot [n \le a],$$

$$f(n > a) = f(n) \cdot [n > a].$$

For any integer n and any function f,

$$f(n) = f(n \le a) + f(n > a),$$

$$f(n > a) = \sum_{bc|n} \mu(b) f(c > a).$$

Hence

$$\begin{aligned}\mu(n) &= \mu(n \le u) + \sum_{bc|n} \mu(b)\mu(c > u) \\ &= \mu(n \le u) + \sum_{bc|n} \mu(b > u)\mu(c > u) + \sum_{bc|n} \mu(b \le u)\mu(c > u).\end{aligned}$$

By Möbius inversion,

$$\begin{aligned}\sum_{bc|n} \mu(b \le v)\mu(c > u) &= \sum_{bc|n} \mu(b \le u)\mu(c) - \sum_{bc|n} \mu(b \le u)\mu(c \le u) \\ &= \mu(n \le u) - \sum_{bc|n} \mu(b \le u)\mu(c \le u).\end{aligned}$$

Therefore

$$\mu(n) = 2\mu(n \le u) + \sum_{bc|n} \mu(b > u)\mu(c > u) - \sum_{bc|n} \mu(b \le u)\mu(c \le u).$$

We can split our ranges of summation:

$$\begin{aligned}\sum_{bc|n} \mu(b > u)\mu(c > u) &= \sum_{bc|n} \mu(u < b \le w)\mu(c > u) \\ &\quad + \sum_{bc|n} \mu(b > w)\mu(u < c \le w) + \sum_{bc|n} \mu(b > w)\mu(c > w),\end{aligned}$$

$$\begin{aligned}\sum_{bc|n} \mu(b \le u)\mu(c \le u) &= \sum_{bc|n} \mu(b \le u)\mu(c \le y) + \sum_{bc|n} \mu(b \le y)\mu(y < c \le u) \\ &\quad + \sum_{bc|n} \mu(y < c \le u)\mu(y < c \le u).\end{aligned}$$

Thus

$$\begin{aligned}\mu(n) = 2\mu(n \le u) &+ \sum_{bc|n} \mu(u < b \le w)\mu(c > u) \\ &+ \sum_{bc|n} \mu(b > w)\mu(u < c \le w) + \sum_{bc|n} \mu(b > w)\mu(c > w) \\ &- \sum_{bc|n} \mu(b \le u)\mu(c \le y) - \sum_{bc|n} \mu(b \le y)\mu(y < c \le u) \\ &- \sum_{bc|n} \mu(y < b \le u)\mu(y < c \le u).\end{aligned} \tag{3.6.3}$$

We denote the terms on the right side of (3.6.3) by $\beta_1(n), \beta_2(n), \ldots, \beta_7(n)$. Set

$$S_j(x) = \sum_{n=1}^{x} \beta_j(n) a_n.$$

Then

$$\sum_{n=1}^{x} \mu(n) a_n = S_1(x) + S_2(x) + S_3(x) + S_4(x) - S_5(x) - S_6(x) - S_7(x). \tag{3.6.4}$$

The term $S_1(x)$ can be bounded trivially by $O(u)$. We can estimate $S_5(x)$ by means of the linear axiom (3.6.1):

$$\begin{aligned}S_5(x) &= \sum_{\substack{1 \le n \le x \\ bc|n}} \mu(b \le u)\mu(c \le y) a_n \\ &= \sum_{b,c} \mu(b \le u)\mu(c \le y) \frac{A(x)}{bc} \\ &= A(x) \cdot \sum_{b \le u} \mu(b)/b \cdot \sum_{c \le y} \mu(c)/c \\ &\ll A(x) \cdot e^{-\kappa\sqrt{\log u}} e^{-\kappa\sqrt{\log y}} \ll A(x) e^{-\kappa\sqrt{\log x}}.\end{aligned}$$

In the same way,

$$S_6(x) \ll A(x) e^{\kappa\sqrt{\log x}}.$$

We can easily prepare S_2 for an application of the bilinear condition (3.6.2):

$$S_2(x) = \sum_{\substack{n \le x \\ bc|n}} \mu(u < b \le w)\mu(c > u)a_n,$$

$$\begin{aligned}\sum_{\substack{x/z \le n \le x \\ bc|n}} \mu(u < b \le w)\mu(c > u)a_n &= \sum_{\substack{x/z \le rs \le x \\ x/zw \le s \le x/u}} f(r)g(s)a_{rs}, \\ &= \sum_{\substack{rs \le x \\ x/zw \le s \le x/u}} f(r)g(s)a_{rs} + O\left(\sum_{n \le x/z} \tau_3(n)a_n\right),\end{aligned}$$

where

$$\begin{aligned} f(r) &= \mu(u < b \le w), \\ g(s) &= \sum_{c|s} \mu(c > u). \end{aligned}$$

Clearly

$$\begin{aligned}\sum_{\substack{s \equiv a \bmod m \\ s \le S}} g(s) &= \sum_{\substack{s \equiv a \bmod m \\ s \le S}} \sum_{c|s} \mu(c > u) = \sum_{d \le S/u} \sum_{u < c \le S/d} \mu(c) \\ &= \sum_{d \le S/u} \left(\sum_{c \le S/d} \mu(c) - \sum_{c \le u} \mu(c)\right) \ll Se^{-\kappa\sqrt{\log S}}.\end{aligned}$$

Hence, by (3.6.2),

$$\sum_{\substack{rs \le x \\ x/zw \le s \le x/u}} f(r)g(s)a_{rs} \ll A(x)(\log x)^{-c_1+1},$$

and so

$$S_2(x) \ll A(x)(\log x)^{-c_1+1} + A(x/z)(\log x)^{\kappa''} \ll x(\log x)^{-c_1+1} + x(\log x)^{-c_6+\kappa''}.$$

The sum $S_3(x)$ can be bounded by $x(\log x)^{-c_1+1} + x(\log x)^{-c_6+\kappa''}$ in exactly the same fashion. Thus, it remains only to bound S_4 and S_7. The complications to follow are

due to the gap between $v(x)$ and $\sqrt{D(x)}$. When there is no such gap, S_7 disappears and S_4 can be bounded much more simply; see Appendix B.1.

We will bound S_7 first. Let $\{\lambda_d\}$ be a Rosser-Iwaniec sieve for the primes $\{p : uy^{-1} < p \leq wu^{-1}\}$ with upper cut wu^{-1}. By definition,

$$\lambda_1 = 1, \quad \lambda_d = 0 \text{ if } d \leq uy^{-1} \text{ or } d > wu^{-1}.$$
$$\lambda_d = 0 \text{ if } p|d \text{ for some } p \leq uy^{-1}.$$

Hence

$$1 = \sum_{d|n} \lambda_d - \sum_{\substack{uy^{-1} < d \leq wu^{-1} \\ d|n}} \lambda_d$$

for every d. Substituting into $\beta_7(n)$, we obtain

$$\begin{aligned}\beta_7(n) = &\sum_{bc|n} \sum_{d|b} \lambda_d \mu(y < b \leq u)\mu(y < c \leq u) \\ &- \sum_{bc|n} \sum_{\substack{uy^{-1} < d \leq wu^{-1} \\ d|b}} \lambda_d \mu(y < b \leq u)\mu(y < c \leq u).\end{aligned}$$

We give the names $\beta_8(n)$ and $\beta_9(n)$ to the terms on the right side of (3.6.1). Let

$$S_8(x) = \sum_{n=1}^{x} \beta_8(n) a_n, \quad S_9(x) = \sum_{n=1}^{x} \beta_9(n) a_n.$$

Let us begin by bounding S_8. The main idea should be clear: since $\sum_{d|b} \lambda_d$ is small for most b, one would think that $\beta_8(n)$ is small as well. We must proceed with caution, however. It is only here, and in the corresponding part for S_4, that we will have to incur in error bound greater than $O(A(x)(\log X)^{-B})$.

We will have to resolve two issues. The domain $y < c \leq u$ of $\mu(y < c \leq u)$ may be wide enough to ruin a naive bound, and, in addition, bc may be too large for (3.6.1)

We write

$$S_8(x) = \sum_{y<b\le u} \sum_{d|b} \lambda_d \mu(y < b \le u) \sum_{h\le x/b} \sum_{c|h} \mu(y < c \le u) a_{bh}.$$

We would like to bound $\sum_{h\le x/b} \sum_{c|h} \mu(y < c \le u) a_h$. Now

$$\begin{aligned}\sum_{c|h} \mu(y < c \le u) &= \sum_{c|h} \mu(c \le u) - \sum_{c|h} \mu(c \le y) \\ &= \sum_{c|h} \mu(c) - \sum_{c|h} \mu(c > u) - \sum_{c|h} \mu(c \le y) \\ &= [h = 1] - \sum_{c|h} \mu(c > u) - \sum_{c|h} \mu(c \le y).\end{aligned}$$

Since $h \ge c \ge y \ge 1$, we may ignore the case $h = 1$. We shall bound

$$\sum_{h\le x/b} \left| \sum_{c|h} \mu(c \le y) a_{bh} \right|. \tag{3.6.5}$$

Let us first look at the other term, viz. $\sum_{h\le x/b} \left| \sum_{c|h} \mu(c \le y) a_{bh} \right|$. Clearly

$$\sum_{c|h} \mu(c > u) a_{bh} = \sum_{c|h} [c > u] \mu(c) a_{bh} = \sum_{c|h} [h/c > u] \mu(h/c) a_{bh}.$$

For h square-free,

$$\sum_{c|h} [h/c > u] \mu(h/c) a_{bh} = \mu(h) \sum_{c|h} [h/c > u] \mu(c) a_{bc} = \mu(h) \sum_{c|h} \mu(c < h/u) a_{bc}.$$

(The expression for h having a small square factor is in essence the same; values of h with large square factors can be eliminated.) Hence

$$\sum_{h\le x/b} \left| \sum_{c|h} \mu(c > u) a_{bh} \right| = \sum_{h\le x/b} \left| \sum_{c|h} \mu(c < h/u) a_{bh} \right|. \tag{3.6.6}$$

Since $bh/u \le x/u \le D(x)$, the right side of (see (3.6.1)) can be bounded like (3.6.5). Let us proceed to bound (3.6.5).

Suppose h has a prime divisor $p \le l$, where l is a fixed positive integer. Then the set of all square-free divisors of h can be partitioned into pairs (c, cp). Clearly $\mu(c) = -\mu(cp)$. Moreover, we have either $c \le y$, $cp \le y$ or $c > y$, $cp > y$, unless c lies in the range $y/l < c \le y$. Thus, all pairs (c, cp) that make a contribution to $\sum_{c|h} \mu(c \le y)$ satisfy $y/l < c \le y$. Hence

$$\left| \sum_{c|h} \mu(c < y) \right| \le \sum_{\substack{c|h \\ y/l < c \le y}} 1.$$

Now define

$$l_0 = 2 = 2^{2^0},\ l_1 = 3 = 2^{2^1}, \ldots,\ h_j = 2^{2^j}, \ldots$$

Note that $x^{1/2} < h_{\lfloor \log_2 \log_2 x \rfloor} \le x$. Let

$$L_0 = \{\text{even numbers}\},$$
$$L_j = \{h \in \mathbb{Z} : (\exists p \le l_j \text{ s.t. } p|h) \wedge (\forall p \le l_{j-1}, p \nmid h)\}.$$

Then, by the above,

$$\begin{aligned} \sum_{\substack{h \le x/b \\ h \in L_j}} \left| \sum_{c|h} \mu(c \le y) \right| a_{bh} &\le \sum_{\substack{h \le x/b \\ h \in L_j}} \sum_{\substack{c|h \\ y/l_j < c \le y}} a_{bh} \\ &\le \sum_{\substack{y/l_j < c \le y \\ p|c \Rightarrow p > l_{j-1}}} \sum_{k \le x/bc} a_{bck}. \end{aligned}$$

By (3.6.1) and the fact that $bc \le y^2 \le D$,

$$\sum_{k \le x/bc} a_{bck} = A_{bc}(x) \sim \frac{A(x)}{bc}.$$

Hence

$$\sum_{\substack{y/l_j<c\le y\\ p|c\Rightarrow p>l_{j-1}}}\sum_{k\le x/bc} a_{bck} \sim \frac{A(x)}{b}\sum_{\substack{y/l_j<c\le y\\ p|c\Rightarrow p>l_{j-1}}}\frac{1}{c} \ll \frac{A(x)}{b}\frac{\log l_j}{\log l_{j-1}} = \frac{2A(x)}{b}. \tag{3.6.7}$$

Considering all sets L_0, L_1, $\ldots$, $L_{\lfloor \log_2 \log_2 x\rfloor}$, we obtain

$$\sum_{h\le x/b}\left|\sum_{c|h}\mu(c\le y)\right| a_{bh} \ll \frac{A(x)}{b}\log\log x.$$

We conclude that

$$\begin{aligned} |S_8(x)| &\le \sum_{y<b\le u}\sum_{d|b}\lambda_d\sum_{h\le x/b}\left|\sum_{c|h}\mu(y<c\le u)\right| a_{bh} \\ &\ll \sum_{y<b\le u}\sum_{d|b}\lambda_d\frac{A(x)}{b}\log\log x. \end{aligned} \tag{3.6.8}$$

(Notice that $\sum_{d|b}\lambda_d$ is always non-negative.) Since

$$\sum_{b\le a}\left(\sum_{d|b}\lambda_d\right) \ll \frac{a}{(\log wu^{-1})/(\log uy^{-1})},$$

we can easily see that

$$\sum_{y<b\le u}\left(\sum_{d|b}\lambda_d\right)\frac{1}{b} \ll \frac{\log uy^{-1}}{(\log wu^{-1})/(\log uy^{-1})} \ll \frac{(\log z)^2}{\log x}.$$

Therefore

$$|S_8(x)| \le \frac{(\log z)^2\log\log x}{\log x}A(x). \tag{3.6.9}$$

It is time to bound $S_9(x)$. We change the order of summation:

$$\begin{aligned} S_9(x) &= \sum_{y<c\le u} \mu(c) \sum_{uy^{-1}\le d\le wu^{-1}} \lambda_d \sum_{y/d<h\le u/d} \mu(hd) \sum_{k\le x/cdh} a_{cdhk} \\ &= \sum_{u<s\le w} \sum_{\substack{d|s \\ uy^{-1}\le d\le wu^{-1}}} \lambda_d \mu(s/d)\mu(d) \sum_{\substack{y/d<h\le u/d \\ \gcd(h,d)=1}} \mu(h) \sum_{k\le x/cdh} a_{cdhk}. \end{aligned}$$

Since d has no small factors when $\lambda_d \neq 0$, it is a simple matter to remove the condition $\gcd(h,d)=1$ with an error of at most $O((\log x)^3/\log z)$. We can make the intervals of summation of d and h independent from each other by slicing $[uy^{-1}, wu^{-1}]$ into intervals of the form $[l, l(1+(\log x))^{-c})$. There are at most $O((\log x)^{c+1})$ such intervals. We obtain

$$S_9(x) \ll (\log x)^{-c'} A(x) + (\log x)^{c+1} \max_{uy^{-1}\le K\le wu^{-1}} \left| \sum_{u<s\le w} f_K(r) g_K(s) a_{rs} \right|, \qquad (3.6.10)$$

where

$$\begin{aligned} f_K(r) &= \sum_{\substack{h|r \\ y/K<h\le u/K}} \mu(h), \\ g_K(s) &= \sum_{\substack{d|s \\ K\le d<K(1+(\log N)^c)}} \lambda_d \mu(d)\mu(s/d). \end{aligned}$$

We can check that $g_K(s)$ averages to zero over $s \equiv a \bmod m$ as we did in (3.6.1). Hence we can apply the bilinear axiom (3.6.2):

$$\sum_{u<r\le w} f(r)g(s) \ll A(x)(\log x)^{-c_1+1}.$$

Thus

$$S_9(x) \ll (\log x)^{-c'} A(x) + (\log x)^{-c_1+c+1}.$$

Remember that we may set c_1 to an arbitrarily high value.

It remains to bound S_4. We can write

$$\begin{aligned}\beta_4(n) &= \sum_{bc|n} \mu(b > w)\mu(c > w) \\ &= \sum_{bc|n} \sum_{d|b} \lambda_d \mu(b > w)\mu(c > w) \\ &- \sum_{bc|n} \sum_{\substack{uy^{-1} \le d \le wu^{-1} \\ d|b}} \lambda_d \mu(b > w)\mu(c > w).\end{aligned}$$

We give the names β_{10} and β_{11} to the terms on the right side of (3.6.1). Let

$$\begin{aligned}S_{10}(x) &= \sum_{n=1}^{x} \beta_{10}(n) a_n, \\ S_{11}(x) &= \sum_{n=1}^{x} \beta_{11}(n) a_n.\end{aligned}$$

We bound $S_{10}(x)$ as we bounded $S_8(x)$. We can obtain an expression similar to (3.6.10) for $S_{11}(x)$:

$$S_{11} \ll (\log x)^{-c'} A(x) + (\log x)^{c+1} \max_{xw^{-2} \le K \le xw^{-1}u^{-1}} \left| \sum_{u < s \le w} f_K(r) g_K(s) \right|,$$

where

$$\begin{aligned}f_K(s) &= \sum_{\substack{d|s \\ K \le d < K(1+(\log N)^c)}} \lambda_d \mu(d)\mu(s/d) \\ g_K(r) &= \sum_{\substack{h|r \\ y/K < h \le u/K}} \mu(h).\end{aligned}$$

Again, we apply (3.6.2) and are done:

$$S_{11}(x) \ll (\log x)^{-c'} A(x) + (\log x)^{-c_1+1}.$$

We conclude by (3.6.4) that

$$\sum_{n=1}^{x} \mu(n) a_n \ll \frac{(\log z)^2 \log\log x}{\log x} A(x).$$

* * *

In the course of the actual procedure we are about to undertake, we will come across some technical difficulties not present in the above outline. For example, we will be forced to sieve over ideals and ideal numbers rather than over rational integers. Our linear sieve axioms will be valid only on average, unlike, say, (3.6.1). Nevertheless, we will be able to follow, in the main, the plan we have traced.

As the method we have devised to eliminate a bothersome interval may have wider applications, it may be worthwhile to review its main idea. We are given the task of estimating a sum

$$\sum_{a,b \le X} F_{ab}.$$

We assume we know how to estimate

$$\sum_{\substack{a,b \le X \\ a \le x(z(x))^{-1}}} F_{ab} \quad \text{and} \quad \sum_{\substack{a,b \le X \\ a \ge xz(x)}} F_{ab}, \tag{3.6.11}$$

where $\log z(x) = o(\sqrt{\log x})$. In order to eliminate the missing interval, we apply a sieve to the constant function $a \mapsto 1$ with respect to the primes larger than $z^2(x)$:

$$\sum_{\substack{a,b \le X \\ x(z(x))^{-1} \le a \le xz(x)}} F_{ab} = \sum_{\substack{a,b \le X \\ x(z(x))^{-1} \le a \le xz(x)}} \sum_{d|a} \lambda_d F_{ab} - \sum_{\substack{a,b \le X \\ x(z(x))^{-1} \le a \le xz(x)}} \sum_{\substack{d|a \\ d > z^2(x)}} \lambda_d F_{ab}. \tag{3.6.12}$$

(Notice the peculiar use of a sieve as an identity rather than an approximation.) The

first term on the right can be seen from sieve theory to be at most

$$O\left(\frac{\log z(x)}{\log x}\cdot(\log xz(x)-\log x(z(x))^{-1})\right)\cdot X.$$

The second term on the right of (3.6.12) can be treated analogously to the first sum in (3.6.11) with variables $a'=a/d$ and $b'=bd$; clearly $a'b'\leq X$ and $a'\leq x(z(x))^{-1}$.

3.6.2 Axioms

Let $K/\mathbb{Q}$ be a cubic extension of $\mathbb{Q}$. Let k_0 be a fixed rational integer. Define

$$\mathcal{R}=\{\mathfrak{r}:\mathfrak{r}\in I_K,\mu_K(\mathfrak{r})^2=1,\ \mu_K(N(\mathfrak{r}/\gcd(k_0,\mathfrak{r})))=1\}. \tag{3.6.13}$$

We write $\mu_{\mathcal{R}}$ for the Möbius function with respect to $\mathcal{R}$:

$$\mu_{\mathcal{R}}(\mathfrak{a})=\prod_{\substack{\mathfrak{p}|\mathfrak{a}\\ \mathfrak{p}\in\mathcal{R}}}(-1)\quad\text{if } \mathfrak{a} \text{ is square-free,}$$

$$\mu_{\mathcal{R}}(\mathfrak{a})=0\qquad\qquad\qquad\text{otherwise.}$$

We are given a bounded sequence $\{a_{\mathfrak{r}}\}_{\mathfrak{r}\in\mathcal{R}}$ of non-negative real numbers, the properties of whose distribution we will now describe.

We abuse notation by writing $\mathfrak{a}<x$, $\mathfrak{a}>x$ when we mean $N\mathfrak{a}<x$, $N\mathfrak{a}>x$; $N\mathfrak{a}<N\mathfrak{b}$ will, however, still mean $N\mathfrak{a}<N\mathfrak{b}$. For $\mathfrak{d}\in\mathcal{R}$, define

$$A_{\mathfrak{d}}(x)=\sum_{\substack{\mathfrak{d}|\mathfrak{n}\\ \mathfrak{n}\leq x}}a_{\mathfrak{n}},\quad A(x)=\sum_{\mathfrak{n}\leq x}a_{\mathfrak{n}}.$$

Write

$$A_{\mathfrak{d}}(x)=\gamma(\mathfrak{d})A(x)+r_{\mathfrak{d}}, \tag{3.6.14}$$

where γ is a bounded multiplicative function supported on $\mathcal{R}$ and $r_{\mathfrak{d}}$ is an error term.

We assume our estimates on γ to be quite strong for all primes above $(\log X)^\kappa$:

$$\sum_{\mathfrak{p}\le x}\gamma(\mathfrak{p}) = \log\log x + \alpha + O((\log x)^{-B}),$$

for any $x > (\log X)^\kappa$, some constant α and any constant $B > 0$, where the implied constant depends on B. Let us be more precise and make clear that what we are avoiding the divisors of a fixed rational integer $\delta \le (\log X)^\kappa$:

$$\sum_{\substack{\mathfrak{p}\le x\\ \mathfrak{p}\nmid\delta}}\gamma(\mathfrak{p}) = \log\log x + \alpha + O((\log x)^{-B}). \tag{3.6.15}$$

We will also allow ourselves the relative luxury of the following assumption on the size of $\gamma(\mathfrak{d})$:

$$\gamma(\mathfrak{d}) \ll 1/N\mathfrak{d}. \tag{3.6.16}$$

Condition (3.6.16) will be fulfilled for the sequence we are ultimately interested in. It is possible to replace (3.6.16) with an average condition; see the remark after (3.6.24).

We have an average bound for the remainder terms $r_{\mathfrak{d}}$: for any $B_1, B_2 > 0$, there is a $C > 0$ such that

$$\sum_{\mathfrak{d}\le x^{2/3}(\log x)^{-C}} \tau^{B_1}(\mathfrak{d}) r_{\mathfrak{d}} \ll (\log x)^{-B_2} A(x). \tag{3.6.17}$$

Typically, $A(x)$ will be about a constant times $x^{2/3}$. We will assume the consequences

$$A(x) \gg x^{1/2}, \tag{3.6.18}$$

$$A(x/z) \ll (\log x)^{-B} A(x) \tag{3.6.19}$$

for any z such that $\log\log x/\log z = o(1)$.

We assume the following axiom.

Bilinear condition. *Let $f, g : I_K \to \mathbb{R}$ satisfy*

$$|f(\mathfrak{a})|, |g(\mathfrak{a})| \ll \tau^2(\mathfrak{a}). \tag{3.6.20}$$

Assume g is a linear combination of the form

$$g(\mathfrak{a}) = \sum_{\mathfrak{d}|\mathfrak{a}} c_{\mathfrak{d}} \mu_{\mathcal{R}}(\mathfrak{d} > \ell) \tag{3.6.21}$$

or

$$g(\mathfrak{a}) = \sum_{\mathfrak{d}|\mathfrak{a}} c_{\mathfrak{d}} \mu'_{\mathcal{R}}(\mathfrak{d} > \ell), \tag{3.6.22}$$

where

$$\mu'_{\mathcal{R}} = \mu_{\mathcal{R}} \cdot (\mathfrak{p} \leq (\log x)^{10} \Rightarrow \mathfrak{p} \nmid \mathfrak{d}),$$

the sequence $c_{\mathfrak{d}}$ is bounded and $\ell > x^{1/\kappa}$ for some constant κ. We assume furthermore that either f or g is zero on all numbers with small prime divisors:

$$\mathfrak{p}|\mathfrak{a}, \mathfrak{q}|\mathfrak{b}, \mathfrak{p}, \mathfrak{q} \leq (\log x)^{10} \Rightarrow f(\mathfrak{a})g(\mathfrak{b}) = 0.$$

Then

$$\sum_{\substack{\mathfrak{a}\mathfrak{b} \leq x \\ x^{1/2}(\log x)^T < N\mathfrak{b} \leq x^{3/2}(\log x)^{-T}}} f(\mathfrak{a})g(\mathfrak{b}) \ll A(x)(\log x)^{-2}, \tag{3.6.23}$$

where T is a constant depending only on B and on the implied constant in (3.6.20).

Write $P(z)$ for $\prod_{\mathfrak{p}<z} \mathfrak{p}$. Write P_{10} for $P((\log x)^{10})$. Let

$$\sum_{*} \cdots$$

be short for

$$\sum_{\substack{\mathfrak{b}\mathfrak{c}|\mathfrak{n} \\ \gcd(\mathfrak{n}/\mathfrak{b}, P_{10}^{\infty})=1}} \cdots$$

We will follow a convention we have already implicitly used in this subsection: κ is a fixed constant given by the sequence $\{a_{\mathfrak{n}}\}$, and we should be ready for it to be arbitrarily large, but fixed; B is a parameter that we can set to be arbitrarily large given our axioms (example: "the number of primes in arithmetic progressions of modulus up to $(\log x)^B$ is ..."); finally, C is a parameter that may have to be taken to be large if a condition is to be satisfied for a chosen value of B.

3.6.3 Technical lemmas

Lemma 3.6.1. *Assume (3.6.15). Then, for any $B > 0$,*

$$\sum_{\substack{\mathfrak{d}\leq y \\ (\mathfrak{d},\mathfrak{m})=1}} \mu(\mathfrak{d})g(\mathfrak{d}) \ll (\log y)^{-B} + (\log y)^3 \sum_{\substack{y^{(\log\log y)^{-2}} \leq \mathfrak{p} \leq y \\ \mathfrak{p}|\mathfrak{m}}} \frac{1}{N\mathfrak{p}}.$$

Proof. As in [FI2], pp. 1048–1049. □

Lemma 3.6.2. *Assume (3.6.17) and (3.6.15). Then*

$$\sum_{\mathfrak{n}\leq x} \tau^4(\mathfrak{n})a_{\mathfrak{n}} \ll (\log x)^{16} A(x).$$

Proof. As in [FI2], p. 1047. □

Lemma 3.6.3. *Assume (3.6.18), (3.6.16) and (3.6.17). Then*

$$\sum_{\mathfrak{n}\leq x} [\mathfrak{n} \leq x^{4/11} \gcd(\mathfrak{n}, P_{10}^{\infty})] \gcd(\mathfrak{n}, P_{10}^{\infty}) a_{\mathfrak{n}} \ll A(x)(\log x)^{-B}.$$

Proof. Clearly

$$\begin{aligned}
\sum_{\mathfrak{n}\le x}[\mathfrak{n}\le x^{4/11}\gcd(\mathfrak{n},P_{10}^{\infty})]a_{\mathfrak{n}} &\le \sum_{\mathfrak{b}\le x^{4/11}}\sum_{\substack{\mathfrak{c}|P_{10}^{\infty}\\ \mathfrak{b}\mathfrak{c}\le x}} a_{\mathfrak{b}\mathfrak{c}}\\
&\le \sum_{\mathfrak{b}\le x^{4/11}}\sum_{\mathfrak{c}\le x^{1/11}} a_{\mathfrak{b}\mathfrak{c}}\\
&+ \sum_{\mathfrak{b}\le x^{1/11}}\sum_{\substack{\mathfrak{c}|P_{10}^{\infty}\\ x^{1/11}<\mathfrak{c}\le x^{1/11}(\log x)^{10}}}\sum_{\substack{\mathfrak{d}\\ \mathfrak{b}\mathfrak{c}\mathfrak{d}\le x}} a_{\mathfrak{b}\mathfrak{c}\mathfrak{d}}\\
&\le x^{5/11}+A(x)(\log x)^{-B}\\
&+ A(x)\sum_{\mathfrak{b}\le x^{4/11}}\sum_{\substack{\mathfrak{c}|P_{10}^{\infty}\\ x^{1/11}\le\mathfrak{c}\le x^{1/11}(\log x)^{10}}}\gamma(\mathfrak{b}\mathfrak{c}).
\end{aligned}$$

The cardinality of $\{\mathfrak{c}\le x^{1/11}(\log x)^{10}:\mathfrak{c}|P_{10}^{\infty}\}$ can be crudely estimated by means of Rankin's trick:

$$\begin{aligned}
\#\{\mathfrak{c}\le m:\mathfrak{c}|P_{10}^{\infty}\} &\le \sum_{\mathfrak{c}|P_{10}^{\infty}}\frac{m^{9/10}}{(N\mathfrak{c})^{9/10}} = m^{9/10}\prod_{\mathfrak{p}|P_{10}^{\infty}}\frac{1}{1-(N\mathfrak{p})^{-9/10}}\\
&\sim m^{9/10}e^{\sum_{\mathfrak{p}|P_{10}^{\infty}}(N\mathfrak{p})^{-9/10}} \ll m^{9/10}e^{C(\log x)/(\log\log x)} \ll m^{9/10+\epsilon}.
\end{aligned}$$

Hence

$$\sum_{\substack{\mathfrak{c}|P_{10}^{\infty}\\ x^{1/11}\le\mathfrak{c}\le x^{1/11}(\log x)^{10}}}\frac{1}{N\mathfrak{c}} \ll x^{-1/110+\epsilon}$$

and thus

$$\sum_{\mathfrak{b}\le x^{4/11+\epsilon}}\sum_{\substack{\mathfrak{c}|P_{10}^{\infty}\\ x^{1/11}\le\mathfrak{c}\le x^{1/11}(\log x)^{10}}}\gamma(\mathfrak{b}\mathfrak{c}) \ll (\log x)x^{-1/110+\epsilon}.$$

□

3.6.4 Bounds and manipulations

Let $z = e^{(\log\log x)(\log\log\log x)^{1/2}}$, $y = x^{1/3}z^{-2}$, $u = x^{1/3}z$, $w = x^{1/2}z^{-1}$. As in (3.6.3) and (3.6.4),

$$\mu_{\mathcal{R}}(\mathfrak{n}) = \beta_1(\mathfrak{n}) + \beta_2(\mathfrak{n}) + \beta_3(\mathfrak{n}) + \beta_4(\mathfrak{n}) - \beta_5(\mathfrak{n}) - \beta_6(\mathfrak{n}) - \beta_7(\mathfrak{n}),$$

$$\sum_{\mathfrak{n}\le x} \mu_{\mathcal{R}}(\mathfrak{n})a_{\mathfrak{n}} = S_1(x) + S_2(x) + S_3(x) + S_4(x) - S_5(x) - S_6(x) - S_7(x),$$

where

$$\beta_1(\mathfrak{n}) = \mu_{\mathcal{R}}(\mathfrak{n} \le u) + \sum_{*} \mu_{\mathcal{R}}(\mathfrak{b})\mu_{\mathcal{R}}(\mathfrak{c} \le u),$$

$$\beta_2(\mathfrak{n}) = \sum_{*} \mu_{\mathcal{R}}(u < \mathfrak{b} \le w)\mu_{\mathcal{R}}(\mathfrak{c} > u),$$

$$\beta_3(\mathfrak{n}) = \sum_{*} \mu_{\mathcal{R}}(\mathfrak{b} > w)\mu_{\mathcal{R}}(u < \mathfrak{c} \le w),$$

$$\beta_4(\mathfrak{n}) = \sum_{*} \mu_{\mathcal{R}}(\mathfrak{b} > w)\mu_{\mathcal{R}}(\mathfrak{c} > w),$$

$$\beta_5(\mathfrak{n}) = \sum_{*} \mu_{\mathcal{R}}(\mathfrak{b} \le u)\mu_{\mathcal{R}}(\mathfrak{c} \le y),$$

$$\beta_6(\mathfrak{n}) = \sum_{*} \mu_{\mathcal{R}}(\mathfrak{b} \le y)\mu_{\mathcal{R}}(y < \mathfrak{c} \le u),$$

$$\beta_7(\mathfrak{n}) = \sum_{*} \mu_{\mathcal{R}}(y < \mathfrak{b} \le u)\mu_{\mathcal{R}}(y < \mathfrak{c} \le u),$$

and

$$S_j(x) = \sum_{\mathfrak{n}\le x} \beta_j(n)a_{\mathfrak{n}}.$$

Clearly

$$\begin{aligned} S_1(x) &= \sum_{\mathfrak{n}\le u} \mu_{\mathcal{R}}(\mathfrak{n})a_{\mathfrak{n}} + \sum_{\mathfrak{n}\le x}\sum_{*} \mu_{\mathcal{R}}(\mathfrak{b})\mu_{\mathcal{R}}(\mathfrak{c} \le u)a_{\mathfrak{n}} \\ &= O(A(u)) + \sum_{\mathfrak{n}\le x} \mu_{\mathcal{R}}(\gcd(\mathfrak{n}, P_{10}^{\infty}))\mu_{\mathcal{R}}(\mathfrak{n}/\gcd(\mathfrak{n}, P_{10}^{\infty}))a_{\mathfrak{n}} \\ &= O(A(u)) + \sum_{\mathfrak{n}\le x} [\mathfrak{n} \le u\gcd(\mathfrak{n}, P_{10}^{\infty})]a_{\mathfrak{n}}. \end{aligned}$$

By (3.6.19) and Lemma 3.6.3, we can conclude that

$$S_1(x) \ll (\log x)^{-B} A(x).$$

We can rewrite S_5 as follows:

$$S_5(x) = \sum_{\mathfrak{n} \le x} \sum_{*} h(\mathfrak{b} \le u) \mu_{\mathcal{R}}(\mathfrak{c} \le y) \sum_{\substack{\mathfrak{d} \le x/uy \\ \mathfrak{p} | \mathfrak{d} \Rightarrow \mathfrak{p} > (\log x)^{10}}} a_{\mathfrak{b}\mathfrak{c}\mathfrak{d}}.$$

Since $\frac{\log(x^{2/3}//((\log x)^C uy))}{\log\log x^{10}} \gg (\log\log x)(\log\log\log x)$, we can apply the fundamental lemma of sieve theory (vd., e.g., [HR], Ch. 2, or [Iw2], Lem 2.5) to obtain

$$\begin{aligned} \sum_{\substack{\mathfrak{d} \le x/uy \\ \mathfrak{p} | \mathfrak{d} \Rightarrow \mathfrak{p} > (\log x)^{10}}} a_{\mathfrak{b}\mathfrak{c}\mathfrak{d}} &= V_{\mathfrak{b}\mathfrak{c}} X (1 + O(e^{-(\log\log x)(\log\log\log x)})) + \text{error} \\ &= V_{\mathfrak{b}\mathfrak{c}} X (1 + O(1/(\log x)^{\log\log\log x})) + \text{error}, \end{aligned}$$

where the error term is collected by (3.6.17), and the leading term in the main term is given by

$$V_{\mathfrak{b}\mathfrak{c}} = \prod_{\substack{\mathfrak{p} \le (\log x)^{10} \\ \mathfrak{p} \nmid \mathfrak{b}\mathfrak{c}}} (1 - \gamma'(\mathfrak{p})),$$

where $\gamma'(\mathfrak{p}) = \gamma(\mathfrak{p})$ for $\mathfrak{p} \nmid \mathfrak{b}\mathfrak{c}$, $\gamma'(\mathfrak{p}) = 0$ for $\mathfrak{p} \nmid \mathfrak{b}\mathfrak{c}$, $\mathfrak{p} \nmid k_0$. We then apply Lemma 3.6.1 and obtain

$$S_5(x) \ll A(x)/(\log x)^B.$$

In the same way,

$$S_6(x) \ll A(x)/(\log x)^B.$$

As in subsection 3.6.1, we have

$$S_2(x) = \sum_{\substack{\mathfrak{r}\mathfrak{s}\le x \\ x/zw\le \mathfrak{s}\le x/w}} f(\mathfrak{r})g(\mathfrak{s})a_{\mathfrak{r}\mathfrak{s}},$$

where

$$f(\mathfrak{r}) = \sum_{\substack{\mathfrak{b}|\mathfrak{r} \\ \gcd(\mathfrak{r}/\mathfrak{b},P_{10})=1}} h(u < \mathfrak{b} \le w),$$

$$g(\mathfrak{s}) = \mu'_{\mathcal{R}}(u < \mathfrak{s} < w).$$

By the bilinear condition (3.6.23),

$$\sum_{\substack{\mathfrak{r}\mathfrak{s}\le x \\ x/zw\le \mathfrak{s}\le x/u}} f(\mathfrak{r})g(\mathfrak{s}) \ll A(x)(\log x)^{-B}.$$

By Lemma 3.6.2,

$$\sum_{n\le x/z} \tau_3(n)a_n \ll A(x/z)(\log x)^{\kappa}.$$

Hence

$$\begin{aligned} S_2(x) &\ll A(x/z)(\log x)^{\kappa} + A(x)(\log x)^{-B} \\ &\ll A(x)(\log x)^{\kappa}/z^2 + A(x)(\log x)^{-B}. \end{aligned}$$

In the same way,

$$S_3(x) = \sum_{\substack{\mathfrak{r}\mathfrak{s}\le x \\ x/zw\le \mathfrak{s}\le x/w}} f(\mathfrak{r})g(\mathfrak{s})a_{\mathfrak{r}\mathfrak{s}} + O\left(\sum_{n\le x/z} \tau_3(n)a_n + A(x/z)\right),$$

where

$$f(\mathfrak{r}) = \sum_{\substack{\mathfrak{c}|\mathfrak{s} \\ \gcd(\mathfrak{s}/\mathfrak{c},P_{10})=1}} \mu'_{\mathcal{R}}(\mathfrak{c} > w),$$

$$g(\mathfrak{s}) = \mu_{\mathcal{R}}(u < \mathfrak{b} \le w)$$

and consequently

$$\begin{aligned} S_3(x) &\ll A(x/z)(\log x)^{\kappa} + A(x)(\log x)^{-B} \\ &\ll A(x)(\log x)^{\kappa}/z^2 + A(x)(\log x)^{-B}. \end{aligned}$$

It is time to bound S_7. Let $\{\lambda_{\mathfrak{d}}\}$ be a generalized Rosser-Iwaniec sieve (see, e.g., [Col2]) for the primes

$$\{\mathfrak{p} \in \mathcal{R} : uy^{-1} < \mathfrak{p} \leq wu^{-1}\}, \tag{3.6.24}$$

upper cut wu^{-1} and sieved set $\mathcal{R}$.

Remark. We could sieve only up to a fractional power of wu^{-1}, and change our bounds only by a constant as a result – a constant that would not necessarily be greater than 1. A Selberg sieve (see the generalization in [Ri1]–[Ri3]) would do just as well; its main defect for our purposes, namely, its having coefficients that may grow as fast as the divisor function, is immaterial in the present context. Notice also that, if we did not have (3.6.16), it would be best to use $\gamma(\mathfrak{d})$ as our input, instead of $1/N\mathfrak{d}$, which we implicitly use by choosing $\mathcal{R}$ to be our sieved set. We have made the latter choice here for the sake of simplicity: it is elements of $\mathcal{R}$, not elements of $\{a_{\mathfrak{n}}\}$, that are being sieved here.

By definition,

$$\begin{aligned} \lambda_1 = 1, \lambda_{\mathfrak{d}} = 0 \text{ if } \mathfrak{d} \leq uy^{-1} \text{ or } \mathfrak{d} > wu^{-1} \\ \lambda_{\mathfrak{d}} = 0 \text{ if } \mathfrak{p}|\mathfrak{d} \text{ for some } \mathfrak{p} \leq uy^{-1}. \end{aligned}$$

Hence

$$1 = \sum_{\mathfrak{d}|\mathfrak{n}} \lambda_{\mathfrak{d}} \; - \sum_{\substack{uy^{-1} < \mathfrak{d} \leq wu^{-1} \\ \mathfrak{d}|\mathfrak{n}}} \lambda_{\mathfrak{d}} \tag{3.6.25}$$

for every $\mathfrak{d} \in \mathcal{R}$. We substitute (3.6.25) into S_7:

$$\begin{aligned} S_7(x) &= \sum_{*} \sum_{\mathfrak{d}|\mathfrak{c}} \lambda_{\mathfrak{d}} h(y < \mathfrak{b} \leq u) \mu_{\mathcal{R}}(y < c \leq u) \\ &- \sum_{*} \sum_{\substack{uy^{-1} < \mathfrak{d} \leq wu^{-1} \\ \mathfrak{d}|\mathfrak{c}}} \lambda_{\mathfrak{d}} h(y \leq b < u) \mu_{\mathcal{R}}(y < c \leq u) \\ &= S_8(x) + S_9(x), \end{aligned}$$

say. The argument between (3.6.5) and (3.6.9) is unchanged; we use the upper bound (3.6.16) to bound $\gamma(\mathfrak{d})$. As a result,

$$S_8(x) \ll \frac{(\log z)^2 \log\log x}{\log x}.$$

We can express S_9 as before:

$$S_9(x) = (\log x)^{-B} A(x) + (\log x)^{C+1} \max_{uy^{-1} \leq R \leq wu^{-1}} \left| \sum_{u < \mathfrak{s} \leq w} f_R(\mathfrak{r}) g_R(\mathfrak{s}) a_{\mathfrak{r}\mathfrak{s}} \right|,$$

where

$$\begin{aligned} f_R(\mathfrak{r}) &= \sum_{\substack{\mathfrak{h}|\mathfrak{r} \\ y/K < \mathfrak{h} \leq u/K \\ \mathfrak{p} < (\log x)^{10} \Rightarrow \mathfrak{p} \nmid \mathfrak{r}/\mathfrak{h}}} h(\mathfrak{h}) \\ g_R(\mathfrak{r}) &= \sum_{\substack{\mathfrak{d}|\mathfrak{s} \\ K \leq \mathfrak{d} \leq K(1+(\log N)^{-C})}} \lambda_{\mathfrak{d}} h(\mathfrak{d}) \mu'_{\mathcal{R}}(\mathfrak{s}/\mathfrak{d}). \end{aligned}$$

Notice that the support of $\lambda_{\mathfrak{d}}$ excludes $[2, (\log x)^{10}]$. We apply the bilinear axiom (3.6.23) and obtain

$$S_9(x) \ll A(x)(\log x)^{-B}.$$

Hence

$$S_7(x) \ll \frac{(\log z)^2 \log\log x}{\log x}.$$

‘ The same bound can be obtained for S_4 by nearly the same argument; see subsection

3.6.1. We conclude that

$$\sum_{\mathfrak{n}\le x} h(\mathfrak{n})a_{\mathfrak{n}} \ll \frac{(\log z)^2 \log\log x}{\log x} \ll \frac{(\log\log x)^5(\log\log\log x)}{\log x}.$$

It is easy to check that the factor $\log\log\log x$ above can be replaced by any increasing function $f(x)$ such that $\lim_{x\to\infty} f(x) = \infty$.

3.6.5 Background and references for axioms

Let $f(x,y) \in \mathbb{Z}[x,y]$ be an irreducible homoegeneous cubic polynoial. By [HBM], Lemma 2.1, we can construct a number field $K/\mathbb{Q}$ of degree $\deg(K/\mathbb{Q}) = 3$ and two elements $\omega_1, \omega_2 \in \mathfrak{O}_K$ linearly independent over $\mathbb{Z}$ such that

$$f(x,y) = N_{K/\mathbb{Q}}(x\omega_1 + y\omega_2)N\mathfrak{d}^{-1},$$

where $\mathfrak{d}$ is the ideal of $\mathfrak{O}_K$ generated by ω_1 and ω_2. By [HBM], Lemmas 2.2 and 2.3, there is a fixed rational integer k_0 such that $(x\omega_1 + y\omega_2)\mathfrak{d}^{-1}$ is always an element of $\mathcal{R}$, where $\mathcal{R}$ is as in (3.6.13); moreover,

$$\mu_R((x\omega_1 + y\omega_2)\mathfrak{d}^{-1}) = \mu(f(x,y)).$$

Given $\eta, \upsilon > 0$ and a lattice $L \subset \mathbb{Z}^2$, we define

$$\begin{aligned} S &= [X, (1+\eta)X] \times [\upsilon X, \upsilon(1+\eta)X] \\ \mathcal{A}_{L,S,\omega_i} &= \{(x\omega_1 + y\omega_2)\mathfrak{d}^{-1} : (x,y) \in L \cap S,\ \gcd(x,y) = 1\}. \end{aligned} \tag{3.6.26}$$

Then

$$\sum_{\substack{(x,y)\in L\cap S \\ \gcd(x,y)=1}} \mu(f(x,y)) = \sum_{\mathfrak{n}\in\mathcal{A}_{L,S,\omega_i}} \mu_{\mathcal{R}}(\mathfrak{n}).$$

Hence it is natural to define

$$a_{\mathfrak{n}} = \begin{cases} 1 & \text{if } \mathfrak{n} \in \mathcal{A}_{L,S,\omega_i}, \\ 0 & \text{otherwise.} \end{cases}$$

Let $x_0 = \max_{\mathfrak{a} \in \mathcal{A}_{L,s,\omega_i}} N\mathfrak{a} = X^3(1 + O(\eta))$. For $x \leq x_0$, let $A(x) = \sum_{N\mathfrak{n} \leq x} a_{\mathfrak{n}}$. Clearly

$$A(x) \sim \frac{\nu \eta^2 X^2}{\zeta(2)[\mathbb{Z}^2 : L]} \prod_{\substack{p \mid [\mathbb{Z}^2 : L] \\ L \cap p\mathbb{Z}^2 = \emptyset}} (1 - p^{-2})^{-1} \prod_{\substack{p \mid [\mathbb{Z}^2 : L] \\ L \cap p\mathbb{Z}^2 \neq \emptyset}} (1 + p^{-1})^{-1},$$

provided that L is not contained in any set of the form $p\mathbb{Z}^2$; if $L \subset p\mathbb{Z}^2$,then $A(x) = 0$ and all of our results are trivial.

Assume

$$\begin{aligned} -\log\log N \ll \log \upsilon \ll \log\log N, \\ \log \eta \gg -\log\log N, \\ \eta / \min(\upsilon, \upsilon^{-1}) = o(1), \end{aligned} \tag{3.6.27}$$

where the second restriction on η is enough for us to avoid associated elements in $\mathfrak{O}_K$.

Axioms (3.6.14)-(3.6.17) are proven for $L = \mathbb{Z}^2$, $\upsilon = 1$ in [HBM], sections 2–3; they are proven for general L in [HBM2], in a slightly different formulation. Since the bound (3.6.17) can absorb powers of $\log x$, and the introduction of $\upsilon \neq 1$ does not require any change in the proofs, and the bounds are uniform for $[\mathbb{Z} : L] \ll (\log N)^B$, $B > 0$ arbitrary. Axiom (3.6.19) is clear. The bilinear axiom is proven in subsection 3.6.6 under the condition (3.6.29). It remains to be seen that all linear combinations of the form (3.6.21) satisfy (3.6.29). Thanks to the standard zero-free regions for Hecke L-functions (see Lemma 3.2.3) we know that $\mu_{\mathcal{R}}$ satisfies (3.6.29) for $[\mathbb{Z}^2 : L] \ll (\log N)^B$ (and the far stronger bound $\ll xe^{-(\log x)^{3/5}/(\log\log x)^{1/5}}$ as well.) It then follows by the fundamental lemma of sieve theory that the function $\mu'_{\mathcal{R}}$ satisfies

(3.6.29) as well. To see (3.6.29) for linear combinations, note simply that

$$\sum_{n\le x}\left(\sum_{d|n} c_d\mu(n/d > n^{1/\kappa})\right) = \sum_{d\le x^{1-1/\kappa}} c_d \sum_{d^{(1-1/\kappa)^{-1}-1}\le m\le x/d} \mu(m)$$

In each inner sum, $x/d > x^{1/\kappa}$, and thus $\log(x/d) \gg \log x$. Hence we bound the inner sum by $C(x/d)(\log x)^{-B}$, C independent of d, and obtain a total bound of at most

$$Cx(\log x)^{-B+1}.$$

3.6.6 The bilinear condition

This subsection is a summarized paraphrase of [H-B], pp. 66–83, and [HBM], pp. 275–284. This rephrasing is necessary because the said references carry their argument for a specific function, whose special properties they use in ultimately inessential ways.

We recapitulate the framework set out in [HBM], p. 258 and p. 277. We let $K/\mathbb{Q}$ be a number field of degree $\deg(K/\mathbb{Q}) = 3$. We are given $\omega_1, \omega_2 \in \mathfrak{O}_K$ linearly independent over $\mathbb{Z}$. Let $\mathfrak{d} \in \mathfrak{O}_K\omega_1 + \mathfrak{O}_K\omega_2$. Let δ be an arbitrary element of $\mathcal{I}^{-1}(\mathfrak{d})$, that is, an ideal number corresponding to $\mathfrak{d}$.

Every class $A \in \mathcal{C}_1(K)$ is a $\mathbb{Z}$-module and as such has a basis $\{w_{A,1}, \cdots, w_{A,3}\}$ consisting of elements of $\mathcal{I}(\mathfrak{O}_K)^\times$. For $A_0 = \mathrm{cl}\,\delta^{-1}$, we can choose $\{w_{A_0,1}, w_{A_0,2}, w_{A_0,3}\}$ so that $\omega_1\delta^{-1} = w_{A_0,1}$ and $\omega_2\delta^{-1} = zw_{A_0,2}$ for some $z \in \mathbb{Z}$. For other classes $A \in \mathcal{C}_1(K)$ we make the choice of basis $\{w_{A,1}, \cdots, w_{A,3}\}$ arbitrarily.

Let $\beta \in \mathcal{I}(\mathfrak{O}_K)^\times$. Let $A_\beta = \mathrm{cl}(\beta\delta)^{-1}$. Write

$$\beta w_{A_\beta,1} = q_{11}w_{A_0,1} + q_{12}w_{A_0,2} + q_{13}w_{A_0,3}$$

$$\beta w_{A_\beta,2} = q_{21}w_{A_0,1} + q_{22}w_{A_0,2} + q_{23}w_{A_0,3}$$

$$\beta w_{A_\beta,3} = q_{31}w_{A_0,1} + q_{32}w_{A_0,2} + q_{33}w_{A_0,3},$$

where $q_{ij} \in \mathbb{Z}$. Define $h(\beta)$ to be $\hat{\beta} = (q_{13}, q_{23}, q_{33}) \in \mathbb{Z}^3$.

We have thus defined a map $h : \mathcal{I}(\mathfrak{O}_K)^\times \to \mathbb{Z}^3$. For any ideal class $A \in \mathcal{C}_1(K)$, the restriction $h_{|A} : A \to \mathbb{Z}^3$ is a $\mathbb{Z}$-linear map whose image is of finite index in $\mathbb{Z}^3$.

We say that $\vec{a} = (a_1, a_2, a_3) \in \mathbb{R}^3$ is *primitive* if $\gcd(a_1, a_2, a_3) = 1$. Let $\vec{a}, \vec{b} \in \mathbb{R}^3$. By $\vec{a} \times \vec{b}$ we mean the *cross product*

$$\vec{a} \times \vec{b} = (a_2b_3 - a_3b_2, a_3b_1 - a_1b_3, a_1b_2 - a_2b_1).$$

Note that, if $\vec{a}$ and $\vec{b}$ are primitive and n is a non-zero integer, we have $\vec{a} \times \vec{b} \in n\mathbb{Z}^3$ if and only if $\vec{b} \equiv \lambda\vec{a} \bmod n$ for some $\lambda \in (\mathbb{Z}/n)^*$.

By a *cube* $C \subset \mathbb{R}^3$ of side ℓ we mean a set of the form $(x, x+\ell] \times (y, y+\ell] \times (z, z+\ell]$.

For $\vec{a} \in \mathbb{Z}^2$, let $\mathfrak{A}_{\vec{a}} = (a_1\omega_1 + a_2\omega_2)\mathfrak{d}^{-1} \in I_K$. Given $\eta, \upsilon > 0$ and a lattice $L \subset \mathbb{Z}^2$, let

$$\begin{aligned}
\Psi_{L,\eta,\upsilon}(\vec{a}) &= [\vec{a} \in L \cap ([X, (1+\eta)X] \times [\upsilon X, \upsilon(1+\eta)X])] \\
\mathcal{A}'_{L,\eta,\upsilon} &= \{\mathfrak{A}_{\vec{a}} : \vec{a} \in L \cap ([X, (1+\eta)X] \times [\upsilon X, \upsilon(1+\eta)X])\} \\
\mathcal{A}_{L,\eta,\upsilon} &= \{\mathfrak{A}_{\vec{a}} : \vec{a} \in L \cap ([X, (1+\eta)X] \times [\upsilon X, \upsilon(1+\eta)X]),\ \gcd(a_1, a_2) = 1\}.
\end{aligned}$$

Let $\mathcal{Q} \in I_K$ be the set of all ideals in I_K that are not divisible by any rational prime. In the following, we use α, β to denote ideal numbers and $\mathfrak{a}$, $\mathfrak{b}$ to denote ideals.

Lemma 3.6.4. *Let $K/\mathbb{Q}$ be a number field of degree 3. Let $\omega_1, \omega_2 \in \mathfrak{O}_K$ be linearly independent over $\mathbb{Z}$. Let $f, g : I_K \to \mathbb{R}$ be given with*

$$|f(\mathfrak{a})|, |g(\mathfrak{a})| \ll \tau^\kappa(\mathfrak{a}). \tag{3.6.28}$$

Assume that, for any $B_1, B_2 > 0$,

$$\sum_{\substack{\vec{b}\in C\\ \vec{b}\in L\cap h(A)}} g(\mathcal{I}(h_A^{-1}(\vec{b}))) \ll_{B_1,B_2} \mathrm{vol}(C)(\log X)^{-B_2} \tag{3.6.29}$$

for any class $A \in \mathcal{C}_1(K)$, any cube $C \subset [X, 2X]^3$ of side $\ell \geq X(\log X)^{-B_1}$, and any lattice coset L of index $[\mathbb{Z}^2 : L] \leq (\log X)^{B_1}$. Let

$$\begin{aligned} -\log\log N \ll \log \upsilon \ll \log\log N,\\ \log\eta \gg -\log\log N,\\ \eta/\min(\upsilon,\upsilon^{-1}) = o(1), \end{aligned} \tag{3.6.30}$$

Then, for any $B > 0$,

$$\sum_{\substack{\mathfrak{a}\mathfrak{b}\in\mathcal{A}'_{L,\eta,\upsilon}\\ X(\log X)^T < N\mathfrak{b}\leq X^{3/2}(\log X)^{-T}\\ \mathfrak{a},\mathfrak{b}\in\mathcal{Q}}} f(\mathfrak{a})g(\mathfrak{b}) \ll X^2(\log X)^{-B}, \tag{3.6.31}$$

where the constant T and the implied constant in (3.6.31) depend only on κ, B and the implied constants in (3.6.28)–(3.6.30).

Proof. The argument is nearly the same as that in [HBM], pp. 278–283. Let $X(\log X)^T < V < X^{3/2}(\log X)^{-T}$. Define

$$S_0 = \sum_{\substack{\mathfrak{a}\mathfrak{b}\in\mathcal{A}'_{L,\eta,\upsilon,\omega_i}\\ V<N\mathfrak{b}\leq 2V\\ \mathfrak{a},\mathfrak{b}\in\mathcal{Q}}} f(\mathfrak{a})g(\mathfrak{b}). \tag{3.6.32}$$

(Notice that S_0 is not the same as $\sum_9(V)$ in [HBM], (6.2); instead, what we have is the first summand on the right hand of [HBM], (6.2). We are avoiding the argument at the beginning of §11 in [H-B], as it implicitly uses a lacunarity condition that we

do not demand.) We can rewrite (3.6.32) as

$$S_0 = \sum_{\substack{\phi(\vec{a})=\delta\alpha\beta,\, \mathcal{I}(\alpha)\in\mathcal{Q} \\ \vec{a}\in\mathbb{Z}^2,\, V<N\beta\leq 2V}} f(\mathcal{I}(\alpha))G_0(\beta)\Psi_{L,\eta}(\vec{a}),$$

where $\phi(\vec{a}) = a_1\omega_1 + a_2\omega_2$,

$$G(\beta) = \begin{cases} g(\mathcal{I}(\beta)) & \text{if } \mathcal{I}(\beta)\in\mathcal{Q}_0 \\ 0 & \text{otherwise,} \end{cases} \qquad G_0(\beta) = \begin{cases} G(\beta) & \text{if } \beta\in\mathcal{Q}_0 \\ 0 & \text{otherwise,} \end{cases}$$

and $\mathcal{Q}_0$ is defined as in [HBM], p. 278. (In short, $\mathcal{Q}_\prime$ is the set of all ideal numbers β satisfying $\mathcal{I}(\beta)\in\mathcal{Q}$ and a geometrical condition necessary to exclude multiplication by units.) In the following we will use κ to mean a constant depending only on the value of κ in the statement and the implied constants in (3.6.28)–(3.6.30). We now apply Cauchy's inequality:

$$\begin{aligned} S_0^2 &\ll \sum_{\substack{\alpha \\ \mathcal{I}(\alpha)\in\mathcal{Q}}} \left| \sum_{\substack{\phi(\vec{a})=\delta\alpha\beta \\ \vec{a}\in\mathbb{Z}^2,\, V<N\beta\leq 2V}} G_0(\beta)\Psi_{L,\eta}(\vec{a}) \right|^2 \cdot \sum_{\substack{\mathfrak{a} \\ N\mathfrak{a}\ll X^3/V}} |f(\mathfrak{a})|^2 \\ &\ll X^3V^{-1}(\log X)^\kappa \sum_{\substack{\alpha \\ \mathcal{I}(\alpha)\in\mathcal{Q}}} \left| \sum_{\substack{\phi(\vec{a})=\delta\alpha\beta \\ \vec{a}\in\mathbb{Z}^2,\, V<N\beta\leq 2V}} G_0(\beta)\Psi_{L,\eta}(\vec{a}) \right|^2. \end{aligned} \tag{3.6.33}$$

As in [HBM], p. 279, we expand (3.6.33) and remove the diagonal terms:

$$S_0 \ll (X^3V^{-1}(\log X)^\kappa \cdot (S_1 + O(X^2(\log X)^\kappa)))^{1/2},$$

where

$$S_1 = \sum_{\substack{\beta_1 \neq \beta_2,\, \vec{a}_i \in \mathbb{Z}^2 \\ V < N\beta_i \leq 2V, i=1,2}} G_0(\beta_1) G_0(\beta_2) \Psi_{L,\eta}(\vec{a}_1) \Psi_{L,\eta}(\vec{a}_2) \psi(\vec{a}_1, \vec{a}_2, \beta_1, \beta_2)$$

with

$$\psi(\vec{a}_1, \vec{a}_2, \beta_1, \beta_2) = \#\{\alpha : \mathcal{I}(\alpha) \in \mathcal{Q},\ \phi(\vec{a}_i) = \delta\alpha\beta_i \text{ for } i = 1, 2\}.$$

As in [HBM], Lemma 6.2, we remove a small area and obtain

$$S_0 \ll X^2 Y^{-1/2} (\log X)^\kappa + X^{3/2} V^{-1/2} S_2^{1/2}$$

with

$$S_2 = \sum_{\substack{\vec{a}_i \in \mathbb{Z}^2,\, \beta_i \in A \\ V < N\beta_i \leq 2V \\ d(h(\beta_1) \times h(\beta_2)) > V X^{-1} Y^{-1}}} G_0(\beta_1) G_0(\beta_2) \Psi_{L,\eta}(\vec{a}_1) \Psi_{L,\eta}(\vec{a}_2) \psi(\vec{a}_1, \vec{a}_2, \beta_1, \beta_2),$$

where A is a class of ideal numbers, Y is a parameter between 1 and $(\log X)^{T/3}$ chosen at our pleasure, and $d((c_1, c_2, c_3)) = \gcd(c_1, c_2, c_3)$. (Here we have implicitly used Lemma 6.1 of [HBM].)

We can now proceed as in [HBM], pp. 280–282, and obtain the following analogue of [HBM], (6.9):

$$S_0 \ll X^2 Y^{-1/2} (\log X)^\kappa + X^{3/2} V^{-1/2} Y^7 S_3^{1/2} (\log X)^\kappa,$$

with

$$S_3 = \sum_{d_1 \in I} \left| \sum_{\substack{\beta_i \in B \\ \hat{\beta}_i \in C_i \cap L_{d_1, i} \\ d(\hat{\beta}_1 \times \hat{\beta}_2) = d}} G(\beta_1) G(\beta_2) \right|,$$

where $A \in \mathcal{C}_1(K)$ is a class of ideal numbers, I is an interval contained in $[VX^{-1}, \infty]$, the lattices $L_{d,i}$ have indices $[\mathbb{Z}^3 : L_{d,i}] | [\mathbb{Z}^3 : L]^3$, and $C_1, C_2 \subset [VX^{-1}, 2VX^{-1}]^3$ are cubes of side about $VX^{-1}(\log X)^{-2T/3}$. As in [HBM], (6.0)–(6.12), we can conclude that

$$S_0 \ll X^2 Y^{-1/2} (\log X)^\kappa + X^{3/2} V^{-1/2} Y^7 S_4^{1/2} (\log X)^\kappa,$$

where

$$S_4 = \sum_{\substack{d_1 \in I \\ d_1 d < d_0}} \left| \sum_{\substack{\beta_i \in B \\ \hat{\beta}_i \in C_i \cap L_{d_1,i} \\ d_1 d | \hat{\beta}_1 \times \hat{\beta}_2}} G(\beta_1) G(\beta_2) \right|$$

with $d_0 = X^{-1} V Y^{15} + V^{1/6}$. We can bound S_4 by means of a large-sieve argument as in [H-B], p. 78–83, and [HBM], p. 283; the contribution from small moduli is estimated by (3.6.29). We obtain

$$\begin{aligned} S_4 \ll & XV[\mathbb{Z}^2 : L]^\kappa (\log X)^\kappa \\ & \cdot (Y^\kappa (\log X)^{-T/2} + Y (\log X)^{-B_1/2} + Y (\log X)^{4B_1} (\log X)^{-B_2}), \end{aligned}$$

where B_1 and B_2 are arbitrarily large. (See [HBM2] for an optimization of the exponent κ in $[\mathbb{Z}^2 : L]^\kappa$.) Set $Y = (\log X)^{2B+2\kappa+2}$, $T = 1000\kappa^2(B + \kappa + 1)$ (say), $B_1 = T$, $B_2 = 9B_1$. Then

$$S_0 \ll X^2 (\log X)^{-(B+1)}.$$

The statement follows immediately.

Corollary 3.6.5. *Let $K/\mathbb{Q}$ be a number field of degree 3. Let $\omega_1, \omega_2 \in \mathfrak{O}_K$ be linearly independent over $\mathbb{Z}$. Let $\eta, \upsilon \in \mathbb{R}^+$, $f, g : I_K \to \mathbb{R}$ satisfy conditions (3.6.28)–(3.6.30). Assume furthermore that*

$$\mathfrak{p} | \mathfrak{a}, \mathfrak{q} | \mathfrak{b}, \mathfrak{p}, \mathfrak{q} \leq (\log x)^{10} \Rightarrow f(\mathfrak{a}) g(\mathfrak{b}) = 0.$$

Then

$$\sum_{\substack{\mathfrak{a}\mathfrak{b}\in\mathcal{A}_{L,\eta,\upsilon} \\ X(\log X)^T<N\mathfrak{b}\leq X^{3/2}(\log X)^{-T} \\ \mathfrak{a},\mathfrak{b}\in\mathcal{Q}}} f(\mathfrak{a})g(\mathfrak{b}) \ll X^2(\log X)^{-B}, \tag{3.6.34}$$

where the constant T and the implied constant in (3.6.31) depend only on κ, B and the implied constants in (3.6.28)–(3.6.30).

By Lemma 3.6.4 and [H-B], p 67. We are simply removing the coprimality condition on $\mathfrak{a}$ and $\mathfrak{b}$, given that $\mathfrak{a}$ and $\mathfrak{b}$ are still kept from having small common factors. □

3.7 Final remarks and conclusions

In section 3.6, we used the small-boxes formalism of [H-B] and [HBM] rather than our own convex-subset formalism. It is easy to see that boxes such as S in (3.6.26) satisfying (3.6.27) can cover convex sets with an error of at most $x(\log x)^{-B}$, where B is arbitrarily large.

We saw it fit to work with λ in sections 3.4 and 3.5, and with μ in section 3.6. (The first choice was due to complete multiplicativity, the second one to symmetry.) Thanks to Propositions 4.2.17 and A.1.2 for $\deg P = 3$, a result on λ implies one for μ, and vice versa, without any degradation in our bounds. Notice, lastly, that the condition $\gcd(x, y) = 1$ implicit in section 3.6 (see $\mathcal{A}_{L,S,\omega_i}$ in (3.6.26)) can be removed as in Lemma 2.4.4.

We collect all our results on cubic polynomials in the following statement.

Theorem 3.7.1. *Let $f(x, y) \in \mathbb{Z}[x, y]$ be a homogeneous polynomial of degree 3. Let α be the Möbius function ($\alpha = \mu$) or the Liouville function ($\alpha = \lambda$). Let S be a convex subset of $[-N, N]^2$. Let $L \subset \mathbb{Z}^2$ be a lattice coset of index $[\mathbb{Z}^2 : L] \leq (\log N)^A$,*

where A is an arbitrarily high constant. Then

$$\sum_{(x,y)\in S\cap L} \alpha(f(x,y)) \ll \begin{cases} \frac{(\log\log N)^5(\log\log\log N)}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]} + \frac{N^2}{(\log N)^A} & \text{if } f \text{ is irreducible,} \\ \frac{\log\log N}{\log N}\frac{\mathrm{Area}(S)}{[\mathbb{Z}^2:L]} + \frac{N^2}{(\log N)^A} & \text{if } f \text{ is reducible,} \end{cases}$$

where the implied constant depends only on f and on A.

Chapter 4

The square-free sieve

> They sought it with thimbles, they sought it with care;
> They pursued it with forks and hope;
> They threatened its life with a railway–share;
> They charmed it with smiles and soap.
>
> Lewis Carroll, *The Hunting of the Snark*

A *square-free sieve* is a result that gives an upper bound for how often a square-free polynomial may adopt values that are not square-free. More generally, we may wish to approximate the cardinality of the set of arguments $x_1, \ldots, x_n$ for which the largest square divisor of the value acquired by $P(x_1, \ldots, x_n)$ equals a given $\mathfrak{d}$, or, as in Chapter 2, we may wish to control the behavior of a function depending on $\mathrm{sq}(P(x_1, \ldots, x_n))$.

We may aim at obtaining an asymptotic expression

$$\text{main term } + O(\text{error term}), \tag{4.0.1}$$

where the main term will depend on the application; in general, the error term will depend only on the polynomial P in question, not on the particular quantity being estimated. We can split the error term further into one term that can be bounded

easily for any P, and a second term, say, $\delta(P)$, which may be rather hard to estimate, and which is unknown for polynomials P of high enough degree. Given this framework, the strongest results in the literature may be summarized as follows:

$\deg_{\text{irr}}(P)$	$\delta(P(x))$	$\delta(P(x,y))$
1	$\sqrt{N}$	1
2	$N^{2/3}$	N
3	$N/(\log N)^{1/2}$	$N^2/\log N$
4		$N^2/\log N$
5		$N^2/\log N$
6		$N^2/(\log N)^{1/2}$

Here $\deg_{\text{irr}}(P)$ denotes the degree of the largest irreducible factor of P. The second column gives $\delta(P)$ for polynomials $P \in \mathbb{Z}[x]$ of given $\deg_{\text{irr}}(P)$, whereas the third column refers to homogeneous polynomials $P \in \mathbb{Z}[x,y]$. The trivial estimates would be $\delta(P(x)) \leq N$ and $\delta(P(x,y)) \leq N^2$. See Appendix A.1 for attributions.

Our task can be divided into two halves. The first one, undertaken in section 4.2, consists in estimating all terms but $\delta(N)$. We do as much in full generality for any P, over any number field, for that matter. The second half regards bounding $\delta(N)$. We improve on all estimates known for $3 \leq \deg P \leq 5$:

$\deg_{\text{irr}}(P)$	$\delta(P(x))$	$\delta(P(x,y))$
3	$N/(\log N)^{0.5718\cdots}$	$N^{3/2}/\log N$
4		$N^{4/3}(\log N)^A$
5		$N^{(5+\sqrt{113})/8+\epsilon}$

Most of our improvements hinge on a change from a local to a global perspective. Such previous work in the field as was purely sieve-based can be seen as an series of purely local estimates on the density of points on curves of non-zero genus. Our techniques involve a mixture of sieves, elliptic curves, sphere packings, and some of the methods described in the epigraph.

4.1 Notation

Let n be a non-zero integer. We write $\tau(n)$ for the number of positive divisors of n, $\omega(n)$ for the number of the prime divisors of n, and $\mathrm{rad}(n)$ for the product of the prime divisors of n. For any $k \geq 2$, we write $\tau_k(n)$ for the number of k-tuples $(n_1, n_2, \ldots, n_k) \in (\mathbb{Z}^+)^k$ such that $n_1 \cdot n_2 \cdot \cdots \cdot n_k = |n|$. Thus $\tau_2(n) = \tau(n)$. We adopt the convention that $\tau_1(n) = 1$. We let

$$\mathrm{sq}(n) = \prod_{p^2|n} p^{v_p(n)-1}.$$

We call a rational integer n *square-full* if $p^2|n$ for every prime p dividing n. Given any non-zero rational integer D, we say that n is *(D)-square-full* if $p^2|n$ for every prime p that divides n but not D.

We denote by $\mathfrak{O}_K$ the ring of integers of a global or local field K. We let I_K be the semigroup of non-zero ideals of $\mathfrak{O}_K$. Given a non-zero ideal $\mathfrak{a} \in I_K$, we write $\tau_K(\mathfrak{a})$ for the number of ideals dividing $\mathfrak{a}$, $\omega_K(\mathfrak{a})$ for the number of prime ideals dividing $\mathfrak{a}$, and $\mathrm{rad}_K(\mathfrak{a})$ for the product of the prime ideals dividing $\mathfrak{a}$. Given a positive integer k, we write $\tau_{K,k}(\mathfrak{a})$ for the number of k-tuples $(\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_k)$ of ideals of $\mathfrak{O}_K$ such that $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2 \cdots \mathfrak{a}_k$. Thus $\tau_2(\mathfrak{a}) = \tau(\mathfrak{a})$. We let

$$\mathrm{sq}_K(\mathfrak{a}) = \begin{cases} \prod_{\mathfrak{p}^2|\mathfrak{a}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})-1} & \text{if } \mathfrak{a} \neq 0, \\ 0 & \text{if } \mathfrak{a} = 0, \end{cases}$$

$$\mu_K(\mathfrak{a}) = \begin{cases} \prod_{\mathfrak{p}|\mathfrak{a}}(-1) & \text{if } \mathrm{sq}_K(\mathfrak{a}) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

We define $\rho(\mathfrak{a})$ to be the positive integer generating $\mathfrak{a} \cap \mathbb{Z}$.

When we say that a polynomial $f \in \mathfrak{O}_K[x]$ or $f \in K[x]$ is *square-free*, we always mean that f is square-free as an element of $K[x]$. In other words, we say that $f \in \mathbb{Z}[x]$

is *square-free* if there is no polynomial $g \in \mathbb{Z}[x]$ such that $\deg g \geq 1$ and $g|f$. See section 2.2 for the definitions of the resultant Res and the discriminant Disc.

Given an elliptic curve E over $\mathbb{Q}$, we write $E(\mathbb{Q})$ for the set of rational (that is, $\mathbb{Q}$-valued) points of E. We denote by $\mathrm{rank}(E)$ the algebraic rank of $E(\mathbb{Q})$.

4.2 Sieving

4.2.1 An abstract square-free sieve

Lemma 4.2.1. *Let K be a number field. Let $\{S_{\mathfrak{a}}\}_{\mathfrak{a}\in I_K}$ be a collection of finite sets, one for each non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}_K$. Let a map $\phi_{\mathfrak{a}_1,\mathfrak{a}_2} : S_{\mathfrak{a}_2} \to S_{\mathfrak{a}_1}$ be given for any non-zero ideals $\mathfrak{a}_1$, $\mathfrak{a}_2$ such that $\mathfrak{a}_1|\mathfrak{a}_2$. Assume $\phi_{\mathfrak{a}_1,\mathfrak{a}_2} \circ \phi_{\mathfrak{a}_2,\mathfrak{a}_3} = \phi_{\mathfrak{a}_1,\mathfrak{a}_3}$ for all $\mathfrak{a}_1$, $\mathfrak{a}_2$, $\mathfrak{a}_3$ such that $\mathfrak{a}_1|\mathfrak{a}_2|\mathfrak{a}_3$. Let $\{f_{\mathfrak{a}}\}_{\mathfrak{a}\in I_K}$, $f_{\mathfrak{a}} : S_{\mathfrak{a}} \to \mathbb{C}$ be given with $|f_{\mathfrak{a}}(r)| \leq 1$ for all $\mathfrak{a} \in I_K$ and all $r \in S_{\mathfrak{a}}$. Let $\{g_{\mathfrak{a}}\}_{\mathfrak{a}\in I_K}$, $g_{\mathfrak{a}} : S_{\mathfrak{a}} \to \mathbb{C}$ be such that*

$$\sum_{\mathfrak{a}\in\mathfrak{I}_{\mathfrak{K}}} \sum_{r\in S_{\mathfrak{a}}} |g_{\mathfrak{a}}(r)|$$

converges. Write

$$s_{\mathfrak{d}} = \sum_{\substack{\mathfrak{a}\in\mathfrak{I}_{\mathfrak{K}} \\ \mathfrak{d}|\mathfrak{a}}} \sum_{r\in S_{\mathfrak{a}}} |g_{\mathfrak{a}}(r)|,$$

$$t_{\mathfrak{d}}(r) = \sum_{\substack{\mathfrak{a} \\ \mathfrak{d}|\mathfrak{a}}} \sum_{\substack{r'\in S_{\mathfrak{a}} \\ \phi_{\mathfrak{d},\mathfrak{a}}(r')=r}} g_{\mathfrak{a}}(r').$$

Let $\gamma : I_K \to \mathbb{Z}^+$ be a map such that $\gamma(\mathfrak{d}_1) \leq \gamma(\mathfrak{d}_1\mathfrak{d}_2) \leq \gamma(\mathfrak{d}_1)\gamma(\mathfrak{d}_2)$ for all $\mathfrak{d}_1, \mathfrak{d}_2 \in I_K$. Then, for any positive integer M,

$$\begin{aligned}\sum_{\mathfrak{a}\in I_K} \sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r) g_{\mathfrak{a}}(r) \leq \sum_{\gamma(\mathfrak{d})\leq M} \sum_{r\in S_{\mathfrak{d}}} \left(\sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{d}}(r)) \right) t_{\mathfrak{d}}(r) \\ + 2 \sum_{\substack{\mathfrak{d}\in I_K \\ M<\gamma(\mathfrak{d})\leq M^2}} \tau_{K,3}(\mathfrak{d}) s_{\mathfrak{d}} + 2 \sum_{\substack{\mathfrak{p} \text{ prime} \\ \gamma(\mathfrak{p})>M}} s_{\mathfrak{p}}.\end{aligned} \tag{4.2.1}$$

Proof. Let $\sigma(\mathfrak{a}) = \prod_{\mathfrak{p}|\mathfrak{a},\, \gamma(\mathfrak{p})\le M} \mathfrak{p}^{v_{\mathfrak{p}}(a)}$. By Möbius inversion, for any $r \in S_{\mathfrak{a}}$,

$$\sum_{\mathfrak{d}|\mathfrak{a}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) = f_{\mathfrak{a}}(r),$$

$$\sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \mathfrak{p}|\mathfrak{d}\Rightarrow\gamma(\mathfrak{p})\le M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) = f_{\sigma(\mathfrak{a})}(\phi_{\sigma(\mathfrak{a}),\mathfrak{a}}(r)).$$

Hence

$$\begin{aligned}\sum_{\mathfrak{a}} \sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r) g_{\mathfrak{a}}(r) = &\sum_{r} \sum_{r\in S_{\mathfrak{a}}} (f_{\mathfrak{a}}(r) - f_{\sigma(\mathfrak{a})}(\phi_{\sigma(\mathfrak{a}),\mathfrak{a}}(r))) g_{\mathfrak{a}}(r) \\ &+ \sum_{\mathfrak{a}} \sum_{r\in S_{\mathfrak{a}}} w_{\mathfrak{a},r} g_{\mathfrak{a}}(r) \\ &+ \sum_{\gamma(\mathfrak{d})\le M} \left(\sum_{r\in S_{\mathfrak{d}}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) \right) t_{\mathfrak{d}}(r),\end{aligned}$$

where we write

$$w_{\mathfrak{a},r} = \sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \mathfrak{p}|\mathfrak{d}\Rightarrow\gamma(\mathfrak{p})\le M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) - \sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \gamma(\mathfrak{d})\le M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)).$$

Since $\mathfrak{a} = \sigma(\mathfrak{a})$ unless $\mathfrak{a}$ is divisible by a prime $\mathfrak{p}$ with $\gamma(\mathfrak{p}) > M$, we know that

$$\sum_{r} \sum_{r\in S_{\mathfrak{a}}} (f_{\mathfrak{a}}(r) - f_{\sigma(\mathfrak{a})}(\phi_{\sigma(\mathfrak{a}),\mathfrak{a}}(r))) g_{\mathfrak{a}}(r) \le \sum_{\substack{\mathfrak{p} \text{ prime} \\ \gamma(\mathfrak{p})>M}} s_{\mathfrak{p}}.$$

Now take $\mathfrak{a}$, r such that

$$\sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \mathfrak{p}|\mathfrak{d}\Rightarrow\gamma(\mathfrak{p})\le M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) \neq \sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \gamma(\mathfrak{d})\le M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)). \tag{4.2.2}$$

This can happen only if $\gamma(\sigma(\mathfrak{a})) > M$. Let $\mathfrak{d}$ be a divisor of $\mathfrak{a}$ with $\gamma(\mathfrak{d}) \le M$. We would like to show that there is a divisor $\mathfrak{d}'$ of $\mathfrak{a}$ such that $\mathfrak{d}|\mathfrak{d}'$ and $M < \gamma(\mathfrak{d}') \le$

M^2. Since $\gamma(\mathfrak{d}) \leq M$, all prime divisors $\mathfrak{p}$ of $\mathfrak{d}$ obey $\gamma(\mathfrak{p}) \leq M$, and thus $\mathfrak{d}|\sigma(\mathfrak{a})$. Write $\sigma(\mathfrak{a}) = \mathfrak{d}\mathfrak{p}_1 \cdots \mathfrak{p}_k$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_\ell$ are not necessarily distinct. Let $\mathfrak{a}_0 = \mathfrak{d}$. For $1 \leq i \leq k$, let $\mathfrak{a}_i = \mathfrak{d}\mathfrak{p}_1 \cdots \mathfrak{p}_i$. Then $\gamma(\mathfrak{a}_0) \leq M$, $\gamma(\mathfrak{a}_k) = \gamma(\sigma(\mathfrak{a})) > M$ and $\gamma(\mathfrak{a}_{i+1}) \leq \gamma(\mathfrak{a}_i)\gamma(\mathfrak{p}_i) \leq \gamma(\mathfrak{a}_i) \cdot M$ for every $1 \leq i < k$. Hence there is an $0 \leq i \leq k$ such that $M < \gamma(\mathfrak{a}_i) \leq M^2$. Since $\mathfrak{d}|\sigma(\mathfrak{a})_i$ and $\mathfrak{a}_i|\sigma(\mathfrak{a})$, we can set $\mathfrak{d}' = \mathfrak{a}_i$.

Now bound the right hand side of (4.2.2) trivially:

$$\sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \gamma(\mathfrak{d}) \leq M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) \leq \sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \gamma(\mathfrak{d}) \leq M}} \tau_K(\mathrm{rad}(\mathfrak{d})).$$

By the foregoing discussion,

$$\sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \gamma(\mathfrak{d}) \leq M}} \tau_K(\mathrm{rad}(\mathfrak{d})) \leq \sum_{\substack{\mathfrak{d}'|\mathfrak{a} \\ M < \gamma(\mathfrak{d}') \leq M^2}} \sum_{\mathfrak{d}|\mathfrak{d}'} \tau_K(\mathrm{rad}(\mathfrak{d})) = \sum_{\substack{\mathfrak{d}'|\mathfrak{a} \\ M < \gamma(\mathfrak{d}') \leq M^2}} \tau_{K,3}(\mathfrak{d}').$$

Since

$$\left| \sum_{\substack{\mathfrak{d}|\mathfrak{a} \\ \mathfrak{p}|\mathfrak{d} \Rightarrow \gamma(\mathfrak{p}) \leq M}} \sum_{\mathfrak{d}'|\mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{a}}(r)) \right| = |f(\sigma(\mathfrak{a}))| \leq 1$$

and since for all terms such that $\gamma(\sigma(\mathfrak{a})) > M$ we have

$$\sum_{\substack{\mathfrak{d}'|\mathfrak{a} \\ M < \gamma(\mathfrak{d}') \leq M^2}} \tau_{K,3}(\mathfrak{d}') \geq 1,$$

we can conclude that

$$\left| \sum_{\mathfrak{a}} \sum_{r \in S_{\mathfrak{a}}} w_{\mathfrak{a},r} g_{\mathfrak{a}}(r) \right|$$

is less than or equal to twice

$$\sum_{\mathfrak{a}} \sum_{r \in S_{\mathfrak{a}}} \sum_{\substack{\mathfrak{d} | \mathfrak{a} \\ M < \gamma(\mathfrak{d}) \leq M^2}} \tau_{K,3}(\mathfrak{d}) \, |g_{\mathfrak{a}}(r)|.$$

Since

$$\sum_{\mathfrak{a}} \sum_{r \in S_{\mathfrak{a}}} \sum_{\substack{\mathfrak{d} | \mathfrak{a} \\ M < \gamma(\mathfrak{d}) \leq M^2}} \tau_{K,3}(\mathfrak{d}) \, |g_{\mathfrak{a}}(r)| \leq \sum_{M < \gamma(\mathfrak{d}) \leq M^2} \tau_{K,3}(\mathfrak{d}) s_{\mathfrak{d}},$$

the result follows. □

4.2.2 Solutions and lattices

Lemma 4.2.2. *Let K be a $\mathfrak{p}$-adic field. Let $P \in \mathfrak{O}_K[x]$ be a square-free polynomial. Then*

$$P(x) \equiv 0 \bmod \mathfrak{p}^n$$

has at most $\max(|\operatorname{Disc} P|_{\mathfrak{p}}^{-1} \cdot \deg P, |\operatorname{Disc} P|_{\mathfrak{p}}^{-3})$ *roots in* $\mathfrak{O}_K/\mathfrak{p}^n$.

Proof. Let π be a prime element of K. If P is of the form $P = \pi Q$ for some $Q \in \mathfrak{O}_K[x]$, the statement follows from the statement for Q. Hence we can assume P is not of the form $P = \pi G$. Write $P = P_1 \cdot P_2 \cdot \cdots \cdot P_l$, $P_i \in \mathfrak{O}_K$, P_i irreducible.

If $n \leq 3v_{\mathfrak{p}}(\operatorname{Disc} P)$, there are trivially at most $\#(\mathfrak{O}_K/\mathfrak{p}^n) = |\mathfrak{p}^n|_{\mathfrak{p}}^{-1} \leq |\operatorname{Disc} P|_{\mathfrak{p}}^{-3}$ roots. Assume $n > 3v_{\mathfrak{p}}(\operatorname{Disc} P)$. Let x be a root of $P(x) \equiv 0 \bmod \mathfrak{p}^n$. Let P_i be a factor for which $v_{\mathfrak{p}}(P_i(x))$ is maximal. By

$$v_{\mathfrak{p}}(P'(x)) = v_{\mathfrak{p}}(\sum_j P_j'(x) \cdot P_1(x) \cdot \cdots \widehat{P_j(x)} \cdot \cdots P_n(x)) \geq \min_j (v_{\mathfrak{p}}(P(x)) - v_{\mathfrak{p}}(P_j(x))),$$

$\min(v_{\mathfrak{p}}(P'(x)), v_{\mathfrak{p}}(P(x))) \leq v_{\mathfrak{p}}(\operatorname{Disc} P)$ and $v_{\mathfrak{p}}(P(x)) > v_{\mathfrak{p}}(\operatorname{Disc} P)$, we have that

$$\min_j (v_{\mathfrak{p}}(P(x)) - v_{\mathfrak{p}}(P_j(x))) \leq v_{\mathfrak{p}}(\operatorname{Disc} P)$$

and hence

$$v_{\mathfrak{p}}(P_i(x)) \geq v_{\mathfrak{p}}(P(x)) - v_{\mathfrak{p}}(\operatorname{Disc} P) \geq n - v_{\mathfrak{p}}(\operatorname{Disc} P) \geq 2v_{\mathfrak{p}}(\operatorname{Disc} P) + 1.$$

On the other hand $\gcd(P_i(x), P_i'(x)) | \operatorname{Disc} P$, and thus $v_{\mathfrak{p}}(P_i'(x)) \leq v_{\mathfrak{p}}(\operatorname{Disc} P)$. By Hensel's lemma we can conclude that P_i is linear. Since $v_{\mathfrak{p}}(P_i(x)) \geq n - v_{\mathfrak{p}}(\operatorname{Disc} P)$, x is a root of

$$P_i(x) \equiv 0 \bmod \mathfrak{p}^{n - v_{\mathfrak{p}}(\operatorname{Disc} P)}.$$

Since P_i is linear and not divisible by $\mathfrak{p}$, it has at most one root in $\mathfrak{O}_K/\mathfrak{p}^{n-v_{\mathfrak{p}}(\operatorname{Disc} P)}$. There are at most $v_{\mathfrak{p}}(\operatorname{Disc} P)$ elements of $\mathfrak{O}_K/\mathfrak{p}^n$ reducing to this root. Summing over all i we obtain that there are at most $l \cdot v_{\mathfrak{p}}(\operatorname{Disc} P)$ roots of $P(x) \equiv 0 \bmod \mathfrak{p}^n$ in $\mathbb{Z}/\mathfrak{p}^n$. Since $l \leq \deg P$, the statement follows. □

Lemma 4.2.3. *Let K be a number field. Let $\mathfrak{m}$ be a non-zero ideal of $\mathfrak{O}_K$. Let $P \in \mathfrak{O}_K[x]$ be a square-free polynomial. Then*

$$\{x \in \mathbb{Z} : P(x) \equiv 0 \bmod \mathfrak{m}\}$$

is the union of at most $|\operatorname{Disc} P|^3 \cdot \tau_{\deg P}(\operatorname{rad}(\rho(\mathfrak{m})))$ arithmetic progressions of modulus $\rho(\mathfrak{m})$.

Proof. By Lemma 4.2.2, for every $\mathfrak{p}|\mathfrak{m}$, the equation

$$P(x) \equiv 0 \bmod \mathfrak{p}^n$$

has at most $|\operatorname{Disc} P|_{\mathfrak{p}}^{-3} \deg P$ roots in $\mathfrak{O}_K/\mathfrak{p}^n$. For any ideal $\mathfrak{a}$, the intersection of $\mathbb{Z}$ with a set of the form

$$\{x \in \mathfrak{O}_K : x \equiv x_0 \bmod \mathfrak{a}\}$$

is either the empty set or an arithmetic progression of modulus $\rho(\mathfrak{a})$. This is in

particular true for $\mathfrak{a} = \mathfrak{p}^n$; the set

$$\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}^n\}$$

is the union of at most $|\operatorname{Disc} P|_{\mathfrak{p}}^{-3} \deg P$ arithmetic progressions of modulus $\rho(\mathfrak{p}^n)$.

Now consider a rational prime p at least one of whose prime ideal divisors divides m. Write $m = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\cdots\mathfrak{p}_k^{n_k}\mathfrak{m}_0$, where $\mathfrak{p}_1, \ldots \mathfrak{p}_k | p$, $n_1 \geq n_2 \geq \cdots \geq n_k$ and $\mathfrak{m}_0$ is prime to p. The set

$$\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}\}$$

is the intersection of the sets

$$\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_j^{n_j}\}, \quad 1 \leq j \leq k.$$

At the same time, it is a disjoint union of arithmetic progressions of modulus

$$\rho(\mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}) = \rho(\mathfrak{p}_1^{n_1}).$$

Since

$$\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_1^{n_1}\}$$

is the disjoint union of at most $|\operatorname{Disc} P|_{\mathfrak{p}}^{-3} \deg P$ arithmetic progressions of modulus $\rho(\mathfrak{p}_1^{n_1})$,

$$\{x \in \mathbb{Z} : x \equiv x_0 \bmod \mathfrak{p}_1^{n_1}\cdots\mathfrak{p}_k^{n_k}\}$$

is the disjoint union of at most $|\operatorname{Disc} P|_{\mathfrak{p}}^{-3} \deg P$ arithmetic progressions of modulus $\rho(\mathfrak{p}_1^{n_1})$.

By (2.2.3) the statement follows. □

Lemma 4.2.4. *Let K be a number field. Let $\mathfrak{m}$ be a non-zero ideal of $\mathfrak{O}_K$. Let $P \in \mathfrak{O}_K[x, y]$ be a non-constant and square-free homogeneous polynomial. Then the*

set

$$S = \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1, \mathfrak{m}|P(x, y)\}$$

is the union of at most $|\operatorname{Disc} P|^3 \cdot \tau_{2\deg P}(\operatorname{rad}(\rho(\mathfrak{m})))$ *disjoint sets of the form* $L \cap \{(x, y) \in \mathbb{Z}^2 : \gcd(x, y) = 1\}$, L *a lattice of index* $[\mathbb{Z}^2 : L] = \rho(\mathfrak{m})$.

Proof. Let $\mathfrak{p}|\mathfrak{m}$. Let $n = v_{\mathfrak{p}}(\mathfrak{m})$. Let $r_1, r_2, \cdots, r_k \in \mathfrak{O}_K/\mathfrak{p}^n$ be the roots of $P(r, 1) \cong 0 \bmod \mathfrak{p}^n$. Let $r'_1, r'_2, \cdots, r'_{k'} \in \mathfrak{O}_K/\mathfrak{p}^n$ be such roots of $P(1, r) \cong 0 \bmod \mathfrak{p}^n$ as satisfy $\mathfrak{p}|r$. Then the set of solutions to $P(x, y) \cong 0 \bmod \mathfrak{p}^n$ in

$$\{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y)\}$$

is the union of the disjoint sets

$$\{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y), x \equiv r_i y \bmod \mathfrak{p}^n\},$$

$$\{(x, y) \in \mathbb{Z}^2 : \mathfrak{p} \nmid \gcd(x, y), y \equiv r_i x \bmod \mathfrak{p}^n\}.$$

Each of these sets is either the empty set or a set of the form $L \cap (\mathbb{Z}^2 - p\mathbb{Z}^2)$, where p is the rational prime lying under $\mathfrak{p}$ and L is a lattice of index $\rho(\mathfrak{p}^n)$. By Lemma 4.2.2, $k + k' \leq 2|\operatorname{Disc} P|_{\mathfrak{p}}^{-3} \deg P$. The rest of the argument is as in Lemma 4.2.3. $\square$

4.2.3 Square-full numbers

Lemma 4.2.5. *Let* K *be a number field. Let* D *be the product of all rational primes ramifying in* $K/\mathbb{Q}$. *Then, for every* $\mathfrak{d} \in I_K$, *the rational integer* $\rho(\mathfrak{d} \operatorname{rad}_K(\mathfrak{d}))$ *is (D)-square-full. For any integer* n, *there are at most* $C \cdot \tau_{\deg(K/\mathbb{Q})+1}(n)$ *ideals* $\mathfrak{d} \in I_K$ *such that* $\rho(\mathfrak{d} \operatorname{rad}_K(\mathfrak{d})) = n$, *where* C *is the product*

$$\prod_p e_p^{\deg(K/\mathbb{Q})/e_p}$$

taken over all primes p ramifying in $K/\mathbb{Q}$.

Proof. The first statement is clear. It is enough to verify the second statement for n of the form p^m. Let e be the ramification degree of p over $K/\mathbb{Q}$. Then the ideals $\mathfrak{d}$ such that $\mathfrak{d}\operatorname{rad}\mathfrak{d}$ divides p^m are of the form $\mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\cdots\mathfrak{p}_k^{a_k}$, where $a_1, a_2, \ldots, a_k$ are non-negative integers less than em and $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$ are the primes lying above p. There are $(em)^k \leq (em)^{\deg(K/\mathbb{Q})/e}$ choices for $a_1, a_2, \ldots, a_e$. Hence there are at most $(em)^{\deg(K/\mathbb{Q})/e}$ ideals $\mathfrak{d}$ such that $\gamma(\mathfrak{d}) = n$. Now $m^l \leq \binom{m+l}{l}$ for all positive m and l. Since $\tau_l(p^m) = \binom{m+l-1}{l-1}$ for $l \geq 2$, the statement follows. □

Lemma 4.2.6. *Let K be a number field. Let m be a positive integer. Let D be the product of all rational primes ramifying in $K/\mathbb{Q}$. Then, for every $\mathfrak{d} \in I_K$, $\operatorname{lcm}(m, \rho(\mathfrak{d}\operatorname{rad}_K(\mathfrak{d})))$ is (Dm)-square-full. For any integer n, there are at most $C \cdot \tau_{\deg(K/\mathbb{Q})+2}(n)$ ideals $\mathfrak{d} \in I_K$ such that $\operatorname{lcm}(m, \rho(\mathfrak{d}\operatorname{rad}_K(\mathfrak{d}))) = n$, where C is the product*

$$\prod_p e_p^{\deg(K/\mathbb{Q})/e_p}$$

taken over all primes p ramifying in $K/\mathbb{Q}$.

Proof. Immediate from Lemma 4.2.5. □

Lemma 4.2.7. *Let K be a number field. Let k be a positive integer. For any $\mathfrak{d} \in I_K$,*

$$\tau_{K,k}(\operatorname{rad}_K(\mathfrak{d})) \leq \tau_{k^{\deg K/\mathbb{Q}}}(\operatorname{rad}(\rho(\mathfrak{d}))).$$

Proof. Let $n \in \mathbb{Z}$ be square-free. For every $\mathfrak{d} \in I_K$ such that $\operatorname{rad}(\rho(\mathfrak{d}))|n$, we have $\mathfrak{d}|\rho(\mathfrak{d})$ and hence $\operatorname{rad}_K(\mathfrak{d})|n$. Thus it is enough to prove $\tau_{K,k}(n) \leq \tau_{k^{\deg K/\mathbb{Q}}}(n)$. Since there are at most $\deg K/\mathbb{Q}$ prime ideals in I_K above a given rational prime, $\tau_{K,k}(n) \leq k^{\deg K/\mathbb{Q}} = \tau_{k^{\deg K/\mathbb{Q}}}(n)$ for n prime. The general case follows by multiplicativity. □

The following two lemmas will be used frequently enough that their repeated mention would be irksome.

Lemma 4.2.8. *For any positive integers k, n, n',*

$$\tau_k(nn') \leq \tau_k(n)\tau_k(n').$$

Proof. Let $S_k(n)$ be the set of all k-tuples of integers $(n_1, n_2, \ldots, n_k)$ with product $\prod_j n_j = n$. There is a map f_k from $S_k(n) \times S_k(n')$ to $S_k(nn')$:

$$((n_1, \ldots, n_k), (n'_1, \ldots, n'_k)) \mapsto (n_1 n'_1, \ldots, n_k n'_k).$$

We can show that f_k is surjective as follows. Let $(n''_1, \ldots, n''_k)$ be given with $\prod_j n''_j = nn'$. Define $n_1 = \gcd(n, n''_1)$, $n_2 = \gcd(n/n_1, n''_2)$, $n_3 = \gcd(n/(n_1 n_2), n''_3)$, $\ldots$; $n'_1 = n''_1/n_1$, $n'_2 = n''_2/n_2$, $n'_3 = n''_3/n_3$, and so on. Then $f((n_1, \ldots, n_k), (n'_1, \ldots, n'_k)) = (n''_1, \ldots, n''_k)$. Hence f_k is surjective. Since $\tau_k(n) = \#S_k(n)$, $\tau_k(n') = \#S_k(n')$, $\tau_k(n'') = \#S_k(n'')$, the statement follows. $\square$

Lemma 4.2.9. *For any positive integers k_1, k_2, n,*

$$\tau_{k_1}(n)\tau_{k_2}(n) \leq \tau_{k_1 k_2}(n).$$

Proof. Let $S_k(n)$ be as in the proof of Lemma 4.2.8. There is a map f_{k_1,k_2} from $S_{k_1 k_2}(n)$ to $S_{k_1}(n) \times S_{k_2}(n)$:

$$(n_1, \ldots, n_{k_1 k_2}) \mapsto \left(\left(\prod_{j_2} n_{(j_2-1)k_1+j_1} \right)_{j_1}, \left(\prod_{j_1} n_{(j_2-1)k_1+j_1} \right)_{j_2} \right).$$

We can show that f_{k_1,k_2} is surjective as follows. See $n = p_1^{e_1} \cdots p_k^{e_j}$ as a box of $e_1 + \cdots + e_j$ primes of different colours. Every $(m_1, \ldots, m_{k_1}) \in S_{k_1}(n)$ (resp. $(m'_1, \ldots, m'_{k_2}) \in S_{k_2}(n)$) gives us a partition of the box into k_1 sets $M_1, \ldots, M_{k_1}$ (resp. k_2 sets $M'_1, \ldots, M'_{k_2}$). Let $n_{(j_2-1)k_1+j_1}$ be the product of the primes in $M_{j_1} \cap M'_{j_2}$. Then $f(n_1, \ldots, n_{k_1 k_2}) = ((m_1, \ldots, m_{k_1}), (m'_1, \ldots, m'_{k_2}))$. Hence f_{k_1,k_2} is surjective. Since

$\tau_{k_1}(n) = \#S_{k_1}(n)$, $\tau_{k_2}(n) = \#S_{k_2}(n)$, $\tau_{k_1k_2}(n) = \#S_{k_1k_2}(n)$, the statement follows. $\square$

Lemma 4.2.10. *Let k be a positive integer. Then*

$$\sum_{\substack{n\le N\\ n \text{ square-full}}} \tau_k(n) \le (1+\log N)^{k^3+k^2-2}N^{1/2}.$$

Proof. Every square-full number can be written as a product of a square and a cube. Hence

$$\begin{aligned}
\sum_{\substack{n\le N\\ n \text{ square-full}}} \tau_k(n) &\le \sum_{n=1}^{\sqrt{N}} \sum_{m=1}^{N^{1/3}/n^{2/3}} \tau_k(n^2m^3) \le \sum_{n=1}^{\sqrt{N}} \tau_k(n)^2 \sum_{m=1}^{N^{1/3}/n^{2/3}} \tau_k(m)^3 \\
&\le \sum_{n=1}^{\sqrt{N}} \tau_k(n)^2 (1+\log m)^{k^3-1}(N/n^2)^{1/3} \\
&\le (1+\log N)^{k^3-1}N^{1/3} \sum_{n=1}^{\sqrt{N}} \frac{\tau_k(n)^2}{n^{2/3}} \\
&\le (1+\log N)^{k^3-1}N^{1/3}(1+\log\sqrt{N})^{k^2-1}(\sqrt{N})^{1/3} \\
&\le (1+\log N)^{k^3+k^2-2}N^{1/2}.
\end{aligned}$$

$\square$

Lemma 4.2.11. *Let k be a positive integer. Then $\sum_{n \text{ square-full}} \frac{\tau_k(n)}{n}$ converges.*

Proof.

$$\sum_{\substack{n=1\\ n \text{ square-full}}}^{\infty} \frac{\tau_k(n)}{n} \le \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{\tau_k(n^2m^3)}{n^2m^3} \le \left(\sum_{n=1}^{\infty} \frac{\tau_k(n)^2}{n^2}\right)\left(\sum_{m=1}^{\infty} \frac{\tau_k(m)^3}{m^3}\right).$$

$\square$

Lemma 4.2.12. *Let k be a positive integer. Then*

$$\sum_{\substack{n>N \\ n \text{ square-full}}} \frac{\tau_k(n)}{n} \ll \frac{(\log N)^{k^2+k^3-2}}{N^{1/2}},$$

where the implied constant depends only on k.

Proof. Since $\sum_{n>x} \tau_k(n)^{l_1}/n^{l_2} \ll (\log x)^{k^{l_1}-1}/x^{l_2-1}$,

$$\begin{aligned}
\sum_{\substack{n>N \\ n \text{ square-full}}} \frac{\tau_k(n)}{n} &\leq \sum_{n>\sqrt{N}} \sum_{m=1}^{\infty} \frac{\tau_k(n^2m^3)}{n^2m^3} + \sum_{n=1}^{\sqrt{N}} \sum_{m\geq (N/n^2)^{1/3}} \frac{\tau_k(n^2m^3)}{n^2m^3} \\
&\ll \left(\sum_{n>\sqrt{N}} \frac{\tau_k(n)^2}{n^2} \right) \left(\sum_{m=1}^{\infty} \frac{\tau_k(m)^3}{m^3} \right) + \sum_{n=1}^{\sqrt{N}} \frac{\tau_k(n^2)}{n^2} \frac{(\log N)^{k^3-1}}{(N/n^2)^{2/3}} \\
&\ll \frac{(\log N)^{k^2-1}}{\sqrt{N}} + \frac{(\log N)^{k^3-1}}{N^{2/3}} \sum_{n=1}^{\sqrt{N}} \frac{\tau_k(n^2)}{n^{2/3}} \\
&\ll \frac{(\log N)^{k^2-1}}{\sqrt{N}} + \frac{(\log N)^{k^3-1}}{N^{2/3}} (\log N)^{k^2-1} N^{1/6}.
\end{aligned}$$

□

Lemma 4.2.13. *Let D and k be positive integers. Then*

$$\sum_{\substack{n=1 \\ n \text{ is } (D)\text{-square-full}}}^{\infty} \tau_k(n) \ll \tau(\mathrm{rad}(D))(\log N)^{k^3+k^2-2} N^{1/2},$$

where the implied constant depends only on k.

Proof. By Lemmas 4.2.8 and 4.2.10,

$$\begin{aligned}\sum_{\substack{n\le N\\ n \text{ is } (D)\text{-square-full}}} \tau_k(n) &= \sum_{m|\operatorname{rad}(D)} \sum_{\substack{n\le N/m\\ n \text{ square-full}}} \tau_k(mn)\\ &\le \sum_{m|\operatorname{rad}(D)} \tau_k(m) \sum_{\substack{n\le N/m\\ n \text{ square-full}}} \tau_k(n)\\ &\ll \sum_{m|\operatorname{rad}(D)} \frac{\tau_k(m)}{m^{1/2}} (\log N)^{k^3+k^2-2} N^{1/2}\\ &\ll \tau(\operatorname{rad}(D))(\log N)^{k^3+k^2-2} N^{1/2}.\end{aligned}$$

□

Lemma 4.2.14. *Let D and k be positive integers. Then*

$$\sum_{\substack{n=1\\ n \text{ is } (D)\text{-square-full}}}^{\infty} \frac{\tau_k(n)}{n} \ll \tau(\operatorname{rad}(D)),$$

where the implied constant depends only on k.

Proof. We have

$$\begin{aligned}\sum_{\substack{n=1\\ n \text{ is } (D)\text{-square-full}}}^{\infty} \frac{\tau_k(n)}{n} &= \sum_{m|\operatorname{rad}(D)} \sum_{\substack{n=1\\ m|n\\ n/m \text{ is square-full}}}^{\infty} \frac{\tau_k(m(n/m))}{m(n/m)}\\ &\le \sum_{m|\operatorname{rad}(D)} \frac{\tau_k(m)}{m} \sum_{\substack{n=1\\ n \text{ is square-full}}}^{\infty} \frac{\tau_k(n)}{n}\\ &\ll \tau(\operatorname{rad}(D)) \sum_{\substack{n=1\\ n \text{ is square-full}}}^{\infty} \frac{\tau_k(n)}{n}.\end{aligned}$$

The statement now follows from Lemma 4.2.11. □

Lemma 4.2.15. *For any positive integers k, N, D,*

$$\sum_{\substack{n>N \\ n \text{ is } (D)\text{-square-full}}} \frac{\tau_k(n)}{n} \ll \tau(\mathrm{rad}(D)) \frac{(\log N)^{k^2+k^3-2}}{\sqrt{N}},$$

where the implied constant depends only on k.

Proof. Clearly

$$\begin{aligned}\sum_{\substack{n>N \\ n \text{ is } (D)\text{-square-full}}} \frac{\tau_k(n)}{n} &\leq \sum_{m|\,\mathrm{rad}(D)} \sum_{\substack{n>N/m \\ n \text{ square-full}}} \frac{\tau_k(mn)}{mn} \\ &\leq \sum_{m|\,\mathrm{rad}(D)} \frac{\tau_k(m)}{m} \sum_{\substack{n>N/m \\ n \text{ square-full}}} \frac{\tau_k(n)}{n}.\end{aligned}$$

Hence, by Lemma 4.2.12,

$$\begin{aligned}\sum_{\substack{n>N \\ n \text{ is } (D)\text{-square-full}}} \frac{\tau_k(n)}{n} &\leq \sum_{m|\,\mathrm{rad}(D)} \frac{\tau_k(m)}{m} \frac{(\log(N/m))^{k^2+k^3-2}}{(N/m)^{1/2}} \\ &\leq \frac{(\log N)^{k^2+k^3-2}}{N^{1/2}} \sum_{m|\,\mathrm{rad}(D)} \frac{\tau_k(m)}{m^{1/2}} \\ &\ll \tau(\mathrm{rad}(D)) \frac{(\log N)^{k^2+k^3-2}}{N^{1/2}}.\end{aligned}$$

□

4.2.4 A concrete square-free sieve

Proposition 4.2.16. *Let K be a number field. Let $f : I_K \times \mathbb{Z} \to \mathbb{C}$, $g : \mathbb{Z} \to \mathbb{C}$ be given with* $\max |f(\mathfrak{a}, x)| \leq 1$, $\max |g(x)| \leq 1$. *Assume that $f(\mathfrak{a}, x)$ depends only on $\mathfrak{a}$ and on $x \bmod \mathfrak{a}$. Let $P \in \mathfrak{O}_K[x]$. Suppose there are $\epsilon_{1,N}, \epsilon_{2,N} \geq 0$ such that for any*

integer a and any positive integer m,

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} g(x) \ll \left(\frac{\epsilon_{1,N}}{m}+\epsilon_{2,N}\right)N. \tag{4.2.3}$$

Then, for any integer a and any positive integer m,

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} f(\mathrm{sq}_K(P(x)),x)g(x) \ll \left(\frac{\epsilon_{1,N}}{m}+\frac{\epsilon'}{m'}\right)N$$
$$+\#\{1\le x\le N : \exists \mathfrak{p}\ s.t.\ \rho(\mathfrak{p})>N^{1/2}, \mathfrak{p}^2|P(x,y)\}, \tag{4.2.4}$$

where

$$\begin{aligned}\epsilon' &= \sqrt{\max(\epsilon_{2,N},N^{-1/2})}\log(-\max(\epsilon_{2,N},N^{-1/2})),\\ m' &= \min(m,\min(N^{1/2},\epsilon_{2,N}^{-1})),\end{aligned} \tag{4.2.5}$$

and both c and the implied constant in (4.2.4) depend only on P, K, and the implied constant in (4.2.3).

Proof. Since the statement is immediate for P constant, we may assume that P is non-constant. Define $S_{\mathfrak{a}} = \mathfrak{O}_K/\mathfrak{a}$. Let $\phi_{\mathfrak{a}_1,\mathfrak{a}_2} : S_{\mathfrak{a}_2} \to S_{\mathfrak{a}_1}$, $\mathfrak{a}_1|\mathfrak{a}_2$, be the natural projection from $S_{\mathfrak{a}_2}$ to $S_{\mathfrak{a}_1}$.

For any $\mathfrak{a}\in I_K$, $r\in S_{\mathfrak{a}}$, set $f_{\mathfrak{a}}(r)=f(\mathfrak{a},x)$, where x is any integer with $x\equiv r \bmod \mathfrak{a}$. Let

$$g_{\mathfrak{a}}(r) = \sum_{\substack{1\le x\le N\\ x\equiv a \bmod m\\ \mathrm{sq}_K(P(x))=\mathfrak{a}\\ x\equiv r \bmod \mathfrak{a}}} g(x).$$

Then

$$\sum_{\substack{1\le x\le N\\ x\equiv a \bmod m}} f(\mathrm{sq}_K(P(x,y)),x)g(x) = \sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r).$$

Our task is thus to estimate $\sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r)$.

Let $s_{\mathfrak{d}}$, $t_{\mathfrak{d}}(r)$ be defined as in the statement of Lemma 4.2.1. Let

$$\gamma(\mathfrak{d}) = \operatorname{lcm}(\rho(\mathfrak{d}\operatorname{rad}_K(\mathfrak{d})), m).$$

Let $M \leq N^{1/2}$; its optimal value will be chosen later. We can now apply Lemma 4.2.1. What remains to do is estimate the right side of the inequality it gives us.

By Lemma 4.2.3,

$$s_{\mathfrak{d}} \leq \#\{1 \leq x \leq N : \mathfrak{d}\operatorname{rad}_K \mathfrak{d} | P(x),\ x \equiv a \bmod m\} \ll \frac{\tau_{\deg P}(\operatorname{rad}_K(\rho(\mathfrak{d})))N}{\gamma(\mathfrak{d})} \quad (4.2.6)$$

for $\gamma(\mathfrak{d}) \leq N$. By definition

$$t_{\mathfrak{d}}(r) = \sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m \\ \mathfrak{d} | \operatorname{sq}_K(P(x)) \\ x \equiv r \bmod \mathfrak{d}}} g(x). \quad (4.2.7)$$

We can bound

$$\sum_{\gamma(\mathfrak{d}) \leq M} \sum_{r \in S_{\mathfrak{d}}} \left(\sum_{\mathfrak{d}' | \mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{d}}(r)) \right) t_{\mathfrak{d}}(r)$$

trivially by

$$\sum_{\gamma(\mathfrak{d}) \leq M} \tau_{K,2}(\operatorname{rad}_K(\mathfrak{d})) \sum_{r \in S_{\mathfrak{d}}} |t_{\mathfrak{d}}(r)|.$$

We then write $\sum_{r \in S_{\mathfrak{d}}} |t_{\mathfrak{d}}(r)|$ in full as

$$\sum_{r \in S_{\mathfrak{d}}} \left| \sum_{\substack{1 \leq x \leq N \\ x \equiv a \bmod m \\ \mathfrak{d} | \operatorname{sq}_K(P(x)) \\ x \equiv r \bmod \mathfrak{d}}} g(x) \right|.$$

By Lemma 4.2.3, the set $\{x \in \mathbb{Z} : \mathfrak{d} | \operatorname{sq}_K(P(x))\}$ is the union of at most

$$|\operatorname{Disc} P|^3 \tau_{\deg P}(\operatorname{rad}(\rho(\mathfrak{d})))$$

disjoint sets of the form of the form $L_c = \{x \in \mathbb{Z} : x \equiv c \bmod \rho(\mathfrak{d} \operatorname{rad}_K(\mathfrak{d}))\}$. For every L_c, there is an $r \in S_{\mathfrak{d}}$ such that $x \equiv r \bmod \mathfrak{d}$ for every $x \in L_c$. Hence

$$\sum_{r \in S_{\mathfrak{d}}} \left| \sum_{\substack{1 \le x \le N \\ x \equiv a \bmod m \\ \mathfrak{d} | \operatorname{sq}_K(P(x)) \\ x \equiv r \bmod \mathfrak{d}}} g(x) \right| \le |\operatorname{Disc} P|^3 \tau_{\deg P}(\operatorname{rad}(\rho(\mathfrak{d}))) \max_c \left| \sum_{\substack{1 \le x \le N \\ x \equiv a \bmod m \\ x \equiv c \bmod \rho(\mathfrak{d} \operatorname{rad}_K(\mathfrak{d}))}} g(x) \right|.$$

We can now apply (4.2.3), obtaining

$$\sum_{r \in S_{\mathfrak{d}}} |t_{\mathfrak{d}}(r)| \ll \tau_{\deg P}(\operatorname{rad}(\rho(\mathfrak{d}))) \left(\frac{\epsilon_{1,N}}{\gamma(\mathfrak{d})} + \epsilon_{2,N} \right) N.$$

Lemma 4.2.1 now yields

$$\begin{aligned}
\sum_{\mathfrak{a} \in I_K} \sum_{r \in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r) g_{\mathfrak{a}}(r) &\le \sum_{\gamma(\mathfrak{d}) \le M} \sum_{r \in S_{\mathfrak{d}}} \left(\sum_{\mathfrak{d}' | \mathfrak{d}} \mu_K(\mathfrak{d}') f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{d}}(r)) \right) t_{\mathfrak{d}}(r) \\
&\quad + 2 \sum_{M < \gamma(\mathfrak{d}) \le M^2} \tau_{K,3}(\mathfrak{d}) s_{\mathfrak{d}} + 2 \sum_{\substack{\mathfrak{p} \text{ prime} \\ \gamma(\mathfrak{p}) > M}} s_{\mathfrak{p}} \\
&\le \sum_{\gamma(\mathfrak{d}) \le M} \tau_{K,2}(\operatorname{rad}_K(\mathfrak{d})) \tau_{\deg P}(\operatorname{rad}(\rho(\mathfrak{d}))) \left(\frac{\epsilon_{1,N}}{\gamma(\mathfrak{d})} + \epsilon_{2,N} \right) N \\
&\quad + 2 \sum_{M < \gamma(\mathfrak{d}) \le M^2} \frac{\tau_{K,3}(\mathfrak{d}) \tau_{\deg P}(\operatorname{rad}(\rho(\mathfrak{d}))) N}{\gamma(\mathfrak{d})} + 2 \sum_{\substack{\mathfrak{p} \text{ prime} \\ \gamma(\mathfrak{p}) > M}} s_{\mathfrak{p}}.
\end{aligned}$$

By Lemma 4.2.7, we get

$$\sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r) \leq \sum_{\gamma(\mathfrak{d})\leq M} \tau_{2^{\deg K}+\deg P}(\mathrm{rad}(\rho(\mathfrak{d})))\left(\frac{\epsilon_{1,N}}{\gamma(\mathfrak{d})}+\epsilon_{2,N}\right)N$$
$$+2\sum_{M<\gamma(\mathfrak{d})\leq M^2}\frac{\tau_{3^{\deg K}+\deg P}(\mathrm{rad}(\rho(\mathfrak{d})))}{\gamma(\mathfrak{d})}N+2\sum_{\substack{\mathfrak{p}\text{ prime}\\ \gamma(\mathfrak{p})>M}} s_{\mathfrak{p}}.$$

By Lemma 4.2.6,

$$\sum_{\gamma(\mathfrak{d})\leq M} \tau_{2^{\deg K}+\deg P}(\mathrm{rad}(\rho(\mathfrak{d})))$$

is at most a constant times

$$\sum_{\substack{n\leq M\\ n\text{ is }(Dm)\text{-square-full}\\ m|n}} \tau_{2^{\deg K}+\deg P}(\mathrm{rad}(n))\tau_{\deg(K/\mathbb{Q})+2}(n),$$

where D is the product of all rational primes ramifying in $K/\mathbb{Q}$. Similarly,

$$\sum_{\gamma(\mathfrak{d})\leq M} \frac{\tau_{2^{\deg K}+\deg P}(\mathrm{rad}(\rho(\mathfrak{d})))}{\gamma(\mathfrak{d})}$$

is at most a constant times

$$\sum_{\substack{n\leq M\\ n\text{ is }(Dm)\text{-square-full}\\ m|n}} \frac{\tau_{2^{\deg K}+\deg P}(\mathrm{rad}(n))\tau_{\deg(K/\mathbb{Q})+2}(n)}{n},$$

and

$$\sum_{M<\gamma(\mathfrak{d})\leq M^2} \frac{\tau_{3^{\deg K}+\deg P}(\mathrm{rad}(\rho(\mathfrak{d})))}{\gamma(\mathfrak{d})}$$

is at most a constant times

$$\sum_{\substack{M<n\leq M^2\\ n \text{ is } (Dm)\text{-square-full}\\ m|n}} \frac{\tau_{3^{degK}+\deg P}(\mathrm{rad}(n))\tau_{\deg(K/\mathbb{Q})+2}(n)}{n}.$$

By Lemma 4.2.3,

$$\begin{aligned}
\sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>M}} s_{\mathfrak{p}} &= \sum_{\substack{\mathfrak{p} \text{ prime}\\ M<\gamma(\mathfrak{p})\leq N\\ \mathfrak{p}\nmid m}} s_{\mathfrak{p}} + \sum_{\substack{\mathfrak{p} \text{ prime}\\ M<\gamma(\mathfrak{p})\leq N\\ \mathfrak{p}|m}} s_{\mathfrak{p}} + \sum_{\substack{\mathfrak{p} \text{ prime}\\ N<\gamma(\mathfrak{p})\leq Nm\\ \mathfrak{p}\nmid m}} s_{\mathfrak{p}} + \sum_{\substack{\mathfrak{p} \text{ prime}\\ N<\gamma(\mathfrak{p})\leq Nm\\ \mathfrak{p}|m}} s_{\mathfrak{p}} + \sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>Nm}} s_{\mathfrak{p}} \\
&\ll \sum_{\substack{p \text{ prime}\\ M<mp^2\leq N}} \frac{N}{mp^2} + \sum_{\substack{p \text{ prime}\\ M<mp\leq N\\ p|m}} \frac{N}{mp} + \sum_{\substack{p \text{ prime}\\ N<mp^2\leq Nm}} \frac{N}{p^2} \\
&+ \sum_{\substack{p \text{ prime}\\ N<mp^2\leq Nm\\ p|m}} \frac{N}{p} + \sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>Nm}} s_{\mathfrak{p}} \\
&\leq \frac{N}{\sqrt{Mm}} + \frac{N\omega(m)}{M} + \frac{N}{\sqrt{N/m}} + m\omega(m) + \sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>Nm}} s_{\mathfrak{p}}.
\end{aligned}$$

Write $rem(M) = \frac{N}{\sqrt{Mm}} + \frac{N\omega(m)}{M} + \frac{N}{\sqrt{N/m}} + m\omega(m)$; it will be swallowed by higher-order terms shortly. (We will assume $m < N^{1/2}$, as the bound would otherwise be trivial.)

Now

$$\begin{aligned}
\sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r) \ll & \sum_{\substack{n\le M\\ n \text{ is } (Dm)\text{-square-full}\\ m|n}} \tau_{q_1}(n)\left(\frac{\epsilon_{1,N}}{n}+\epsilon_{2,N}\right)N \\
& + \sum_{\substack{M<n\le M^2\\ n \text{ is } (Dm)\text{-square-full}\\ m|n}} \frac{\tau_{q_2}(n)}{n}N + rem(M) + \sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>N}} s_{\mathfrak{p}} \\
\le & \sum_{\substack{n\le M/m\\ n \text{ is } (Dm)\text{-square-full}}} \tau_{q_1}(n)\tau_{2q_1}(m)\left(\frac{\epsilon_{1,N}}{mn}+\epsilon_{2,N}\right)N \\
& + \sum_{\substack{n> M/m\\ n \text{ is } (Dm)\text{-square-full}}} \frac{\tau_{q_2}(n)\tau_{2q_2}(m)}{mn}N + rem(M) + \sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>Nm}} s_{\mathfrak{p}},
\end{aligned}$$

where $q_1 = (2^{\deg K}+\deg P)(\deg(K/\mathbb{Q})+1)$, $q_2 = (3^{\deg K}+\deg P)(\deg(K/\mathbb{Q})+1)$. Now note that

$$\sum_{\substack{\mathfrak{p} \text{ prime}\\ \gamma(\mathfrak{p})>N}} s_{\mathfrak{p}} \ll \#\{1\le x\le N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p})>N^{1/2}, \mathfrak{p}^2|P(x,y)\}.$$

By Lemmas 4.2.13, 4.2.14 and 4.2.15 we can conclude that

$$\begin{aligned}
\sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r) \ll & \left(\frac{\epsilon_{1,N}}{m}+\epsilon_{2,N}(\log M)^{q_3}\sqrt{M/m}+\frac{(\log M)^{q_4}}{\sqrt{Mm}}\right) \\
& \cdot \tau_{q_5}(m)\tau(\mathrm{rad}(Dm))N \\
& + rem(M) + \#\{-N\le x\le N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p})>N^{1/2}, \mathfrak{p}^2|P(x,y)\} \\
& \ll \left(\frac{\epsilon_{1,N}}{m}+\epsilon_{2,N}(\log M)^{q_3}\sqrt{M/m}+\frac{(\log M)^{q_4}}{\sqrt{Mm}}\right)\tau_{q_6}(m)N \\
& + \#\{-N\le x\le N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p})>N^{1/2}, \mathfrak{p}^2|P(x,y)\},
\end{aligned}$$

where $q_3 = q_1^3+q_1^2-2$, $q_4 = q_2^3+q_2^2-2$, $q_5 = \max(2q_1, 2q_2)$, $q_6 = 2q_5$. Set $M = \min\left(N^{1/2}, \frac{1}{\epsilon_{2,N}}\right)$, $c_1 = q_6$, $c_2 = \max(q_3, q_4)$. The statement follows. $\square$

Proposition 4.2.17. *Let K be a number field. Let $f : I_K \times \{(x,y) \in \mathbb{Z}^2 : \gcd(x,y) = 1\} \to \mathbb{C}$, $g : \{(x,y) \in \mathbb{Z}^2 : \gcd(x,y) = 1\} \to \mathbb{C}$ be given with $\max|f(\mathfrak{a},x,y)| \leq 1$, $\max|g(x,y)| \leq 1$. Assume that $f(\mathfrak{a},x,y)$ depends only on $\mathfrak{a}$ and on $\{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$. Let $P \in \mathfrak{O}_K[x,y]$ be a homogeneous polynomial. Let S be a subset of $\mathbb{R}^2$. Suppose there are $\epsilon_{1,N}$, $\epsilon_{2,N} \geq 0$ such that for any lattice coset $L \subset \mathbb{Z}^2$,*

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} g(x,y) \ll \left(\frac{\epsilon_{1,N}}{[\mathbb{Z}^2 : L]} + \epsilon_{2,N}\right) N^2. \tag{4.2.8}$$

Then, for any lattice coset $L \subset \mathbb{Z}^2$,

$$\begin{aligned} \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} & f(\mathrm{sq}_K(P(x,y)),x,y)g(x,y) \\ & \ll \left(\frac{\epsilon_{1,N}}{[\mathbb{Z}^2 : L]} + \frac{\epsilon'}{\sqrt{m'}}\right) N^2 \\ & + \{-N \leq x,y \leq N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p}) > N, \mathfrak{p}^2 | P(x,y)\}, \end{aligned} \tag{4.2.9}$$

where

$$\epsilon' = \sqrt{\max(\epsilon_{2,N}, N^{-1/2})}\log(-\max(\epsilon_{2,N}, N^{-1/2})),$$
$$m' = \min([\mathbb{Z}^2 : L], \min(N^{1/2}, \epsilon_{2,N}^{-1})),$$

the constants c_1 and c_2 depend only on P and K, and the implied constant in (4.2.9) depends only on P, K and the implied constant in (4.2.8).

Proof. Since the statement is immediate for P constant we may assume that P is non-constant. Define $S_{\mathfrak{a}} = \prod_{\mathfrak{p}|\mathfrak{a}} \mathbb{P}^1(\mathfrak{O}_K/\mathfrak{p})$. Let $\phi_{\mathfrak{a}_1,\mathfrak{a}_2} : K_{\mathfrak{a}_2} \to K_{\mathfrak{a}_1}$, $\mathfrak{a}_1|\mathfrak{a}_2$, be the natural projection from $S_{\mathfrak{a}_2}$ to $S_{\mathfrak{a}_1}$. Write $\phi_{\mathfrak{a}}(x,y) = \{\frac{x \bmod \mathfrak{p}}{y \bmod \mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{a}} \in S_{\mathfrak{a}}$ for any coprime x, y.

For any $\mathfrak{a} \in I_K$, $r \in S_{\mathfrak{a}}$, set $f_{\mathfrak{a}}(r) = f(\mathfrak{a},x,y)$, where x, y are any coprime integers

with $\phi_{\mathfrak{a}}(x,y) = r$. Let

$$g_{\mathfrak{a}}(r) = \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1 \\ \mathrm{sq}_K(P(x,y))=\mathfrak{a} \\ \phi_{\mathfrak{a}}(x,y)=r}} g(x,y).$$

Then

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1}} f(\mathrm{sq}_K(P(x,y)),x,y)g(x,y) = \sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r).$$

The question now is how to estimate $\sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r)$.

Let $s_{\mathfrak{d}}$, $t_{\mathfrak{d}}(r)$ be as in the statement of Lemma 4.2.1. Let

$$\gamma(\mathfrak{d}) = \mathrm{lcm}(\rho(\mathfrak{d}\,\mathrm{rad}_K(\mathfrak{d})), [\mathbb{Z}^2 : L]).$$

Let $M \le N$. By Lemmas 2.2.1 and 4.2.4,

$$\begin{aligned} s_{\mathfrak{d}} &\le \#\{(x,y)\in S\cap[-N,N]^2\cap L : \gcd(x,y)=1, \mathfrak{d}\,\mathrm{rad}_K(\mathfrak{d})|P(x,y)\} \\ &\ll \frac{\tau_{2\deg P}(\mathrm{rad}_K(\rho(\mathfrak{d})))N^2}{\gamma(\mathfrak{d})} \end{aligned}$$

for $\gamma(\mathfrak{d}) \le N^2$. By definition,

$$t_{\mathfrak{d}}(r) = \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1 \\ \mathfrak{d}|\,\mathrm{sq}_K(P(x,y)) \\ \phi_{\mathfrak{d}}(x,y)=r}} g(x,y). \tag{4.2.10}$$

We can bound

$$\sum_{\gamma(\mathfrak{d})\le M}\sum_{r\in S_{\mathfrak{d}}}\left(\sum_{\mathfrak{d}'|\mathfrak{d}}\mu_K(\mathfrak{d}')f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{d}}(r))\right)t_{\mathfrak{d}}(r)$$

trivially by

$$\sum_{\gamma(\mathfrak{d})\le M}\tau_{K,2}(\mathrm{rad}_K(\mathfrak{d}))\sum_{r\in S_{\mathfrak{d}}}|t_{\mathfrak{d}}(r)|.$$

We write $\sum_{r\in S_{\mathfrak{d}}} |t_{\mathfrak{d}}(r)|$ in full as

$$\sum_{r\in S_{\mathfrak{d}}} \left| \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1 \\ \mathfrak{d}|\operatorname{sq}_K(P(x,y)) \\ \phi_{\mathfrak{d}}(x,y)=r}} g(x,y) \right|.$$

By Lemma 4.2.4, the set $\{(x,y)\in\mathbb{Z}^2 : \gcd(x,y)=1, \mathfrak{d}|\operatorname{sq}_K(P(x))\}$ is the union of at most $|\operatorname{Disc} P|^3\tau_{2\deg P}(\operatorname{rad}_K(\mathfrak{d}))$ disjoint sets of the form

$$R\cap\{(x,y)\in\mathbb{Z}^2 : \gcd(x,y)=1\},$$

where R is a lattice of index $\rho(\mathfrak{d}\operatorname{rad}_K(\mathfrak{d}))$. For every R of index $\rho(\mathfrak{d}\operatorname{rad}_K(\mathfrak{d}))$, there is an $r\in S_{\mathfrak{d}}$ such that $\phi_{\mathfrak{d}}(x,y)=r$ for every $(x,y)\in R$. Hence

$$\sum_{r\in S_{\mathfrak{d}}} \left| \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1 \\ \mathfrak{d}|\operatorname{sq}_K(P(x,y)) \\ \phi_{\mathfrak{d}}(x,y)=r}} g(x,y) \right|$$

is equal to at most $(\operatorname{Disc} P)^3\tau_{2\deg P}(\operatorname{rad}(m))$ times

$$\max_{\substack{R \\ [\mathbb{Z}^2:R]=\gamma(\mathfrak{d})}} \left| \sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L \\ \gcd(x,y)=1 \\ (x,y)\in R}} g(x,y) \right|.$$

We can now apply (4.2.8), obtaining

$$\sum_{\substack{(x,y)\in S\cap[-N,N]^2\cap L\\ \gcd(x,y)=1\\ (x,y)\in R}} g(x,y) \ll \left(\frac{\epsilon_{1,N}}{\gamma(\mathfrak{d})}+\epsilon_{2,N}\right)N^2.$$

Lemma 4.2.1 now yields

$$\begin{aligned}\sum_{\mathfrak{a}\in I_K}\sum_{r\in S_{\mathfrak{a}}} f_{\mathfrak{a}}(r)g_{\mathfrak{a}}(r) &\le \sum_{\gamma(\mathfrak{d})\le M}\sum_{r\in S_{\mathfrak{a}}}\left(\sum_{\mathfrak{d}'|\mathfrak{d}}\mu_K(\mathfrak{d}')f_{\mathfrak{d}/\mathfrak{d}'}(\phi_{\mathfrak{d}/\mathfrak{d}',\mathfrak{d}}(r))\right)t_{\mathfrak{d}}(r)\\ &\quad+2\sum_{M<\gamma(\mathfrak{d})\le M^2}\tau_{K,3}(\mathfrak{d})s_{\mathfrak{d}}+2\sum_{\substack{\mathfrak{p}\text{ prime}\\ \gamma(\mathfrak{p})>M}}s_{\mathfrak{p}}\\ &\le \sum_{\gamma(\mathfrak{d})\le M}\tau_{K,2}(\mathrm{rad}_K(\mathfrak{d}))\tau_{2\deg P}(\mathrm{rad}(\rho(\mathfrak{d})))\left(\frac{\epsilon_{1,N}}{\phi(\gamma(\mathfrak{d}))}+\epsilon_{2,N}\right)N^2\\ &\quad+2\sum_{M<\gamma(\mathfrak{d})\le M^2}\frac{\tau_{K,3}(\mathfrak{d})\tau_{2\deg P}(\mathrm{rad}(\rho(\mathfrak{d}))N^2}{\gamma(\mathfrak{d})}+2\sum_{\substack{\mathfrak{p}\text{ prime}\\ \gamma(\mathfrak{p})>M}}s_{\mathfrak{p}}.\end{aligned}$$

The remainder of the argument is the same as in Proposition 4.2.16. □

Remark. Proposition 4.2.17 still holds if "lattice coset" is replaced by "lattice" throughout the statement.

4.3 A global approach to the square-free sieve

4.3.1 Elliptic curves, heights and lattices

As is usual, we write $\hat{h}$ for the canonical height on an elliptic curve E, and h_x, h_y for the height on E with respect to x, y:

$$h_x((x,y)) = \begin{cases} 0 & \text{if } P=O,\\ \log H(x) & \text{if } P=(x,y),\end{cases}$$

$$h_y((x,y)) = \begin{cases} 0 & \text{if } P = O, \\ \log H(y) & \text{if } P = (x,y), \end{cases}$$

where O is the origin of E, taken to be the point at infinity, and

$$H(y) = (H_K(y))^{1/[K:\mathbb{Q}]},$$
$$H_K(y) = \prod_v \max(|y|_v^{n_v}, 1),$$

where K is any number field containing y, the product $\prod_v$ is taken over all places v of K, and n_v denotes the degree of $K_v/\mathbb{Q}_v$.

In particular, if x is a rational number x_0/x_1, $\gcd(x_0, x_1) = 1$, then

$$H(x) = H_{\mathbb{Q}}(x) = \max(|x_0|, |x_1|),$$
$$h_x((x,y)) = \log(\max(|x_0|, |x_1|)).$$

The differences $|\hat{h} - \frac{1}{2}h_x|$ and $|\hat{h} - \frac{1}{3}h_y|$ are bounded on the set of all points of E (not merely on $E(\mathbb{Q})$). This basic property of the canonical height will be crucial in our analysis.

Lemma 4.3.1. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. For every square-free rational integer d, let E_d be the elliptic curve*

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

Let $P = (x,y) \in E_d(\mathbb{Q})$. Consider the point $P' = (x, d^{1/2}y)$ on E_1. Then $\hat{h}(P) = \hat{h}(P')$, where the canonical heights are defined on E_d and E_1, respectively,

Proof. Clearly $h_x(P') = h_x(P)$. Moreover $(P+P)' = P' + P'$. Hence

$$\hat{h}(P) = \frac{1}{2}\lim_{N\to\infty} 4^{-N} h_x([2^N]P) = \frac{1}{2}\lim_{N\to\infty} 4^{-N} h_x([2^N]P') = \hat{h}(P').$$

□

Lemma 4.3.2. *Let $f \in \mathbb{Z}[x]$ be an irreducible cubic polynomial of non-zero discriminant. Let E be the elliptic curve given by $E : y^2 = f(x)$. Let $d \in \mathbb{Z}$ be square-free. Let x, y be rational numbers, $y \neq 0$, such that $P = (x, d^{1/2}y)$ lies on E. Then*

$$h_y(P) \geq \frac{3}{8} \log |d| + C_f,$$

where C_f is a constant depending only on f.

Proof. Write $y = y_0/y_1$, where y_0 and y_1 are coprime integers. Then

$$H(y) = \max\left(\frac{|y_0||d|^{1/2}}{\sqrt{\gcd(d, y^2)}}, \frac{|y_1|}{\sqrt{\gcd(d, y_1^2)}}\right). \tag{4.3.1}$$

Write a for the leading coefficient of f. Let $p | \gcd(d, y_1^2)$, $p \nmid a$. Since d is square-free, $p^2 \nmid \gcd(d, y^2)$. Suppose $p^2 \nmid y_1$. Then $\nu_p(dy^2) = -1$. However, $dy^2 = f(x)$ implies that, if $\nu_p(x) \geq 0$, then $\nu_p(dy^2) \geq 0$, and if $\nu_p(x) < 0$, then $\nu_p(dy^2) \leq -3$. Contradiction. Hence $p | \gcd(d, y_1^2)$, $p \nmid a$ imply $p^2 \nmid \gcd(d, y_1^2)$, $p^2 | y_1$. Therefore $|y_1| \geq (\gcd(d, y_1^2)/a)^2$.

By (4.3.1) it follows that

$$\begin{aligned} H(P) &\geq \max\left(\frac{|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{|y_1|}{\sqrt{\gcd(d, y_1^2)}}\right) \\ &\geq \max\left(\frac{|d|^{1/2}}{\sqrt{\gcd(d, y_1^2)}}, \frac{(\gcd(d, y_1^2))^{3/2}}{a^2}\right). \end{aligned}$$

Since $\max(|d|^{1/2}z^{-1/2}, z^{3/2}/a_3^2)$ is minimal when $|d|^{1/2}z^{-1/2} = z^{3/2}/a_3^2$, i.e., when $z = a_3|d|^{1/4}$, we obtain

$$H(P) \geq |d|^{3/8}|a_1|^{-1/2}.$$

Hence

$$h_y(P) = \log H(P) \geq \frac{3}{8}\log|d| - \frac{1}{2}\log|a|.$$

□

Corollary 4.3.3. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. For every square-free rational integer d, let E_d be the elliptic curve*

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

Let $P = (x, y) \in E_d(\mathbb{Q})$. Then

$$\hat{h}(P) \geq \frac{1}{8}\log|d| + C_f,$$

where C_f is a constant depending only on f.

Proof. Let $P' = (x, d^{1/2}y) \in E_1$. By Lemma 4.3.1, $\hat{h}(P) = \hat{h}(P')$. The difference $|\hat{h} - h_x|$ is bounded on E. The statement follows from Lemma 4.3.2. □

The following crude estimate will suffice for some of our purposes.

Lemma 4.3.4. *Let Q be a positive definite quadratic form on $\mathbb{Z}^r$. Suppose $Q(\vec{x}) \geq c_1$ for all non-zero $\vec{x} \in \mathbb{Z}^r$. Then there are at most*

$$(1 + 2\sqrt{c_2/c_1})^r$$

values of $\vec{x}$ for which $Q(\vec{x}) \leq c_2$.

Proof. There is a linear bijection $f : \mathbb{Q}^r \to \mathbb{Q}^r$ taking Q to the square root of the Euclidean norm: $Q(\vec{x}) = |f(\vec{x})|^2$ for all $\vec{x} \in \mathbb{Q}^r$. Because $Q(\vec{x}) > c_1$ for all non-zero $\vec{x} \in \mathbb{Z}^r$, we have that $f(\mathbb{Z}^r)$ is a lattice $L \subset \mathbb{Q}^r$ such that $|\vec{x}| \geq c_1^{1/2}$ for all $\vec{x} \in L$, $\vec{x} \neq 0$. We can draw a sphere $S_{\vec{x}}$ of radius $\frac{1}{2}c_1^{1/2}$ around each point $\vec{x}$ of L. The

spheres do not overlap. If $\vec{x} \in L$, $|\vec{x}| \in c_2^{1/2}$, then $S_{\vec{x}}$ is contained in the sphere S' of radius $c_2^{1/2} + c_1^{1/2}/2$ around the origin. The total volume of all spheres $S_{\vec{x}}$ within S' is no greater than the volume of S'. Hence

$$\#\{\vec{x} \in L : |\vec{x}| \leq c_2^{1/2}\} \cdot (c_1^{1/2}/2)^r \leq (c_2^{1/2} + c_1^{1/2}/2)^r.$$

The statement follows. □

Corollary 4.3.5. *Let E be an elliptic curve over $\mathbb{Q}$. Suppose there are no non-torsion points $P \in E(\mathbb{Q})$ of canonical height $\hat{h}(P) < c_1$. Then there are at most*

$$O\left((1 + 2\sqrt{c_2/c_1})^{\mathrm{rank}(E)}\right)$$

points $P \in E(\mathbb{Q})$ for which $\hat{h}(P) < c_2$. The implied constant is absolute.

Proof. The canonical height $\hat{h}$ is a positive definite quadratic form on the free part $\mathbb{Z}^{\mathrm{rank}(E)}$ of $E(\mathbb{Q}) \sim \mathbb{Z}^{\mathrm{rank}(E)} \times T$. A classical theorem of Mazur's [Maz] states that the cardinality of T is at most 16. Apply Lemma 4.3.4. □

Note that we could avoid the use of Mazur's theorem, since Lemmas 4.3.1 and 4.3.2 imply that the torsion group of E_d is either $\mathbb{Z}/2$ or trivial for large enough d.

4.3.2 Twists of cubics and quartics

Let $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 4. For every square-free $d \in \mathbb{Z}$, consider the curve

$$C_d : dy^2 = f(x). \tag{4.3.2}$$

If there is a rational point (r, s) on C_d, then there is a birational map from C_d to the elliptic curve

$$E_d : dy^2 = x^3 + a_2x^2 + (a_1a_3 - 4a_0a_4)x - (4a_0a_2a_4 - a_1^2a_4 - a_0a_3^2). \tag{4.3.3}$$

Moreover, we can construct such a birational map in terms of (r, s) as follows. Let (x, y) be a rational point on C_d. We can rewrite (4.3.2) as

$$y^2 = \frac{1}{d}f(x).$$

We change variables:

$$x_1 = x - r, \quad y_1 = y$$

satisfy

$$y^2 = \frac{1}{d}\left(\frac{1}{4!}f^{(4)}(r)x_1^4 + \frac{1}{3!}f^{(3)}(r)x_1^3 + \frac{1}{2!}f''(r)x_1^2 + \frac{1}{1!}f'(r)x_1 + f(r)\right).$$

We now apply the standard map for putting quartics in Weierstrass form:

$$\begin{aligned} x_2 &= (2s(y_1 + s) + f'(r)x_1/d)/x_1^2, \\ y_2 &= (4s^2(y_1 + s) + 2s(f'(r)x_1/d + f''(r)x_1^2/(2d)) - (f'(r)/d)^2x_1^2/(2s))/x_1^3 \end{aligned}$$

satisfy

$$y_2^2 + A_1x_2y_2 + A_3y_2 = x_2^3 + A_2x_2^2 + A_4x_2 + A_6 \tag{4.3.4}$$

with

$$\begin{aligned} A_1 &= \frac{1}{d}f'(r)/s, & A_2 &= \frac{1}{d}(f''(r)/2 - (f'(r))^2/(4f(r))), \\ A_3 &= \frac{2s}{d}f^{(3)}(r)/3!, & A_4 &= -\frac{1}{d^2} \cdot 4f(r) \cdot \frac{1}{4!}f^{(4)}(r), \\ A_6 &= A_2A_4. \end{aligned}$$

To take (4.3.4) to E_d, we apply a linear change of variables:

$$x_3 = dx_2 + r(a_3 + 2a_4 r),$$
$$y_2 = \frac{d}{2}(2y_2 + a_1 x_2 + a_3)$$

satisfy

$$dy_3^2 = x_3^3 + a_2 x_3^2 + (a_1 a_3 - 4a_0 a_4)x_3 - (4a_0 a_2 a_4 - a_1^2 a_4 - a_0 a_3^2).$$

We have constructed a birational map $\phi_{r,s}(x, y) \mapsto (x_3, y_3)$ from C_d to E_d.

Now consider the equation

$$dy^2 = a_4 x^4 + a_3 x^3 z + a_2 x^2 z^2 + a_1 x z^3 + a_0 z^4. \tag{4.3.5}$$

Suppose there is a solution (x_0, y_0, z_0) to (4.3.5) with $x_0, y_0, z_0 \in \mathbb{Z}$, $|x_0|, |z_0| \leq N$, $z_0 \neq 0$. Then $(x_0/z_0, y_0/z_0^2)$ is a rational point on (4.3.2). We can set $r = x_0/z_0$, $s = y_0/z_0^2$ and define a map $\phi_{r,s}$ from C_d to E_d as above. Now let $x, y, z \in \mathbb{Z}$, $|x|, |z| \leq N$, $z_0 \neq 0$, be another solution to (4.3.5). Then

$$P = \phi_{r,s}(x_0/z_0, y_0/z_0^2)$$

is a rational point on E_d. Notice that $|y_0|, |y| \ll (N^4/d)^{1/2}$. Write

$$\phi_{r,s}(P) = (u_0/u_1, v),$$

where $u_0, u_1 \in \mathbb{Z}$, $v \in \mathbb{Q}$, $\gcd(u_0, u_1) = 1$. By a simple examination of the construction of $\phi_{r,s}$ we can determine that $\max(u_0, u_1) \ll N^7$, where the implied constant depends only on $a_0, a_1, \cdots, a_4$. In other words,

$$h_x(P) \leq 7 \log N + C, \tag{4.3.6}$$

where C is a constant depending only on a_j. Notice that (4.3.6) holds even for $(x, y, z) = (x_0, y_0, z_0)$, as then P is the origin of E.

The value of $h_x(P)$ is independent of whether P is considered as a rational point of E_d or as a point of E_1. Let $\hat{h}_{E_1}(P)$ be the canonical height of P as a point of E_1. Then

$$|\hat{h}_{E_1}(P) - \frac{1}{2}h_x(P)| \leq C',$$

where C' depends only on f. By Lemma 4.3.1, the canonical height $\hat{h}_{E_1}(P)$ of P as a point of E_1 equals the canonical height $\hat{h}_{E_d}(P)$ of P as a point of E_d. Hence

$$|\hat{h}_{E_d}(P) - \frac{1}{2}h_x(P)| \leq C'.$$

Then, by (4.3.6),

$$\hat{h}_{E_d}(P) \leq \frac{7}{2}\log N + (C/2 + C').$$

We have proven

Lemma 4.3.6. *Let $f(x, z) = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \in \mathbb{Z}[x, z]$ be an irreducible homogeneous polynomial. Then there is a constant C_f such that the following holds. Let N be any positive integer. Let d be any square-free integer. Let $S_{d,1}$ be the set of all solutions $(x, y, z) \in \mathbb{Z}^3$ to*

$$dy^2 = f(x, z)$$

satisfying $|x|, |z| \leq N$, $\gcd(x, z) = 1$. Let $S_{d,2}$ be the set of all rational points P on

$$E_d : dy^2 = x^3 + a_2x^2 + (a_1a_3 - 4a_0a_4)x - (4a_0a_2a_4 - a_1^2a_4 - a_0a_3^2) \tag{4.3.7}$$

with canonical height

$$\hat{h}(P) \leq \frac{7}{2}\log N + C_f.$$

Then there is an injective map from $S_{d,1}$ to $S_{d,2}$.

We can now apply the results of subsection 4.3.1.

Proposition 4.3.7. *Let $f(x,z) = a_4x^4 + a_3x^3z + a_2x^2z^2 + a_1xz^3 + a_0z^4 \in \mathbb{Z}[x,z]$ be an irreducible homogeneous polynomial. Then there are constants $C_{f,1}$, $C_{f,2}$, $C_{f,3}$ such that the following holds. Let N be any positive integer. Let d be any square-free integer. Let S_d be the set of all solutions $(x,y,z) \in \mathbb{Z}^3$ to*

$$dy^2 = f(x,z)$$

satisfying $|x|, |z| \leq N$, $\gcd(x,z) = 1$. Then

$$\#S_d \ll \begin{cases} \left(1 + 2\sqrt{(\frac{7}{2}\log N + C_{f,1})/(\frac{1}{8}\log|d| + C_{f,2})}\right)^{\mathrm{rank}(E_d)} & \text{if } |d| \geq C_{f,4}, \\ \left(1 + 2C_{f,3}\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{\mathrm{rank}(E_d)} & \text{if } |d| < C_{f,4}, \end{cases}$$

where $C_{f,4} = e^{9C_{f,2}}$, E_d is as in (4.3.7), and the implied constant depends only on f.

Proof. If $|d| \leq C_{f,4}$, apply Corollary 4.3.5 and Lemma 4.3.6. If $|d| > C_{f,4}$, apply Corollary 4.3.3, Corollary 4.3.5 and Lemma 4.3.6. □

4.3.3 Divisor functions and their averages

As is usual, we denote by $\omega(d)$ the number of prime divisors of a positive integer d. Given an extension $K/\mathbb{Q}$, we define

$$\omega_K(d) = \sum_{\substack{\mathfrak{p} \in I_K \\ \mathfrak{p} | d}} 1.$$

Lemma 4.3.8. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 3 and non-zero discriminant. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x) = 0$. For every square-free*

rational integer d, let E_d be the elliptic curve given by

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

Then

$$\mathrm{rank}(E_d) = C_f + \omega_K(d) - \omega(d),$$

where C_f is a constant depending only on f.

Proof. Write $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. Let $f_d(x) = a_3x^3 + da_2x^2 + d^2a_1x + d^3a_0$. Then $d\alpha$ is a root of $f_d(x) = 0$. Clearly $\mathbb{Q}(d\alpha) = \mathbb{Q}(\alpha)$. If p is a prime of good reduction for E_1, then E_d will have additive reduction at p if $p|d$, and good reduction at p if $p \nmid d$. The statement now follows immediately from the standard bound in, say, [BK], Prop. 7.1. □

Lemma 4.3.9. *Let $K/\mathbb{Q}$ be a non-Galois extension of $\mathbb{Q}$ of degree 3. Let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. Let $K'/\mathbb{Q}$ be the quadratic subextension of $K/\mathbb{Q}$. Then the following statements are equivalent:*

- *p splits as $p = \mathfrak{p}_1\mathfrak{p}_2$ in $K/\mathbb{Q}$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime ideals of K,*
- *p does not split in $K'/\mathbb{Q}$.*

Proof. Clearly $\mathrm{Gal}(K/\mathbb{Q}) = S_3$. Consider the Frobenius element Frob_p as a conjugacy class in S_3. There are three conjugacy classes in S_3; we shall call them C_1 (the identity), C_2 (the transpositions) and C_3 (the 3-cycles). If $\mathrm{Frob}_p = C_1$, then p splits completely in K and in K'. It remains to consider the other two cases, $\mathrm{Frob}_p = C_2$ and $\mathrm{Frob}_p = C_3$.

Suppose $\mathrm{Frob}_p = C_2$. Then p splits as $p = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3$ in $L/\mathbb{Q}$. We have

$$C_2 = \{\mathrm{Frob}_{\mathfrak{q}_1}, \mathrm{Frob}_{\mathfrak{q}_2}, \mathrm{Frob}_{\mathfrak{q}_3}\}.$$

Hence exactly one of $\mathrm{Frob}_{\mathfrak{q}_1}$, $\mathrm{Frob}_{\mathfrak{q}_2}$, $\mathrm{Frob}_{\mathfrak{q}_3}$ is the transposition fixing K. Say $\mathrm{Frob}_{\mathfrak{q}_1}$ fixes K. Let $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3 \in I_K$ be the primes (not distinct) lying under $\mathfrak{q}_1$, $\mathfrak{q}_2$ and $\mathfrak{q}_3$. Then $\deg(K_{\mathfrak{p}_1}/\mathbb{Q}_p) = 1$, whereas $\deg(K_{\mathfrak{p}_i}/\mathbb{Q}_p) = 2$ for $i = 2, 3$. Hence p splits as $p = \mathfrak{p}_1\mathfrak{p}_2$ in $K/\mathbb{Q}$. Since $\deg(L/K') = 3$ is odd and $N\mathfrak{q}_i = p^2$ is an even power of p, we can see that p cannot split in $K'/\mathbb{Q}$.

Finally, consider $\mathrm{Frob}_p = C_3$. Then p splits as $p = \mathfrak{q}_1\mathfrak{q}_2$ in $L/\mathbb{Q}$. Since $\deg(L/K')$ and $\deg(K/\mathbb{Q})$ are both odd, it follows that p splits in $K'/\mathbb{Q}$ but not in $K/\mathbb{Q}$. $\square$

Lemma 4.3.10. *Let $K/\mathbb{Q}$ be an extension of $\mathbb{Q}$ of degree 3. Let α be a positive real number. Let*

$$S_\alpha(X) = \sum_{n \le X} 2^{\alpha\omega_K(n) - \alpha\omega(n)}.$$

Then

$$\begin{aligned} S_\alpha(X) &\sim C_{K,\alpha} X (\log X)^{(2^{2\alpha}-1)/3} \text{ if } K/\mathbb{Q} \text{ is Galois,} \\ S_\alpha(X) &\sim C_{K,\alpha} X (\log X)^{\frac{1}{2}(2^{\alpha}-1)+\frac{1}{6}(2^{2\alpha}-1)} \text{ if } K/\mathbb{Q} \text{ is not Galois,} \end{aligned} \tag{4.3.8}$$

where $C_{K,\alpha} > 0$ depends only on K and α, and the dependence on α is continuous.

Proof. Suppose $K/\mathbb{Q}$ is Galois. Then, for $\Re s > 1$,

$$\sigma_{K/\mathbb{Q}}(s) = \prod_{\mathfrak{p} \in I_K} \frac{1}{1 - (N\mathfrak{p})^{-s}} = \prod_{p \text{ ramified}} \frac{1}{1 - p^{-s}} \prod_{\substack{p \text{ unsplit} \\ \& \text{ unram.}}} \frac{1}{1 - p^{-3s}} \prod_{p \text{ split}} \frac{1}{(1 - p^{-s})^3}.$$

Hence

$$\prod_{p \text{ split}} (1 + \beta p^{-s}) = L_1(s)(\zeta_{K/\mathbb{Q}}(s))^{\beta/3}, \tag{4.3.9}$$

where $L_1(s)$ is continuous and bounded on $\{s : \Re s > 1 - 1/4\}$. Now

$$\begin{aligned} 2^{\alpha\omega_K(n)-\alpha\omega(n)} &= \prod_{\substack{p|n \\ p \text{ split in } K/\mathbb{Q}}} 2^{2\alpha} = \prod_{\substack{p|n \\ p \text{ split in } K/\mathbb{Q}}} (1 + (2^{2\alpha} - 1)) \\ &= \sum_{\substack{ab=n \\ p|a \Rightarrow p \text{ split}}} \prod_{p|a} (2^{2\alpha} - 1). \end{aligned}$$

Hence

$$\begin{aligned} \sum_n 2^{\alpha\omega_K(n)-\alpha\omega(n)} n^{-s} &= \left(\sum_n n^{-s}\right) \cdot \sum_{\substack{n \\ p|n \Rightarrow p \text{ split}}} \prod_{p|n} (2^{2\alpha} - 1) n^{-s} \\ &= \zeta(s) \cdot \prod_{p \text{ split}} (1 + (2^{2\alpha} - 1)p^{-s}). \end{aligned}$$

By (4.3.9) it follows that

$$\sum_n 2^{\alpha\omega_K(n)-\alpha\omega(n)} n^{-s} = L_1(s)(\zeta_{K/\mathbb{Q}}(s))^{(2^{2\alpha}-1)/3} \zeta(s).$$

Both $\zeta(s)$ and $\zeta_{K/\mathbb{Q}}$ have a pole of order 1 at $s = 1$. By a Tauberian theorem (see, e.g., [PT], Main Th.) we can conclude that

$$\frac{1}{X} \sum_{n \le X} 2^{\alpha\omega_K(n)-\alpha\omega(n)} \sim C_{K,\alpha} (\log X)^{(2^{2\alpha}-1)/3}$$

for some positive constant $C_{K,\alpha} > 0$.

Now suppose that $K/\mathbb{Q}$ is not Galois. Denote the splitting type of a prime p in $K/\mathbb{Q}$ by $p = \mathfrak{p}_1\mathfrak{p}_2$, $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $p = \mathfrak{p}_1^2\mathfrak{p}_2$, etc. Then

$$\zeta_{K/\mathbb{Q}}(s) = \prod_{\mathfrak{p} \in I_K} \frac{1}{(1 - (N\mathfrak{p})^{-s})} = L_2(s) \prod_{p = \mathfrak{p}_1\mathfrak{p}_2} \frac{1}{(1 - p^{-s})} \prod_{p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} \frac{1}{(1 - p^{-s})^3},$$

where $L_2(s)$ is continuous, non-zero and bounded on $\{s : \Re s > 1 - \frac{1}{4}\}$. Let $L/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$. Let $K'/\mathbb{Q}$ be the quadratic subextension of $L/\mathbb{Q}$. Then

we obtain from Lemma 4.3.9 that

$$\prod_{p=\mathfrak{p}_1\mathfrak{p}_2} \frac{1}{(1-p^{-s})} = \prod_{p \text{ unsplit in } K'/\mathbb{Q}} \frac{1}{(1-p^{-s})} = L_3(s)\zeta(s)\zeta_{K'/\mathbb{Q}}^{-1/2}(s),$$

where $L_3(s)$ is continuous and bounded on $\{s : \Re s > 1 - \frac{1}{4}\}$.

Now

$$\begin{aligned}
2^{\alpha\omega_K(n)-\alpha\omega(n)} &= \prod_{\substack{p|n \\ p=\mathfrak{p}_1\mathfrak{p}_2}} 2^{\alpha} \prod_{\substack{p|n \\ p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}} 2^{2\alpha} \\
&= \prod_{\substack{p|n \\ p=\mathfrak{p}_1\mathfrak{p}_2}} (1+(2^{\alpha}-1)) \prod_{\substack{p|n \\ p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}} (1+(2^{2\alpha}-1)) \\
&= \sum_{\substack{abc=n \\ p|a \Rightarrow p=\mathfrak{p}_1\mathfrak{p}_2 \\ p|b \Rightarrow p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}} \prod_{p|a}(2^{\alpha}-1) \prod_{p|b}(2^{2\alpha}-1).
\end{aligned}$$

Hence

$$\begin{aligned}
\sum_n 2^{\alpha\omega_K(n)-\alpha\omega(n)} n^{-s} &= \left(\sum_n n^{-s}\right) \cdot \sum_{\substack{n \\ p|n \Rightarrow p=\mathfrak{p}_1\mathfrak{p}_2}} \prod_{p|n}(2^{\alpha}-1)n^{-s} \\
&\quad \cdot \sum_{\substack{n \\ p|n \Rightarrow p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3}} \prod_{p|n}(2^{2\alpha}-1)n^{-s} \\
&= \zeta(s) \prod_{p=\mathfrak{p}_1\mathfrak{p}_2} (1+(2^{\alpha}-1)p^{-s})^{-1} \prod_{p=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3} (1+(2^{2\alpha}-1)p^{-s})^{-1} \\
&= L_4(s)\zeta(s)(\zeta_{K/\mathbb{Q}}(s))^{(2^{2\alpha}-1)/3}(\zeta(s)\zeta_{K'/\mathbb{Q}}^{-1/2}(s))^{(2^{\alpha}-1)-(2^{2\alpha}-1)/3}.
\end{aligned}$$

Since $\zeta(s)$, $\zeta_{K/\mathbb{Q}}$ and $\zeta_{K'/\mathbb{Q}}$ each have a pole of order 1 at $s = 1$, we can apply a Tauberian theorem as before, obtaining

$$\frac{1}{X}\sum_{n \le X} 2^{\alpha\omega_K(n)-\alpha\omega(n)} \sim C_{K,\alpha}(\log X)^{\frac{1}{2}(2^{\alpha}-1)+\frac{1}{6}(2^{2\alpha}-1)}.$$

□

4.3.4 The square-free sieve for homogeneous quartics

We need the following simple lemma.

Lemma 4.3.11. *Let $f \in \mathbb{Z}[x, z]$ be a homogeneous polynomial. Then there is a constant C_f such that the following holds. Let N be a positive integer larger than C_f. Let p be a prime larger than N. Then there are at most $12\deg(f)$ pairs $(x, y) \in \mathbb{Z}^2$, $|x|, |z| \leq N$, $\gcd(x, z) = 1$, such that*

$$p^2 | f(x, z). \tag{4.3.10}$$

Proof. If N is large enough, then p does not divide the discriminant of f. Hence

$$f(r, 1) \equiv 0 \bmod p^2 \tag{4.3.11}$$

has at most $\deg(f)$ solutions in $\mathbb{Z}/p^2$. If N is large enough for p^2 not to divide the leading coefficients of f, then $(x, z) = (1, 0)$ does not satisfy (4.3.10). Therefore, any solution (x,z) to (4.3.10) gives us a solution $r = x/z$ to (4.3.11). We can focus on solutions $(x, y) \in \mathbb{Z}^2$ to (4.3.10) with x, y non-negative, as we need only flip signs to repeat the procedure for the other quadrants.

Suppose we have two solutions $(x_0, z_0), (x_1, z_1) \in \mathbb{Z}^2$, $0 \leq |x_0|, |x_1|, |z_0|, |z_1| \leq N$, $\gcd(x_0, z_0) = \gcd(x_1, z_1) = 1$, such that

$$x_0/z_0 \equiv r \equiv x_1/z_1 \bmod p^2.$$

Then

$$x_0 z_1 - x_1 z_0 \equiv 0 \bmod p^2.$$

Since $0 \leq x_j, z_j \leq N$ and $p > N$, we have that

$$-p^2 < x_0 z_1 - x_1 z_0 < p^2,$$

and thus $x_0 z_1 - x_1 z_0$ must be zero. Hence $x_0/z_0 = x_1/z_1$. Since $\gcd(x_0, z_0) = \gcd(x_1, z_1) = 1$ and $\operatorname{sgn}(x_0) = \operatorname{sgn}(x_1)$, it follows that $(x_0, z_0) = (x_1, z_1)$. $\square$

Remark. It was pointed out by Ramsay [Ra] that an idea similar to that in Lemma 4.3.11 suffices to improve Greaves's bound for homogeneous sextics [Gre] from $\delta(N) = N^2(\log N)^{-1/3}$ to $\delta(N) = N^2(\log N)^{1/2}$.

Proposition 4.3.12. *Let $f \in \mathbb{Z}[x, z]$ be a homogeneous irreducible polynomial of degree 4. Let*

$$\delta(N) = \{x, z \in \mathbb{Z}^2 : |x|, |z| \leq N, \gcd(x, z) = 1, \exists p > N \text{ s.t. } p^2 | f(x, y)\}.$$

Then

$$\delta(N) \ll N^{4/3}(\log N)^A,$$

where A and the implied constant depend only on f.

Proof. Write $A = \max_{|x|,|z| \leq N} f(x, z)$. Clearly $A \ll N^4$. We can write

$$\begin{aligned}\delta(N) \leq & \sum_{0<|d|\leq M} \#\{x, y, z \in \mathbb{Z}^3, |x|, |z| \leq N, \gcd(x, z) = 1 : dy^2 = f(x, z)\} \\ & + \sum_{N<p\leq\sqrt{A/M}} \#\{x, z \in \mathbb{Z}^2, |x|, |z| \leq N, \gcd(x, z) = 1 : p^2 | f(x, z)\}.\end{aligned}$$

Let $M \leq N^3$. By Lemma 4.3.11,

$$\sum_{N<p\leq\sqrt{A/M}} \#\{x, z \in \mathbb{Z}^2, |x|, |z| \leq N, \gcd(x, z) = 1 : p^2 | f(x, z)\} \ll \frac{1}{\log N}\sqrt{N^{4-\beta}},$$

where $\beta = (\log M)/(\log N)$. It remains to estimate

$$\sum_{0<|d|\leq M} S(d),$$

where we write

$$S(d) = \#\{x, y, z \in \mathbb{Z}^3, |x|, |z| \leq N, \gcd(x, z) = 1 : dy^2 = f(x, z)\}.$$

Let $C_{f,1}$, $C_{f,2}$, $C_{f,3}$, $C_{f,4}$ be as in Proposition 4.3.7. Let K, C_f, ω and ω_K be as in Lemma 4.3.8. Write $C_{f,5}$ for C_f.

By Proposition 4.3.7,

$$\sum_{0<|d|<C_{f,4}} S(d) \ll \left(1 + 2C_{f,3}\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{C_1} \ll (\log N)^{C_2},$$

where $C_1 = \max_{0<d<C_{f,4}} \operatorname{rank}(E_d)$, C_2 and the implied constant depend only on f. Let ϵ be a small positive real number. By Proposition 4.3.7 and Lemma 4.3.8,

$$\begin{aligned}\sum_{C_{f,4}\leq|d|<N^\epsilon} S(d) &\ll \sum_{C_{f,4}\leq|d|<N^\epsilon} \left(1 + 2\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{\operatorname{rank}(E_d)} \\ &\ll \sum_{C_{f,4}\leq|d|<N^\epsilon} \left(1 + 2\sqrt{\frac{7}{2}\log N + C_{f,1}}\right)^{C_{f,5}+\omega_K(d)-\omega(d)}.\end{aligned}$$

We have the following crude bounds:

$$\omega(d) \leq \frac{\log|d|}{\log\log|d|}, \quad \omega_K(d) \leq 3\omega(d). \tag{4.3.12}$$

Hence

$$\sum_{C_{f,4}\le|d|<N^\epsilon} S(d) \ll \sum_{C_{f,4}\le d<N^\epsilon} (\log N)^{C_{f,5}+2\log d/\log\log d}$$
$$\le N^\epsilon(\log N)^{C_1}(\log N)^{2\epsilon\log N/\log\log N}$$
$$\le (\log N)^{C_1}N^{3\epsilon},$$

where C depends only on f and ϵ. For any d with $|d| > N^\epsilon$, Proposition 4.3.7 and Lemma 4.3.8 give us

$$S(d) \ll \left(1+2\sqrt{(\frac{7}{2}\log N + C_{f,1})/(\frac{1}{8}\epsilon\log N + C_{f,2})}\right)^{\mathrm{rank}(E_d)}$$
$$\ll (12\epsilon^{-1/2})^{C_{f,5}+\omega_K(d)-\omega(d)} \le 2^{C_2\omega_K(d)-C_2\omega_K(d)},$$

where C_2 depends only on f and ϵ. By Lemma 4.3.10 we can conclude that

$$\sum_{N^\epsilon<|d|\le M} S(d) \ll \sum_{d=1}^{M} 2^{C_2\omega_K(d)-C_2\omega_K(d)}$$
$$\ll C_3M(\log N)^{C_4},$$

where C_3 and C_4 depend only on f and ϵ. Set $M = N^{4/3}$, $\epsilon = 1/4$. □

4.3.5 Homogeneous cubics

Proposition 4.3.13. *Let $f \in \mathbb{Z}[x,z]$ be a homogeneous irreducible polynomial of degree 3. Let*

$$\delta(N) = \{x,z\in\mathbb{Z}^2 : |x|,|z|\le N, \gcd(x,z)=1, \exists p>N \ s.t. \ p^2|f(x,y)\}.$$

Then

$$\delta(N) \ll N^{4/3}(\log N)^A,$$

where A and the implied constant depend only on f.

Proof. Write $A = \max_{|x|,|z|\le N} f(x,z)$. Clearly $A \ll N^4$. We can write

$$\delta(N) \le \sum_{0<|d|\le M} \#\{x,y,z \in \mathbb{Z}^3, |x|,|z| \le N, \gcd(x,z)=1 : dy^2 = f(x,z)\}$$
$$+ \sum_{N<p\le\sqrt{A/M}} \#\{x,z \in \mathbb{Z}^2, |x|,|z| \le N, \gcd(x,z)=1 : p^2 | f(x,z)\}.$$

Let $M \le N^2$. By Lemma 4.3.11, the second term on the right is $O(N^{2-\beta/2}/\log N)$. Now notice that any point $(x,y,z) \in \mathbb{Z}^3$ on $dy^2 = f(x,z)$ gives us a rational point $(x',y') = (x/z, y/z^2)$ on

$$d'y'^2 = f(x',1), \tag{4.3.13}$$

where $d' = dz$. Moreover, a rational point on (4.3.13) can arise from at most one point $(x,y,z) \in \mathbb{Z}^3$, $\gcd(x,z)=1$, in the given fashion.

If $d \le M$, then $|d'| = |dz| \le MN$. The height $h_x(P)$ of the point $P = (x/z, y/z^2)$ is at most N. It follows by Lemma 4.3.1 that $\hat{h}(P) \le N + C_f$, where C_f is a constant depending only on f. By Corollaries 4.3.3 and 4.3.5, there are at most

$$O((1+2\sqrt{(\log N + C_f')/(\log|d| + C_f)})^{\mathrm{rank}(E_d)})$$

rational points P of height $\hat{h}(P) \le N + C_f$. We proceed as in Proposition 4.3.12, and obtain that

$$\sum_{0<|d|\le M} \#\{x,y,z \in \mathbb{Z}^3, |x|,|z| \le N, \gcd(x,z)=1 : dy^2 = f(x,z)\}$$

is at most $O(MN(\log N))^A$. Set $\beta = 1/3$. □

4.3.6 Homogeneous quintics

We extract the following result from [Gre].

Lemma 4.3.14. *Let $f \in \mathbb{Z}[x,y]$ be a homogeneous irreducible polynomial of degree at most 5. For all $M < N^{\deg f}$, $\epsilon > 0$,*

$$\sum_{d=1}^{M} \#\{x,y,z \in \mathbb{Z}^3, |x|,|z| \leq N, \gcd(x,z)=1 : dy^2 = f(x,z)\} \ll N^{(18-\frac{1}{2}\beta^2)/(10-\beta)+\epsilon}, \tag{4.3.14}$$

where $\beta = (\log M)/(\log N)$. The implied constant depends only on f and ϵ.

Proof. By [Gre], Lemmas 5 and 6, where the parameters d and z (in the notation of [Gre], not ours) are set to the values $d = 1$ and $z = N^{(1-\beta/2)/(5/2-\beta/4)}$. □

Proposition 4.3.15. *Let $f \in \mathbb{Z}[x,z]$ be a homogeneous irreducible polynomial of degree 5. Let*

$$\delta(N) = \{x,z \in \mathbb{Z}^2 : |x|,|z| \leq N, \gcd(x,z)=1, \exists p > N \text{ s.t. } p^2 | P(x,y)\}.$$

Then, for any $\epsilon > 0$,

$$\delta(N) \ll N^{(5+\sqrt{113})/8+\epsilon}$$

where the implied constant depends only on f and ϵ.

Proof. Let $A = \max_{|x|,|z|\leq N} f(x,z)$. Clearly $A \ll N^{\deg(f)}$. We can write

$$\begin{aligned}\delta(N) \leq &\sum_{0<|d|\leq M} \#\{x,y,z \in \mathbb{Z}^3, |x|,|z| \leq N, \gcd(x,z)=1 : dy^2 = f(x,z)\} \\ &+ \sum_{N<p\leq\sqrt{A/M}} \#\{x,z \in \mathbb{Z}^2, |x|,|z| \leq N, \gcd(x,z)=1 : p^2 | f(x,z)\}.\end{aligned}$$

By Lemmas 4.3.14 and 4.3.11,

$$\delta(N) \ll N^{(18-\frac{1}{2}\beta^2)/(10-\beta)+\epsilon} + \frac{1}{\log N}\sqrt{N^{\deg(f)-\beta}},$$

where $\beta = (\log M)/(\log N)$. Set $\beta = (15-\sqrt{113})/4$. □

4.3.7 Quasiorthogonality, kissing numbers and cubics

Lemma 4.3.16. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. Let d be a square-free integer. Then, for any two distinct integer points $P = (x, y) \in \mathbb{Z}^2$, $P' = (x', y') \in \mathbb{Z}^2$ on the elliptic curve*

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

we have

$$\hat{h}(P + P') \leq 3 \max(\hat{h}(P), \hat{h}(P')) + C_f,$$

where C_f is a constant depending only on f.

Proof. Write $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. Let $P + P' = (x'', y'')$. By the group law,

$$\begin{aligned} x'' &= \frac{d(y_2 - y_1)^2}{a_3(x_2 - x_1)^2} - \frac{a_2}{a_3} - x_1 - x_2 \\ &= \frac{d(y_2 - y_1)^2 - a_2(x_2 - x_1)^2 - a_3(x_2 - x_1)^2(x_1 + x_2)}{a_3(x_2 - x_1)^2}. \end{aligned}$$

Clearly $|a_3(x_2 - x_1)^2| \leq 4|a_3| \max(|x_1|^2, |x_2|^2)$. Now

$$|d(y_2 - y_1)^2| \leq 4|d| \max(y_1^2, y_2^2) = 4 \max(|f(x_1)|, |f(x_2)|).$$

Hence

$$|d(y_2 - y_1)^2 - a_2(x_2 - x_1)^2 - a_3(x_2 - x_1)^2(x_1 + x_2) \leq A \max(|x|^3, |x'|^3),$$

where A is a constant depending only on f. Therefore

$$\begin{aligned} h_x(P) &= \log(\max(|\operatorname{num}(x'')|, |\operatorname{den}(x'')|)) \\ &\leq 3\max(\log|x|, \log|x'|) + \log A \\ &\leq 3\max(h_x(P), h_x(P')) + \log A. \end{aligned}$$

By Lemma 4.3.1, the difference $|\hat{h} - h_x|$ is bounded by a constant independent of d. The statement follows immediately. $\square$

Consider the elliptic curve

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

There is a $\mathbb{Z}$-linear map from $E_d(\mathbb{Q})$ to $\mathbb{R}^{\operatorname{rank}(E_d)}$ taking the canonical height to the square of the Euclidean norm. In other words, any given integer point $P = (x, y) \in E_d$ will be taken to a point $L(P) \in \mathbb{R}^{\operatorname{rank}(E_d)}$ whose Euclidean norm $|L(P)|$ satisfies

$$|L(P)|^2 = \hat{h}(P) = \log x + O(1),$$

where the implied constant depends only on f. In particular, the set of all integer points $P = (x, y) \in E_d$ with

$$N^{1-\epsilon} \leq x \leq N \tag{4.3.15}$$

will be taken to a set of points $L(P)$ in $\mathbb{R}^{\operatorname{rank}(E_d)}$ with

$$(1-\epsilon)\log N + O(1) \leq |L(P)|^2 \leq \log N + O(1).$$

Let $P, P' \in E_d$ be integer points satisfying (4.3.15). Assume $L(P) \neq L(P')$. By

Lemma 4.3.16,

$$|L(P)+L(P')|^2 = |L(P+P')|^2 \leq 3\max(|L(P)|^2, |L(P')|^2) + O(1).$$

Therefore, the inner product $L(P)\cdot L(P')$ satisfies

$$\begin{aligned}
L(P)\cdot L(P') &= \frac{1}{2}(|L(P)+L(P')|^2 - (|L(P)|^2 + |L(P')|^2)) \\
&\leq \frac{1}{2}(3\max(|L(P)|^2, |L(P')|^2) + O(1) - (|L(P)|^2 + |L(P')|^2)) \\
&\leq \frac{1}{2}((1+\epsilon)\log(N) + O(1)) \\
&\leq \frac{1}{2}\frac{(1+\epsilon)+O((\log N)^{-1})}{(1-\epsilon)^2}|L(P)||L(P')|.
\end{aligned}$$

We have proven

Lemma 4.3.17. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. Let d be a square-free integer. Consider the elliptic curve*

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

Let S be the set

$$\{(x,y) \in \mathbb{Z}^2 : N^{1-\epsilon} \leq |x| \leq N, dy^2 = f(x)\}.$$

Let L be a linear map taking $E(\mathbb{Q})$ to $\mathbb{R}^{\mathrm{rank}(E_d)}$ and the canonical height $\hat{h}$ to the square of the Euclidean norm. Then, for any distinct points $P, P' \in L(S) \subset \mathbb{R}^{\mathrm{rank}(E_d)}$ with the angle θ between P and P' is at least

$$\arccos\left(\frac{1}{2}\frac{(1+\epsilon)+O((\log N)^{-1})}{(1-\epsilon)^2}\right) = 60^\circ + O(\epsilon + (\log N)^{-1}),$$

where the implied constant depends only on f.

Let $A(\theta, n)$ be the maximal number of points that can be arranged in $\mathbb{R}^n$ with

angular separation no smaller than θ. Kabatiansky and Levenshtein ([KL]; vd. also [CS], (9.6)) show that, for n large enough,

$$\frac{1}{n}\log_2 A(n,\theta) \leq \frac{1+\sin\theta}{2\sin\theta}\log_2\frac{1+\sin\theta}{2\sin\theta} - \frac{1-\sin\theta}{2\sin\theta}\log_2\frac{1-\sin\theta}{2\sin\theta}.$$

Thus we obtain

Corollary 4.3.18. *Let $f \in \mathbb{Z}[x]$ be a cubic polynomial of non-zero discriminant. Let d be a square-free integer. Consider the elliptic curve*

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

Let S be the set

$$\{(x,y) \in \mathbb{Z}^2 : N^{1-\epsilon} \leq |x| \leq N, dy^2 = f(x)\}.$$

Then

$$\#S \ll 2^{(\alpha + O(\epsilon + (\log N)^{-1}))\operatorname{rank}(E_d)},$$

where

$$\alpha = \frac{2+\sqrt{3}}{2\sqrt{3}}\log_2\frac{2+\sqrt{3}}{2\sqrt{3}} + \frac{2-\sqrt{3}}{2\sqrt{3}}\log_2\frac{2-\sqrt{3}}{2\sqrt{3}}$$

and the implied constants depend only on f.

Notice that we are using the fact that the size of the torsion group is bounded.

Proposition 4.3.19. *Let $f \in \mathbb{Z}[x]$ be an irreducible cubic polynomial. Let*

$$\delta(N) = \{1 \leq x \leq N : \exists p > N^{1/2} \text{ s.t. } p^2 | f(x)\}.$$

Then

$$\delta(N) \ll N(\log N)^{-\beta}, \tag{4.3.16}$$

where

$$\beta = -((2^{2\alpha} - 1)/9 - 2/3) = 0.5839\ldots$$

if the discriminant of f is a square,

$$\beta = -\left(\frac{1}{6}(2^{\alpha} - 1) + \frac{1}{18}(2^{2\alpha} - 1) - 2/3\right) = 0.5718\ldots$$

if the discriminant of f is not a square, and

$$\alpha = \frac{2+\sqrt{3}}{2\sqrt{3}} \log_2 \frac{2+\sqrt{3}}{2\sqrt{3}} + \frac{2-\sqrt{3}}{2\sqrt{3}} \log_2 \frac{2-\sqrt{3}}{2\sqrt{3}} = 0.4014\ldots.$$

The implied constant in (4.3.16) depends only on f.

Proof. Let $A = \max_{1 \le x \le N} f(x)$. Clearly $A \ll N^3$. We can write

$$\begin{aligned}\delta(N) \le & \sum_{N^{1/2} < p < \sqrt{A/M}} \#\{1 \le x \le N : p^2 | f(x)\} \\ & + \{1 \le x \le N^{1-\epsilon} : \exists p > N^{1/2} \text{ s.t. } p^2 | f(x)\} \\ & + \sum_{1 \le |d| \le M} \#\{x, y \in \mathbb{Z}^2 : N^{1-\epsilon} \le x \le N, dy^2 = f(x)\}.\end{aligned}$$

Let $M \le N^2$. Then the first term is at most

$$\sum_{N^{1/2} < p < \sqrt{A/M}} 3 \ll \frac{3\sqrt{A/M}}{\log \sqrt{A/M}} \ll \frac{N^{3/2} M^{-1/2}}{\log N}.$$

The second term is clearly no greater than $N^{1-\epsilon}$. It remains to bound

$$\sum_{1 \le |d| \le M} B(d),$$

where

$$B(d) = \#\{x, y \in \mathbb{Z}^2 : N^{1-\epsilon} \le x \le N, dy^2 = f(x)\}.$$

By Lemma 4.3.8 and Corollary 4.3.18

$$B(d) \ll 2^{(\alpha+O(\epsilon+(\log N)^{-1}))(\omega_K(d)-\omega(d))},$$

where K is as in Lemma 4.3.8 and α is as in Corollary 4.3.18. Thanks to (4.3.12), we can omit the term $O((\log N)^{-1})$ from the exponent. Hence it remains to estimate

$$S(M) = \sum_{1\le d\le M} 2^{(\alpha+O(\epsilon))(\omega_K(d)-\omega(d))}.$$

By Lemma 4.3.10,

$$S(M) \ll M(\log M)^{(2^{2(\alpha+\epsilon)}-1)/3} \text{ if } K/\mathbb{Q} \text{ is Galois,}$$
$$S(M) \ll M(\log M)^{\frac{1}{2}(2^{\alpha+\epsilon}-1)+\frac{1}{6}(2^{2(\alpha+\epsilon)}-1)} \text{ if } K/\mathbb{Q} \text{ is not Galois.}$$

Let $\epsilon = (\log\log M)^{-1}$. Note that $K/\mathbb{Q}$ is Galois if and only if the discriminant of f is a square. Then

$$S(M) \ll M(\log M)^{(2^{2\alpha}-1)/3} \text{ if } \mathrm{Disc}(f) \text{ is a square,}$$
$$S(M) \ll M(\log M)^{\frac{1}{2}(2^{\alpha}-1)+\frac{1}{6}(2^{2\alpha}-1)} \text{ if } \mathrm{Disc}(f) \text{ is not a square.}$$

Set

$$M = N(\log N)^{-2(2^{2\alpha}-1)/9-2/3} \text{ if } \mathrm{Disc}(f) \text{ is a square,}$$
$$M = N(\log N)^{-\frac{1}{3}(2^{\alpha}-1)-\frac{1}{9}(2^{2\alpha}-1)-2/3} \text{ if } \mathrm{Disc}(f) \text{ is not a square.}$$

Hence

$$S(M) = N(\log N)^{(2^{2\alpha}-1)/9-2/3} \text{ if } \mathrm{Disc}(f) \text{ is a square,}$$
$$S(M) = N(\log N)^{\frac{1}{6}(2^{\alpha}-1)+\frac{1}{18}(2^{2\alpha}-1)-2/3} \text{ if } \mathrm{Disc}(f) \text{ is not a square.}$$

The statement follows. □

4.4 Square-free integers

In Chapter 2, we had the chance to employ the framework from section 4.2 in its full generality. We will now give a simpler and more traditional application.

Theorem 4.4.1. *Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree 3. Then the number of positive integers $x \leq N$ for which $f(x)$ is square-free is given by*

$$N \prod_p \left(1 - \frac{\ell(p^2)}{p^2}\right) + O(N(\log N)^{-\beta}), \tag{4.4.1}$$

where

$$\beta = \begin{cases} 0.5839\ldots & \text{if the discriminant of } f \text{ is a square,} \\ 0.5718\ldots & \text{if the discriminant of } f \text{ is not a square,} \end{cases}$$

$$\ell(m) = \#\{x \in \mathbb{Z}/m : f(x) \equiv 0 \bmod m\}.$$

Note that ϵ is an arbitrarily small positive number, and that the implied constant depends in (4.4.1) depends only on f and ϵ.

Proof. Define the terms needed for Lemma 4.2.1 as follows. Let $K = \mathbb{Q}$. Let $\gamma(d) = d\,\mathrm{rad}(d)$. Let $S_a = \{\emptyset\}$ for every $a \in \mathbb{Z}^+$; let $\phi_{a_1,a_2} : S_{a_2} \to S_{a_1}$ be the map taking $\emptyset$ to $\emptyset$. Define

$$f_a(\emptyset) = \begin{cases} 1 & \text{if } a = 1, \\ 0 & \text{otherwise,} \end{cases}$$

$$g_a(\emptyset) = \sum_{\substack{1 \leq x \leq N \\ \mathrm{sq}(f(x)) = a}} 1.$$

Then the cardinality of $\{1 \leq x \leq N : f(x) \text{ square-free}\}$ equals

$$\sum_{a \in \mathbb{Z}^+} \sum_{r \in S_a} f_a(r) g_a(r),$$

which is the expression on the left side of the inequality (4.2.1). It remains to estimate

the right side.

Write $f(a)$, $g(a)$ instead of $f_a(\emptyset)$, $g_a(\emptyset)$ for the sake of brevity. Then

$$\sum_{\gamma(d)\le M}\sum_{r\in S_d}\left(\sum_{d'|d}\mu(d')f(d/d')\right)t_d(r)=\sum_{\gamma(d)\le M}\mu(d)t_d(r)=\sum_{\gamma(d)\le M}\mu(d)\sum_{\substack{1\le x\le N\\ d|\operatorname{sq}(f(x))}}1$$
$$=\sum_{d^2\le M}\mu(d)\sum_{\substack{1\le x\le N\\ d^2|f(x)}}1.$$

Assume $M\le N$. Then

$$\begin{aligned}\sum_{d^2\le M}\mu(d)\sum_{\substack{1\le x\le N\\ d^2|f(x)}}1&=\sum_{\substack{d\text{ square-free}\\ d^2\le M}}\mu(d)\frac{N\ell(d^2)}{d^2}+O(M^{1/2})\\&=\sum_{d}\mu(d)\frac{N\ell(d^2)}{d^2}-\sum_{d^2>M}\mu(d)\frac{N\ell(d^2)}{d^2}+O(M^{1/2})\\&=N\prod_p\left(1-\frac{\ell(p^2)}{p^2}\right)+O\left(N\sum_{d^2>M}\frac{\tau_3(d)}{d^2}+M^{1/2}\right)\\&=N\prod_p\left(1-\frac{\ell(p^2)}{p^2}\right)+O(NM^{-1/2}(\log N)^3).\end{aligned}$$

Assume $M\le\sqrt{N}$. We may now bound the second term on the right side of (4.2.1). By Lemmas 4.2.3 and 4.2.15,

$$\begin{aligned}\sum_{M<\gamma(d)\le M^2}\tau_3(d)s_d&=\sum_{M<\gamma(d)\le M^2}\tau_3(d)\sum_{\substack{1\le x\le N\\ \gamma(d)|f(x)}}1\\&\ll\sum_{M<\gamma(d)\le M^2}\tau_3(d)\tau_3(\operatorname{rad}(d))\frac{N}{\gamma(d)}\\&\ll M^{-1/2}N(\log M)^{9^2+9^3-2}.\end{aligned}$$

The remaining term of (4.2.1) is

$$2\sum_{\substack{p\\ p^2>M}} s_p = 2\sum_{p>\sqrt{M}}\sum_{\substack{1\le x\le N\\ p^2|f(x)}} 1 = 2\sum_{\sqrt{M}<p\le N^{1/2}}\sum_{\substack{1\le x\le N\\ p^2|f(x)}} 1 + 2\sum_{p>N^{1/2}}\sum_{\substack{1\le x\le N\\ p^2|f(x)}} 1.$$

By Lemma 4.2.15,

$$\sum_{\sqrt{M}<p\le N^{1/2}}\sum_{\substack{1\le x\le N\\ p^2|f(x)}} 1 \ll \sum_{p\ge\sqrt{M}} \frac{N}{p^2} \ll M^{-1/2}N.$$

Hence we have

$$\#\{1\le x\le N : f(x) \text{ square-free}\} = N\prod_p\left(1-\frac{\ell(p)}{p^2}\right) + 2\sum_{\substack{p>N^{1/2}\\ p^2|f(x)}} 1 + O(NM^{-1/2}(\log M)^{9^2+9^3-2}).$$

Set $M = N^{1/2}$. Notice that, for N large enough, no more than three squares of primes p^2, $p > N^{1/2}$, may divide $f(x)$ for any $1 \le x \le N$. Thus

$$\sum_{\substack{p>N^{1/2}\\ p^2|f(x)}} 1 \ll \{1\le x\le N : \exists p > N^{1/2} \text{ s.t. } p^2|f(x)\}.$$

By Proposition 4.3.19, the statement follows. □

Theorem 4.4.2. *Let $f \in \mathbb{Z}[x,y]$ be a homogeneous polynomial of degree no greater than 6. Then the number of integer pairs $(x,y) \in \mathbb{Z}^2 \cap [-N,N]^2$ for which $f(x,y)$ is*

square-free is given by

$$4N^2\prod_p\left(1-\frac{\ell_2(p^2)}{p^4}\right)+\begin{cases}O(N(\log N)^{A_1}) & \text{if } \deg_{\mathrm{irr}}(f)=1,2,\\ O(N^{4/3}(\log N)^{A_2}) & \text{if } \deg_{\mathrm{irr}}(f)=3,4,\\ O(N^{(5+\sqrt{113})/8+\epsilon}) & \text{if } \deg_{\mathrm{irr}}(f)=5,\\ O(N^2(\log N)^{-1/2}) & \text{if } \deg_{\mathrm{irr}}(f)=6,\end{cases}$$

where ϵ is an arbitrarily small positive number, A_1 is an absolute constant, A_2 depends only on f, the implied constant depends only on f and ϵ, $\deg_{\mathrm{irr}}$ denotes the degree of the irreducible factor of f of largest degree, and

$$\ell_2(m)=\#\{(x,y)\in(\mathbb{Z}/m)^2 : f(x,y)\equiv 0 \bmod m\}.$$

Proof. Set K, γ, S_a, ϕ_{a_1,a_2} and f_a as in the proof of Theorem 4.4.1. Let

$$g_a(\emptyset)=\sum_{\substack{(x,y)\in\mathbb{Z}^2\cap[-N,N]^2\\ \mathrm{sq}(f(x))=a}}1.$$

We proceed as in Theorem 4.4.1. Let $M\le N$. Then

$$\begin{aligned}\sum_{d^2\le M}\mu(d)\sum_{\substack{(x,y)\in\mathbb{Z}^2\cap[-N,N]^2\\ d^2|f(x)}}1&=\sum_{d^2\le M}\mu(d)\frac{4N^2\ell_2(d^2)}{d^4}+O(M^{1/2}N)\\ &=\sum_{d}\mu(d)\frac{4N^2\ell_2(d^2)}{d^4}-\sum_{d^2>M}\mu(d)\frac{4N^2\ell_2(d^2)}{d^4}+O(M^{1/2}N)\\ &=4N^2\prod_p\left(1-\frac{\ell_2(p^2)}{p^4}\right)+O(N^2M^{-1/2}(\log N)^3).\end{aligned}$$

Notice that the first equality is justified even for $M>N^{1/2}$, as the solutions to $d^2|f(x)$ fall into lattices of index d^2 with $d\mathbb{Z}^2$ as their pairwise intersection. By Lemmas 2.2.1

and 4.2.15,

$$\begin{aligned}\sum_{M<\gamma(d)\le M^2} \tau_3(d)s_d &= \sum_{M<\gamma(d)\le M^2} \tau_3(d) \sum_{\substack{(x,y)\in\mathbb{Z}^2\cap[-N,N]^2\\ \gamma(d)|f(x)}} 1 \\ &\ll \sum_{M<\gamma(d)\le M^2} \tau_3(d)\tau_{12}(\mathrm{rad}(d))\frac{N^2}{\gamma(d)} \\ &\ll M^{-1/2}N^2(\log M)^{A_1},\end{aligned}$$

where $A_1 = 36^2 + 36^3 - 2$. The remaining term is

$$2\sum_{\substack{p\\ p^2>M}} s_p = \sum_{p>\sqrt{M}} \sum_{\substack{(x,y)\in\mathbb{Z}^2\cap[-N,N]^2\\ p^2|f(x)}} 1,$$

which is at most a constant times

$$M^{-1/2}N^2 + \{x, z \in \mathbb{Z}^2 : |x|, |z| \le N, \gcd(x,z) = 1, \exists p > N \text{ s.t. } p^2|f(x,y)\}.$$

Use Prop. 4.3.13 for $\deg_{\mathrm{irr}}(f) = 3$, Prop. 4.3.12 for $\deg_{\mathrm{irr}}(f) = 4$ and Prop. 4.3.15 for $\deg_{\mathrm{irr}}(f) = 5$. Use the trivial bound for $\deg_{\mathrm{irr}}(f) = 1, 2$, and the estimate in [Gre], Lemma 3, for $\deg_{\mathrm{irr}}(f) = 6$. $\square$

Appendix A

Addenda on the root number

A.1 Known instances of conjectures $\mathfrak{A}_i$ and $\mathfrak{B}_i$ over the rationals

The quantitative versions of $\mathfrak{A}_i$ and $\mathfrak{B}_i$ were introduced in subsections 2.4.1 and 2.5.3. As before, we denote by $\deg_{\mathrm{irr}} P$ the degree of the irreducible factor of P of highest degree.

Proposition A.1.1. *Conjecture* $\mathfrak{A}_1(\mathbb{Q}, P, \delta(N))$ *holds for*

1. $\deg_{\mathrm{irr}} P = 1$, $\delta(N) = \sqrt{N}$,
2. $\deg_{\mathrm{irr}} P = 2$, $\delta(N) = N^{2/3}$,
3. $\deg_{\mathrm{irr}} P = 3$, $\delta(N) = N(\log N)^{-0.5839\ldots}$ *if the discriminants of all irreducible factors of degree* 3 *of* P *are square,*
4. $\deg_{\mathrm{irr}} P = 3$, $\delta(N) = N(\log N)^{-0.5718\ldots}$, *in general.*

Proof. The case $\deg_{\mathrm{irr}} P = 1$ is trivial. The result for $\deg_{\mathrm{irr}} P = 2$ is due to Estermann ([Es]). See Chapter 4 for $\deg_{\mathrm{irr}} P = 3$. The best previous bound for $\deg_{\mathrm{irr}} P = 3$, namely $\delta(N) = N(\log N)^{-1/2}$, was due to Hooley ([Hoo], Ch. IV). $\square$

Proposition A.1.2. *Conjecture* $\mathfrak{A}_2(\mathbb{Q}, P, \delta(N))$ *holds for*

1. $\deg_{\text{irr}} P = 1$, $\delta(N) = 1$,

2. $\deg_{\text{irr}} P = 2$, $\delta(N) = N$,

3. $\deg_{\text{irr}} P = 3$, $\delta(N) = N^{3/2}/(\log N)$,

4. $\deg_{\text{irr}} P = 4$, $\delta(N) = N^{4/3}(\log N)^A$,

5. $\deg_{\text{irr}} P = 5$, $\delta(N) = N^{(5+\sqrt{113})/8+\epsilon}$,

6. $\deg_{\text{irr}} P = 6$, $\delta(N) = N^2/(\log N)^{1/2}$,

where ϵ *is an arbitrarily small positive integer, and* A *and the implied constant depends only on* ϵ.

Proof. The cases $\deg_{\text{irr}} P = 1$ and $\deg_{\text{irr}} P = 2$ are trivial. See Chapter 4 for $3 \leq \deg_{\text{irr}} P \leq 6$. The best previous bound for $\deg_{\text{irr}} P = 3, 4, 5$ was $N^2(\log N)^{-1}$, due to Greaves [Gre]. While, in the cited work, Greaves gives the bound $N^2(\log N)^{-1/3}$, his methods suffice to obtain $N^2(\log N)^{-1/2}$, as was remarked by Ramsay ([Ra], 1991, unpublished; see reference in [GM]). □

Proposition A.1.3. *Hypothesis* $\mathfrak{B}_1(\mathbb{Q}, P, \eta(N), \epsilon(N))$ *holds for* $\deg P = 1$, $\eta(N) = (\log N)^A$, $\epsilon(N) = C_1 e^{-C_2(\log N)^{3/5}/(\log\log N)^{1/5}}$, *where* A *is arbitrarily large and* C_1, C_2 *depend on* A *and* P.

Proof. By Siegel-Walfisz (vd. [Wa], V §5 and V §7). (For an elementary proof of equivalence with the Prime Number Theorem, see, e.g., [A].) □

Proposition A.1.4. *Hypothesis* $\mathfrak{B}_2(\mathbb{Q}, P, \eta(N), \epsilon(N))$ *holds for*

1. $\deg(P) = 1$, $\eta(N) = (\log N)^A$, $\epsilon(N) = C_1 e^{-C_2(\log N)^{3/5}/(\log\log N)^{1/5}}$, A *arbitrarily large,* C_1, C_2 *depending on* A *and* P,

2. $\deg(P) = 2$, $\eta(N) = (\log N)^A$, $\epsilon(N) = C_1 e^{-C_2(\log N)^{3/5-\epsilon}}$, *$A$ arbitrarily large, ϵ an arbitrarily small positive number, C_1, C_2 depending on A, P and ϵ,*

3. $\deg(P) = 3$, *P reducible,* $\eta(N) = (\log N)^A$, $\epsilon(N) = C\frac{\log\log N}{\log N}$, *$A$ arbitrarily large, C depending on A and P,*

4. $\deg(P) = 3$, *P irreducible,* $\eta(N) = (\log N)^A$, $\epsilon(N) = C\frac{(\log\log N)^5 \log\log\log N}{\log N}$, *$A$ arbitrarily large, C depending on A and P.*

Proof. The case $\deg P = 1$ follows immediately from Proposition A.1.3. For $\deg P = 2, 3$, see Chapter 3. As was said before, the case $\deg P = 2$ is in essence well-known and classical. □

A.2 Reducing hypotheses on number fields to their rational analogues

Given a number field K and a polynomial $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathfrak{O}_K[x]$ (or a homogeneous polynomial $P(x, y) = a_n x^n + a_{n-1}x^{n-1}y + \cdots + a_0 \in \mathfrak{O}_K[x, y]$), we define

$$K_P = \mathbb{Q}\left(\frac{a_{n-1}}{a_n}, \frac{a_{n-2}}{a_n}, \cdots, \frac{a_0}{a_n}\right).$$

Lemma A.2.1. *Let K be a number field. Let $P \in \mathfrak{O}_K[x]$ be a monic, irreducible polynomial. Suppose $K = K_P$. Then there is a finite set D of rational primes such that for every $x \in \mathbb{Z}$ and every rational prime p not in D,*

1. *at most one prime ideal $\mathfrak{p} \in I_K$ lying over p divides $P(x)$,*

2. *if some $\mathfrak{p} \in I_K$ lying over p divides $P(x)$, then $\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p} = p$,*

3. $\sum_{\mathfrak{p}\in I_K, \mathfrak{p}|p} v_{\mathfrak{p}}(P(x)) = v_p(\mathfrak{N}_{K/\mathbb{Q}}P(x))$.

Proof. Let $L/\mathbb{Q}$ be the Galois closure of $K/\mathbb{Q}$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$, $H = \mathrm{Gal}(L/K)$. Then for any ideal $\mathfrak{a} \in I_K$,

$$\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{a} = \prod_{\sigma H} \sigma\mathfrak{a},$$

where the product is taken over all cosets $\sigma H \subset G$ of H. Let σ be an element of G not in H. By definition, σ cannot leave K fixed. Since the ratios among the coefficients of P generate $K_P = K$, σ would leave K fixed if P_σ were a multiple of P. Hence P_σ is not a multiple of P. Since P is irreducible, it follows that P and P_σ are coprime. Let D be the set of all rational primes lying under prime ideals dividing $\mathrm{Disc}(P, P_\sigma)$ for some $\sigma \in G$ not in H.

Suppose there are two distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2 \in I_K$ such that $\mathfrak{p}_1, \mathfrak{p}_2 | P(x)$, $\mathfrak{p}_1, \mathfrak{p}_2 | p$, $p \notin D$. Then $\mathfrak{p}_1' | \mathfrak{p}_1$, $\mathfrak{p}_2' | \mathfrak{p}_2$ for some prime ideals $\mathfrak{p}_1', \mathfrak{p}_2' \in I_L$. There is a $\sigma \in G$ such that $\sigma\mathfrak{p}_1' = \mathfrak{p}_2'$. Then $\mathfrak{p}_2'$ divides both P and P_σ. Since $\mathfrak{p}_1 \neq \mathfrak{p}_2$, σ does not fix K. Hence $\sigma \notin H$. Therefore $\mathfrak{p}_2' | \mathrm{Disc}(P, P_\sigma)$, and thus $\mathfrak{p}_2'$ must lie over a prime in D. Contradiction. Hence (1) is proven.

Now take $\mathfrak{p} \in I_K$ lying over $p \notin D$. Assume $\mathfrak{p} | P(x)$ for some $x \in \mathbb{Z}$. Obviously

$$\mathfrak{N}_{L/\mathbb{Q}}\mathfrak{p} = \prod_{\sigma \in G} \sigma\mathfrak{p} = \left(\prod_{\sigma H} \sigma\mathfrak{p} \right)^{\deg L/K}.$$

Since $p \notin D$ and $\mathfrak{p} | P(x)$, we have $\gcd(\sigma\mathfrak{p}, \sigma'\mathfrak{p}) = 1$ for σ, σ' with $\sigma H \notin \sigma' H$. Therefore $\prod_{\sigma H} \sigma\mathfrak{p}$ divides p. Hence $\mathfrak{N}_{L/\mathbb{Q}}\mathfrak{p} | p^{\deg L/K}$. Since $\mathfrak{N}_{L/\mathbb{Q}}\mathfrak{p} = (\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p})^{\deg L/K}$, we have $\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p} | p$. Therefore $\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p} = p$; this is (2).

Finally,

$$v_p(\mathfrak{N}_{K/\mathbb{Q}}P(x)) = v_p\left(\mathfrak{N}_{K/\mathbb{Q}}\left(\prod_{\substack{\mathfrak{p}\in I_K\\ \mathfrak{p}|p}} \mathfrak{p}^{v_{\mathfrak{p}}(P(x))}\right)\right) = v_p\left(\prod_{\substack{\mathfrak{p}\in I_K\\ \mathfrak{p}|p}} (\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p})^{v_{\mathfrak{p}}(P(x))}\right)$$

$$= v_p\left(\prod_{\substack{\mathfrak{p}\in I_K\\ \mathfrak{p}|p}} p^{v_{\mathfrak{p}}(P(x))}\right) = \sum_{\substack{\mathfrak{p}\in I_K\\ \mathfrak{p}|p}} v_{\mathfrak{p}}(P(x)).$$

□

Lemma A.2.2. *Let K be a number field. Let $P \in \mathfrak{O}_K[x,y]$ be an irreducible polynomial. Suppose $K = K_P$. Then there is a finite set D of rational primes such that for all coprime $x, y \in \mathbb{Z}$ and every rational prime p not in D,*

1. *at most one prime ideal $\mathfrak{p} \in I_K$ lying over p divides $P(x,y)$,*
2. *if some $\mathfrak{p} \in I_K$ lying over p divides $P(x,y)$, then $\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p} = p$,*
3. *$\sum_{\mathfrak{p}\in I_K, \mathfrak{p}|p} v_{\mathfrak{p}}(P(x,y)) = v_p(\mathfrak{N}_{K/\mathbb{Q}}P(x,y))$.*

Proof. Same as that of Lemma A.2.1. □

Proposition A.2.3. *Let K be a number field. Let $P \in \mathfrak{O}_K[x]$ be a square-free, non-constant polynomial. Let $P = P_1P_2\cdots P_k$, P_i irreducible in $\mathfrak{O}_K[x]$. Then Conjecture $\mathfrak{A}_1(K, P, \delta(N))$ is equivalent to Conjecture $\mathfrak{A}_1(\mathbb{Q}, Q, \delta(N))$, where the polynomial $Q(x) \in \mathbb{Z}[x]$ is defined as the product of the irreducible factors of $\mathfrak{N}_{K_{P_i}/\mathbb{Q}}(c_iP_i(x)) \in \mathbb{Z}[x]$, $i = 1, \cdots, k$, where $c_1, \ldots, c_k$ are constants in $\mathfrak{O}_K$.*

Proof. Since $\mathfrak{A}_1(K, P_1 \cdot P_2, \delta(N))$ is equivalent to $\mathfrak{A}_1(K, P_1, \delta(N)) \wedge \mathfrak{A}_1(K, P_2, \delta(N))$, it is enough to prove the statement for P irreducible. Choose a non-zero $c \in \mathfrak{O}_K$ such that the leading coefficient of cP lies in K_P. Then all coefficients of cP lie in $\mathfrak{O}_{K_P}$. Since we can take $N^{1/2}$ to be larger than every prime divisor of c, it follows that we

can assume that P has all its coefficients in $\mathfrak{O}_{K_P}$. Since we can also let $N^{1/2}$ be larger than all primes ramifying in K/K_P, we can assume $K = K_P$.

Let

$$S_1(N) = \{1 \leq x \leq N : \exists \mathfrak{p} \text{ s.t. } \rho(\mathfrak{p}) > N^{1/2}, \mathfrak{p}^2 | P(x)\}$$

$$S_2(N) = \{1 \leq x \leq N : \exists p \text{ s.t. } p > N^{1/2}, p^2 | \mathfrak{N}_{K/\mathbb{Q}} P(x)\}.$$

We recall that conjecture $\mathfrak{A}_1(K, P, \delta(N))$ states that $\#S_1(N) \ll \delta(N)$, whereas conjecture $\mathfrak{A}_1(\mathbb{Q}, \mathfrak{N}_{K/\mathbb{Q}} P, \delta(N))$ states that $\#S_2(N) \ll \delta(N)$. We can assume $N^{1/2} \geq \max_{p|D} p$, where D is as in Lemma A.2.1. Then, for every prime ideal $\mathfrak{p} \in I_K$ such that $\rho(\mathfrak{p}) > N^{1/2}$, $\mathfrak{p}^2 | P(x)$, Lemma A.2.1 implies that $\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p} = \rho(\mathfrak{p}) > N^{1/2}$. Obviously, if $\mathfrak{p}^2 | P(x)$, then $(\mathfrak{N}_{K/\mathbb{Q}}\mathfrak{p})^2 | \mathfrak{N}_{K/\mathbb{Q}} P(x)$. Thus $S_1(N)$ is a subset of $S_2(N)$. Conversely, if there is a rational prime p such that $p^2 | P(x)$, $p > N^{1/2} \geq \max_{p|D} p$, we obtain from Lemma A.2.1 that $\mathfrak{p}^2 | P(x)$ for some $\mathfrak{p}$ lying over p. Hence $S_2(N) \subset S_1(N)$, and therefore $S_1(N) = S_2(N)$, for sufficiently large N. The statement follows immediately. □

Proposition A.2.4. *Let K be a number field. Let $P \in \mathfrak{O}_K[x, y]$ be a non-constant homogeneous polynomial. Let $P = P_1 P_2 \cdots P_k$, P_i irreducible in $\mathfrak{O}_K[x, y]$. Then Conjecture $\mathfrak{A}_2(K, P, \delta(N))$ is equivalent to Conjecture $\mathfrak{A}_2(\mathbb{Q}, Q, \delta(N))$, where the polynomial $Q(x, y) \in \mathbb{Z}[x, y]$ as the product of the irreducible factors of $\mathfrak{N}_{K_{P_i}/\mathbb{Q}}(c_i P_i(x, y)) \in \mathbb{Z}[x]$, $i = 1, \cdots, k$, where $c_1, \ldots, c_k$ are constants in $\mathfrak{O}_K$.*

Proof. Same as that of Proposition A.2.3. □

As was pointed out in the introduction, Hypothesis $\mathfrak{B}_i(K, P, \eta(N), \epsilon(N))$ is false for some choices of K and P. Thus we cannot hope to reduce it to the case $K = \mathbb{Q}$ without restrictions. We will, however, analyse the situation completely, provided that $K/\mathbb{Q}$ is Galois: we can then show $\mathfrak{B}_i(K, P, \eta(N), \epsilon(N))$ to be false in some cases and equivalent to $\mathfrak{B}_i(K, P, \eta(N), \epsilon(N))$ in all other cases.

Lemma A.2.5. *Let K be a number field. Let L be a finite Galois extension of K. Suppose* $\deg(L/K)$ *is odd. Then the restriction of λ_L to I_K equals λ_K.*

Proof. Let $\mathfrak{p} \in I_K$ be a prime ideal. Let e and f be the ramification degree and the inertia degree of $\mathfrak{p}$, respectively. Write

$$\mathfrak{p} = \mathfrak{P}_1^e \cdots \mathfrak{P}_n^e,$$

where n is the number of primes of I_L lying over $\mathfrak{p}$. Since $\deg(L/K) = efn$, both e and n must be odd. Hence

$$\lambda_L(\mathfrak{p}) = \lambda_L(\mathfrak{P}_1^e \cdots \mathfrak{P}_n^e) = (-1)^{ne} = -1 = \lambda_K(\mathfrak{p}).$$

Since λ_L is completely multiplicative, we conclude that $\lambda_L(\mathfrak{a}) = \lambda_K(\mathfrak{a})$ for all $\mathfrak{a} \in I_K$. $\square$

Given a non-zero ideal $\mathfrak{m} \in I_K$, we define $I_K^{\mathfrak{m}}$ to be the semigroup of ideals prime to $\mathfrak{m}$ and $P_K^{\mathfrak{m}}$ to be the semigroup of principal ideals (x) with $x \equiv 1 \bmod \mathfrak{m}$ and x totally positive.

Lemma A.2.6. *Let K be a number field. Let L be a finite extension of K. Suppose $\deg(L/K)$ is even. Then the restriction of λ_L to $\mathfrak{O}_K$ is pliable.*

Proof. The order $\deg(L/K)$ of $\mathrm{Gal}(L/K)$ is even. Hence there is an element $\sigma \in \mathrm{Gal}(L/K)$ of order 2. Let K' be the fixed field of σ. Once we show that $\lambda_L|_{\mathfrak{O}'_K}$ is pliable, we will have by Lemma 2.3.9 that $\lambda_L|_{\mathfrak{O}_K} = (\lambda_L|_{\mathfrak{O}'_K})|_{\mathfrak{O}_K}$.

Let $\mathfrak{p} \in I'_K$. Then

$$\lambda_L(\mathfrak{p}) = \begin{cases} 1 & \text{if } \mathfrak{p} \text{ splits or ramifies,} \\ -1 & \text{if } \mathfrak{p} \text{ is unsplit.} \end{cases}$$

Let $\mathfrak{m}$ be the conductor of L/K'. Let $H^{\mathfrak{m}} = (\mathfrak{N}_{L/K'} I_L^{\mathfrak{m}}) P_K^{\mathfrak{m}}$. By class field theory (see, e.g., [Ne], p. 428),

- $H^{\mathfrak{m}}$ is an open subgroup of $I_K^{\mathfrak{m}}$ of index 2,
- a prime ideal $\mathfrak{p} \in I_K^{\mathfrak{m}}$ splits if and only if it lies in $H^{\mathfrak{m}}$.

Therefore, given an ideal $\mathfrak{a} \in I_K$, we have $\lambda_K(\mathfrak{a}) = 1$ if and only if $\mathfrak{a}_0 \in H^{\mathfrak{m}}$, where we write $\mathfrak{a} = \mathfrak{a}_{\mathfrak{m}}\mathfrak{a}_{\mathfrak{m},0}$, $\mathfrak{a}_{\mathfrak{m}}|\mathfrak{m}^{\infty}$, $\mathfrak{a}_{\mathfrak{m},0} \in I_K^{\mathfrak{m}}$. Since $H^{\mathfrak{m}}$ contains $I_K^{\mathfrak{m}}$, we have that $\lambda_K(\mathfrak{a})$ depends only on $\mathfrak{a}_{\mathfrak{m},0}P_K^{\mathfrak{m}}$. Since we can tell $\mathfrak{a}_{\mathfrak{m}}$ from the coset of $P_K^{\mathfrak{m}} \subset I_K$ in which $\mathfrak{a}$ lies, we can say that $\lambda_K(\mathfrak{a})$ depends only on $\mathfrak{a}P_K^{\mathfrak{m}}$.

For every real infinite place v of K, let $U_v = \mathbb{R}^+$. For every $\mathfrak{p}|\mathfrak{m}$, let $U_{\mathfrak{p}} = 1 + \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})}\mathfrak{O}_{K_{\mathfrak{p}}}$. Let x be a non-zero element of $\mathfrak{O}_K$. Suppose we are given $xU_{\mathfrak{p}}$ for every $\mathfrak{p}|\mathfrak{m}$ and xU_v for every real infinite place v. Then, by the Chinese remainder theorem, we know $xP_K^{\mathfrak{m}}$. By the above paragraph, we can tell $\lambda_K(\mathfrak{a})$ from $xP_K^{\mathfrak{m}}$. We conclude that λ_K is pliable with respect to $\{v, U_v, 0\}_{v \text{ real}} \cup \{\mathfrak{p}, U_{\mathfrak{p}}, 0\}_{\mathfrak{p}|\mathfrak{m}}$. $\square$

Proposition A.2.7. *Let K be a finite Galois extension of $\mathbb{Q}$. Let $P \in \mathfrak{O}_K[x]$ be a square-free, non-constant polynomial. Let $P = P_1P_2\cdots P_k$, P_i irreducible in $\mathfrak{O}_K[x]$. Then*

$$\lambda_K(P(x)) = f(x) \cdot \lambda\left(\prod_{\substack{i \\ \deg(K/K_{P_i}) \text{ odd}}} \mathfrak{N}_{K_{P_i}/\mathbb{Q}}(c_iP_i(x))\right),$$

where $f : \mathbb{Z} \to \{-1, 0, 1\}$ is affinely pliable and $c_1, \cdots, c_k$ are constants in $\mathfrak{O}_K$.

Proof. Since (a) λ_K and λ are completely multiplicative, and (b) the product of affinely pliable functions is affinely pliable, it is enough to prove the statement for the case of P irreducible. Choose a non-zero $c \in \mathfrak{O}_K$ such that the leading coefficient of cP lies in K_P. Then every coefficient of cP lies in K_P.

If $\deg(K/K_{P_i})$ is even, Lemma A.2.6 gives us that the restriction of λ_K to $\mathfrak{O}_{K_P}$ is pliable. By Proposition 2.3.2, it follows that the map $x \mapsto \lambda_K(cP(x))$ is pliable on $\mathfrak{O}_K$. Since $\lambda_K(P(x)) = \lambda_K(c)\lambda_K(cP(x))$, we are done.

Suppose $\deg(K/K_{P_i})$ is odd. By Lemma A.2.5, $\lambda_K(cP(x)) = \lambda_{K_P}(cP(x))$. Let D

be as in Lemma A.2.1. Then

$$\lambda_{K_P}\left(\prod_{\rho(\mathfrak{p})\notin D}\mathfrak{p}^{v_{\mathfrak{p}}(cP(x))}\right)=\lambda\left(\prod_{p\notin D}p^{v_p(\mathfrak{N}_{K_P/\mathbb{Q}}(cP(x)))}\right),$$

where, as before, we write $\rho(\mathfrak{p})$ for the rational prime lying under $\mathfrak{p}$. Clearly

$$\lambda_{K_P}(cP(x))=\prod_{\rho(\mathfrak{p})\in D}(-1)^{v_{\mathfrak{p}}(cP(x))}\cdot\lambda_{K_P}\left(\prod_{\rho(\mathfrak{p})\notin D}\mathfrak{p}^{v_{\mathfrak{p}}(cP(x))}\right).$$

Set $f(x)=\prod_{\rho(\mathfrak{p})\in D}(-1)^{v_{\mathfrak{p}}(cP(x))}$. Since there are finitely many prime ideals lying over elements of D, we conclude that f is a product of finitely many affinely pliable functions, and is thus pliable itself. □

Proposition A.2.8. *Let K be a finite Galois extension of $\mathbb{Q}$. Let $P\in\mathfrak{O}_K[x,y]$ be a square-free, non-constant homogeneous polynomial. Let $P=P_1P_2\cdots P_k$, P_i irreducible in $\mathfrak{O}_K[x,y]$. Then*

$$\lambda_K(P(x))=f(x,y)\cdot\lambda\left(\prod_{\substack{i\\ \deg(K/K_{P_i})\ odd}}\mathfrak{N}_{K_{P_i}/\mathbb{Q}}(c_iP_i(x,y))\right),$$

where $f:\mathbb{Z}^2\to\{-1,0,1\}$ is pliable and $c_1,\cdots,c_k$ are constants in $\mathfrak{O}_K$.

Proof. Same as that of Proposition A.2.7. □

Corollary A.2.9. *Let K be a finite Galois extension of $\mathbb{Q}$. Let $P\in\mathfrak{O}_K[x]$ be a square-free, non-constant polynomial. Let $P=P_1P_2\cdots P_k$, P_i irreducible in $\mathfrak{O}_K[x]$. Let*

$$Q(x)=\prod_{\substack{i\\ \deg(K/K_{P_i})\ odd}}\mathfrak{N}_{K_{P_i}/\mathbb{Q}}(c_iP_i(x)),$$

where $c_1,\cdots,c_k\in\mathfrak{O}_K$ are is in Proposition A.2.7. Then

- $\mathfrak{B}_1(K, P, \eta(N), \epsilon(N))$ *is equivalent to* $\mathfrak{B}_1(\mathfrak{Q}, Q, \eta(N), \epsilon(N))$ *if* Q *is not of the form* cR^2, $c \in \mathfrak{O}_K$, $R \in \mathfrak{O}_K[x]$,

- $\mathfrak{B}_1(K, P, \eta(N), \epsilon(N))$ *is false if* Q *is of the form* cR^2, $c \in \mathfrak{O}_K$, $R \in \mathfrak{O}_K[x]$.

Proof. Immediate from Proposition A.2.7 and Lemma 2.3.12. □

Corollary A.2.10. *Let* K *be a finite Galois extension of* $\mathbb{Q}$. *Let* $P \in \mathfrak{O}_K[x, y]$ *be a square-free, non-constant homogeneous polynomial. Let* $P = P_1 P_2 \cdots P_k$, P_i *irreducible in* $\mathfrak{O}_K[x, y]$. *Let*

$$Q(x, y) = \prod_{\substack{i \\ \deg(K/K_{P_i}) \text{ odd}}} \mathfrak{N}_{K_{P_i}/\mathbb{Q}}(c_i P_i(x, y)),$$

where $c_1, \cdots, c_k \in \mathfrak{O}_K$ *are is in Proposition A.2.8. Then*

- $\mathfrak{B}_2(K, P, \eta(N), \epsilon(N))$ *is equivalent to* $\mathfrak{B}_2(\mathfrak{Q}, Q, \eta(N), \epsilon(N))$ *if* Q *is not of the form* cR^2, $c \in \mathfrak{O}_K$, $R \in \mathfrak{O}_K[x, y]$,

- $\mathfrak{B}_2(K, P, \eta(N), \epsilon(N))$ *is false if* Q *is of the form* cR^2 *for some* $c \in \mathfrak{O}_K$, $R \in \mathfrak{O}_K[x, y]$.

Proof. Immediate from Proposition A.2.8 and Lemma 2.3.13. □

A.3 Ultrametric analysis, field extensions and pliability

In this appendix, we show how pliable functions arise naturally in the context of extensions of local fields. While the rest of the present work does not depend on the following results, the reader might find that the following instantiation of pliability illuminates the said concept.

Let K be a field of characteristic zero. Consider a polynomial $f(x)$ with coefficients in $K((t))$:

$$f(x) = x^n + a_{n-1}(t)x^{n-1} + a_{n-2}(t)x^{n-2} + \cdots + a_0(t). \tag{A.3.1}$$

The Newton-Puiseux method yields fractional power series $\eta_i(t)$, $i = 1, 2, \ldots, n$,

$$\eta_i(t) = c_{k,i}t^{k/l} + c_{k+1,i}t^{(k+1)/l} + \cdots \tag{A.3.2}$$

with coefficients in a finite extension L/K, such that

$$f(x) = \prod_i (x - \eta_i(t))$$

formally. In particular, if $f(x)$ is irreducible over $\overline{K}((t))$, we have

$$\begin{aligned} \eta_0(t) &= c_k t^{k/n} + c_{k+1}t^{(k+1)/n} + \cdots \\ \eta_j(t) &= c_k \omega^{kj} t^{k/n} + c_{k+1}\omega^{(k+1)j}t^{(k+1)/n} + \cdots, \ 1 < j < n, \end{aligned} \tag{A.3.3}$$

where ω is a primitive nth root of unity.

We may rephrase this as follows: any finite extension R of $K((t))$ may be embedded in $L((t^{1/k}))$ for some positive integer l and some finite extension L of K. Regard $K((t))$ as a local field with respect to the valuation

$$v_t(c_k t^k + c_{k+1}t^{k+1} + \cdots) = k \text{ if } c_k \neq 0. \tag{A.3.4}$$

What (A.3.3) then implies is that any totally ramified finite Galois extension of $K((t))$ of degree n can be identified with $K((t^{1/n}))$. An unramified finite Galois extension of $K((t))$ can be written as $L((t))$, where L is the residue field of the extension, and as such a finite Galois extension of L. Hence an arbitrary finite Galois extension R of $K((t))$ can be identified with $L((t^{1/l}))$, where l is a positive integer and L is a finite

Galois extension of L.

Assume from now on that K is a $\mathfrak{p}$-adic field. Let $\mathcal{C}_g^\infty(K,t)$ be the ring of power series $\eta(t) \in K[[t]]$ that converge in a neighbourhood of 0. (In other words, $\mathcal{C}_g^\infty(K,t)$ is the ring of germs of analytic functions around 0.) Let $\mathcal{M}_g^\infty(K,t)$ be the field of fractions of $\mathcal{C}_g^\infty(t)$. It is a local field with respect to the valuation v_t defined in (A.3.4).

Consider $\eta \in K((t))$. By the *radius of convergence* $r(\eta)$ of η we mean the largest $r \geq 0$ such that $t^{-v_t(\eta)}\eta$ converges inside the open ball $B_0(r)$ of radius r about zero. We can see η as an element of $\mathcal{M}_g^\infty(K,t)$ if and only if $r(\eta) > 0$. Write

$$\eta = c_{-k}t^{-k} + c_{-k+1}t^{-k+2} + \cdots .$$

Then $r(\eta)$ is positive if and only if $c_j \ll M^j$ for some $M > 0$.

While $\mathcal{M}_g^\infty(K,t)$ is not complete with respect to its valuation v_t, it is nevertheless Henselian. A *Henselian* field is one for which Hensel's lemma holds. To see that $\mathcal{M}_g^\infty(K,t)$ is Henselian, it is enough to examine the algorithm that proves Hensel's lemma in its simplest incarnation. Let $f = x^n + a_{n-1}(t)x^{n-1} + \cdots + a_0(t)x^{n-1}$ be a polynomial with coefficients in $\mathcal{C}_g^\infty(K,t)$; let $\bar{f} = x^n + a_{n-1}(0)x^{n-1} + \cdots + a_0(0)x^{n-1}$ be its reduction to a polynomial with coefficients in the residue field K of $\mathcal{C}_g^\infty(K,t)$. If $\bar{f}(0) = 0$ and $\overline{f'}(0) \neq 0$, the Henselian algorithm produces a root $x(t) \in K((t))$ of $f(x) = 0$ satisfying $\overline{x(t)} = x(0) = 0$. We must check that the coefficients of the root $x(t)$ thus produced are majorized by some M^j. Since K is non-archimedean, this follows easily from the fact that the coefficients of $a_0, a_1, \ldots a_{n-1}$ are majorized by some $M_0^j, M_1^j, \ldots M_{n-1}^j$. Hence $x(t) \in \mathcal{M}_g^\infty(K,t)$, and so $\mathcal{M}_g^\infty(K,t)$ is Henselian.

The Newton-Puiseux method for solving (A.3.1) starts with the coefficients

$$a_{n-1}(t), \ldots, a_0(t) \in K((t))$$

and manipulates them to produce (A.3.2). These manipulations are of four kinds:

transforming t linearly, embedding $K((t))$ in $L((t))$, embedding $K((t))$ in $K((t^{1/l}))$ and expressing a polynomial

$$x^n + a_{n-1}(t)x^{n-1} + \cdots + a_0(t), \quad a_i \in K((t))$$

as a product

$$(x^{n_1} + \alpha_{n_1-1}(t)x^{n_1-1} + \cdots + \alpha_0(t))(x^{n_2} + \beta_{n_2-1}(t)x^{n_2-1} + \cdots + \beta_0(t)), \quad \alpha_i, \beta_i \in K((t))$$

by means of Hensel's lemma. It is clear that the every one of the first three operations takes a series with a non-trivial radius of convergence to a series with a non-trivial radius of convergence. That the fourth operation produces $\alpha_i, \beta_i \in \mathcal{M}_g^\infty(K,t)$ when given $a_i \in \mathcal{M}_g^\infty(K,t)$ follows from the fact that $\mathcal{M}_g^\infty(K,t)$ is Henselian.

Thus the formal solutions (A.3.2) in $L((t^{1/l}))$ to

$$x^n + a_{n-1}(t)x^{n-1} + \cdots + a_0(t) = 0$$

constructed by the Newton-Puiseux method lie in fact in $\mathcal{M}_g^\infty(L, t^{1/l})$, provided that $a_i(t) \in \mathcal{M}_g^\infty(K,t)$. See [DR] for explicit expressions for the radii of convergence of (A.3.2).

Thanks to this closure property of $\mathcal{M}_g^\infty(K,t)$, various matters work out much as for $K((t))$. Any finite Galois extension of $\mathcal{M}_g^\infty(K,t)$ can be identified with $\mathcal{M}_g^\infty(L, t^{1/l})$ for some finite Galois extension L of K and some positive integer l; if the extension is unramified, it is of the form $\mathcal{M}_g^\infty(L,t)$; if it is totally ramified, it is of the form $\mathcal{M}^\infty(K, t^{1/n})$, where n is the degree of the extension. Since the closure

of $K[[t]]$ in $L((t^{1/l}))$ is $L[[t^{1/l}]]$, the closure of $\mathcal{C}_g^\infty(K,t)$ in $\mathcal{M}_g^\infty(L,t^{1/l})$ is $\mathcal{C}_g^\infty(L,t^{1/l})$.

Let $t_0 \in K$. Define the *specialization map* $\mathrm{Sp}_{t_0} : \mathcal{M}_g^\infty(K,t) \to K$ taking $f \in \mathcal{M}_g^\infty(K,t)$ to $f(t_0)$, if t_0 is within the radius of convergence of f, and to 0 otherwise.

If $R = \mathcal{M}_g^\infty(L, t^{1/l})$ is a finite Galois extension of $\mathcal{M}_g^\infty(K, t)$, then $\mathrm{Sp}_{t_0}(R) = L(t_0^{1/l})$ for every $t_0 \in K$. Thus

$$t \mapsto \mathrm{Sp}_t(R)$$

is a map from K to the set of finite Galois extensions of K.

Lemma A.3.1. *Let K be a $\mathfrak{p}$-adic field. Let R be a finite Galois extension of $\mathcal{M}_g^\infty(K, t)$. Then the map*

$$t \mapsto \mathrm{Sp}_t(R)$$

is affinely pliable at 0.

Proof. We know that R is of the form $\mathcal{M}_g^\infty(L, t^{1/l})$ for some positive integer l and some finite Galois extension L of K. Let $U = 1 + \pi_K^{2l+1}\mathfrak{O}_K$. Suppose $t, t' \in K^*$ belong to the same coset of U. Then $t/t' \in U$, and thus $v_K(t/t' - 1) \geq 2l + 1$. By Hensel's lemma it follows that $x^l = t/t'$ has a root $x_0 \in K$. Choose lth roots $t^{1/l}$, $t'^{1/l}$ of t and t' such that $t^{1/l}/t'^{1/l} = x_0$. Then $L(t^{1/l}) = L(t'^{1/l})$. Therefore the map

$$t \mapsto \mathrm{Sp}_t(R)$$

is affinely pliable at zero. □

Lemma A.3.2. *Let K be a $\mathfrak{p}$-adic field. Let $a_0, a_1, \ldots, a_{n-1} \in \mathcal{M}_g^\infty(K, t)$. Let $\mathcal{M}_g^\infty(L, t^{1/l})$ be the splitting field of*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \tag{A.3.5}$$

over $\mathcal{M}_g^\infty(K, t)$. Let $\eta_1, \eta_2, \ldots, \eta_n \in \mathcal{M}_g^\infty(L, t^{1/l})$ be the roots of (A.3.5). Then there is an $r > 0$ such that $\eta_1(t_0), \ldots, \eta_n(t_0)$ converge and

$$\mathrm{Sp}_{t_0}(\mathcal{M}_g^\infty(L, t^{1/l})) = K(\eta_1(t_0), \ldots, \eta_n(t_0))$$

for $t_0 \in B_{K,0}(r) - \{0\}$.

Proof. Clearly $K(\eta_1(t_0), \ldots, \eta_n(t_0)) \subset \mathrm{Sp}_{t_0}(\mathcal{M}_g^\infty(L, t^{1/l}))$ for t within the radii of convergence of $\eta_1, \ldots \eta_n$. To prove $\mathrm{Sp}_t(\mathcal{M}_g^\infty(L, t_0^{1/l})) \subset K(\eta_1(t_0), \ldots, \eta_n(t_0))$, it is enough to show that

$$K(\eta_1(t_0), \ldots, \eta_n(t_0))$$

contains a basis of L as a vector space over K as well as an lth root of t_0. Let s_0 be an lth root of t and let $s_1, \ldots, s_m$ form a basis of L over K. Consider $s_0, \ldots, s_m$ as elements of $\mathcal{M}_g^\infty(L, t^{1/l})$. Since $\mathcal{M}_g^\infty(L, t^{1/l}) = (\mathcal{M}_g^\infty(K, t))(\eta_1, \ldots, \eta_n)$, one can reach s_i after a finite number of additions, substractions, multiplications and divisions starting from $\eta_1, ..., \eta_n$ and a finite number of elements of $\mathcal{M}_g^\infty(K, t)$. Each of this operations takes two series with positive radii of convergence to a series with a positive radius of convergence. Let r be the minimum of all the radii of convergence of the finitely many objects appearing in the process. Then, for $t_0 \in B_{K,0}(r)$, each operation $\spadesuit$ takes two series $\rho_1, \rho_2 \in \mathcal{M}_g^\infty(L, t^{1/l})$ to a series $\rho_1 \spadesuit \rho_2 \in \mathcal{M}_g^\infty(L, t^{1/l})$ taking the value $\rho_1(t_0) \spadesuit \rho_2(t_0)$ at t_0. Since $\eta_1(t_0), \ldots, \eta_n(t_0) \in K(\eta_1(t_0), \ldots, \eta_n(t_0))$ and $K(\eta_1(t_0), \ldots, \eta_n(t_0))$ is closed under $\spadesuit = +, -, *, /$, it follows that $K(\eta_1(t_0), \ldots, \eta_n(t_0))$ contains $s_0, s_1, \ldots, s_n$. Hence $\mathrm{Sp}_t(\mathcal{M}_g^\infty(L, t_0^{1/l})) \subset K(\eta_1(t_0), \ldots, \eta_n(t_0))$. $\square$

Now let $a_0, a_1, \ldots, a_{n-1}$ be rational functions on t with coefficients in K. For every $t_0 \in K$,

$$b_{t_0,0}(t) = a_0(t + t_0), b_{t_0,1}(t) = a_1(t + t_0), \ldots, b_{t_0,n-1}(t) = a_{n-1}(t + t_0)$$

can be seen as elements of $\mathcal{M}_g^\infty(K, t)$. Moreover,

$$b_{\infty,0}(t) = a_0(1/t), \ldots, b_{\infty,n-1} = a_{n-1}(1/t)$$

can be seen as elements of $\mathcal{M}_g^\infty(K,t)$, as they are rational functions on t.

Proposition A.3.3. *Let K be a $\mathfrak{p}$-adic field. Let $a_0, a_1, \ldots, a_{n-1} \in K(t)$. Define a function $\mathfrak{S}$ from K to the set of finite Galois extensions of K as follows: for $t_0 \in K$, let $\mathfrak{S}(t_0)$ be the splitting field of $x^n + a_{n-1}(t_0)x^{n-1} + \cdots + a_0(t_0) = 0$ over K if $a_0(t_0), a_1(t_0), \ldots, a_{n-1}(t_0)$ are finite; let $\mathfrak{S}(t_0)$ be K otherwise. Then $\mathfrak{S}$ is affinely pliable.*

Proof. Let $t_0 \in \mathbb{P}^1(K)$. By Lemma A.3.2, there are a positive integer l, a finite Galois extension L of K and an open ball V around zero such that, for all $t \in V - \{0\}$,

$$K(\eta_{t_0,1}(t), \ldots, \eta_{t_0,n}(t)) = \mathrm{Sp}_t(\mathcal{M}_g^\infty(L, t^{1/l})),$$

where $\eta_{t_0,1}(t), \ldots, \eta_{t_0,n}(t)$ are the roots of

$$x^n + b_{t_0,n-1}(t)x^{n-1} + \cdots + b_{t_0,0} = 0.$$

By Lemma A.3.1, $\mathrm{Sp}_t(M_g^\infty(L, t^{1/l}))$ is affinely pliable. Therefore the restriction of $K(\eta_1(t), \ldots, \eta_n(t))$ to V is affinely pliable at 0.

It follows from the definition of $b_{t_0,n-1}, \ldots, b_{t_0,0}$ that

$$K(\eta_1(t), \ldots, \eta_n(t)) = \begin{cases} \mathfrak{S}(t + t_0) & \text{if } t_0 \neq \infty \\ \mathfrak{S}(1/t) & \text{if } t_0 = \infty. \end{cases}$$

Hence, for every $t_0 \neq \infty$ there is an open ball V_{t_0} around t_0 such that $\mathfrak{S}(t)|_{V_{t_0}}$ is affinely pliable at t_0. Moreover, $\mathfrak{S}(1/t)|_{V_*}$ is affinely pliable at 0 for some open ball V_* around 0. This is the same as saying that there is an open subgroup U of K such that $\mathfrak{S}(1/t)$ depends only on tU for $t \in V_* - \{0\}$. Since U is a group, the map $tU \to t^{-1}U$ is well-defined and bijective. Hence depending only on tU is the same as depending only on $(1/t)U$. Therefore we can say that $\mathfrak{S}$ depends only on $(1/t)U$ for $t \in V_\infty$; in

other words, $\mathfrak{S}(t)$ depends only on tU for t in a neighborhood $V_\infty = 1/V_*$ of infinity. Thus $\mathfrak{S}(t)$ is affinely pliable at 0 when restricted to neighbourhood V_∞ of infinity.

Since $\mathbb{P}^1(K)$ is compact, it is covered by a finite subcover of $\{V_{t_0}\}_{t_0 \in \mathbb{P}^1(K)}$. Let the subcover be $\{V_s\}_{s \in S}$, S a finite subset of $\mathbb{P}_1(K)$. By the above $\mathfrak{S}|_{V_s}$ for every $s \in S$. Since V_s is a ball, its characteristic function $t \mapsto [t \in V_s]$ is affinely pliable. Hence

$$\mathfrak{S}(t) = \sum_{s \in S} [t \in V_s]((\mathfrak{S}|_{V_s})(t))$$

is affinely pliable. □

Given Proposition A.3.3 and Lemma 2.3.14, it is a simple matter to show that, given an elliptic curve $\mathcal{E}$ over $K(t)$, the map taking an element $t \in K$ to the minimal extension over which $\mathcal{E}(t)$ acquires good reduction is affinely pliable.

A.4 The root number in general

Let $H_k^*(N)$ be the set of newforms of even positive weight k on $\Gamma_0(N)$. Every newform $f \in H_k^*(N)$ has a root number η_f. It is a well-known fact that the average of the root numbers of the elements of $H_2^*(N)$ tends to zero as N goes to infinity. As some suboptimal bounds on the error term are labouriously derived in the recent literature, it may be worthwhile to point out that there is an exact expression for the total $\sum_f \eta_f$ of the root numbers of newforms $f \in H_2^*(N)$. This expression can be bounded easily from above and below.

Let W_N be the canonical involution for level N:

$$W_N : g \mapsto g|_{w_N},$$

where w_N is the matrix $\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Every newform $f \in H_k^*(N)$ is an eigenfunction

of W_N with eigenvalue η_f.

Let $S_k(N)$ be the space of cusp forms of weight k on $\Gamma_0(N)$. For $LM = N$, $f \in H_k^*(M)$, let $S_k(L; f)$ be the space of linear combinations of $\{f_{|\ell} : \ell | L\}$, where

$$f_{|\ell}(z) = \ell^{-k/2} f(\ell z).$$

Since the functions $f_{|\ell}$ for fixed f are linearly independent, $\{f_{|\ell} : \ell | L\}$ is actually a basis for $S_k(L; f)$. By ([AL], Thm 5) we have

$$S_k(N) = \bigoplus_{LM=N} \bigoplus_{f \in H_k^*(M)} S_k(L; f)$$

as a direct sum of orthogonal Hilbert spaces under the Petersson inner product on $S_k(N)$.

Consider an $f \in H_k^*(L; f)$. For $\ell | L$,

$$\begin{aligned}(W_N f_{|\ell})(z) &= (z\sqrt{N})^{-k} f_{|\ell}\left(\frac{-1}{Nz}\right) = (z\sqrt{N})^{-k} \ell^{k/2} f\left(\frac{-1}{(ML/\ell)z}\right) \\ &= \left(\frac{L}{\ell}\right)^{k/2} (W_M f)\left(\frac{L}{\ell} z\right) = \eta_f \left(\frac{L}{\ell}\right)^{k/2} f\left(\frac{L}{\ell} z\right) = \eta_f f_{|(L/\ell)}(z).\end{aligned} \tag{A.4.1}$$

Hence the trace of W_N on $S_k(L; f)$ is η_f if L is a perfect square and zero otherwise. Summing over all $f \in H_k^*(M)$ we obtain

$$\mathrm{Tr}(W_N, S_k(N)) = \sum_{\substack{LM=N \\ L \text{ a square}}} \sum_{f \in H_k^*(M)} \eta_f. \tag{A.4.2}$$

By Möbius inversion

$$\sum_{f \in H_k^*(N)} \eta_f = \sum_{R^2 M = N} \mu(R) \, \mathrm{Tr}(W_M, S_k(M)). \tag{A.4.3}$$

Now consider the curves $\Gamma_0(N) \backslash \mathbb{H}$ and $(\Gamma_0(N) \cdot W_N) \backslash \mathbb{H}$, where $\Gamma_0(N) * W_N$ is the

group obtained by adjoining W_N to $\Gamma_0(N)$. Let $S_k(\Gamma_0(N) * W_N)$ be the set of cusp forms of weight k on $(\Gamma_0(N) * W_N)\backslash\mathbb{H}$. Write $s_k(\Gamma_0(N))$ and $s_k(\Gamma_0(N) * W_N)$ for the cardinalities of $S_k(N)$ and $S_K(\Gamma_0(N) * W_N)$, respectively. Our goal is to compute

$$\mathrm{Tr}(W_N, S_k(N)) = 2s_k(\Gamma_0(N) * W_N) - s_k(\Gamma_0(N)).$$

By Gauss-Bonnet,

$$\frac{1}{2\pi}\,\mathrm{Vol}(\Gamma_0(N)\backslash\mathbb{H}) = 2g - 2 + m + \sum_{i=1}^{r}(1 - 1/e_i),$$

where g is the genus of $\Gamma_0(N)\backslash\mathbb{H}$, m is the number of its inequivalent cusps and e_1, e_2,... are the orders of its inequivalent elliptic points. Similarly,

$$\frac{1}{2\pi}\left(\frac{1}{2}\,\mathrm{Vol}(\Gamma_0(N)\backslash\mathbb{H})\right) = \frac{1}{2\pi}\,\mathrm{Vol}((\Gamma_0(N) * W_N)\backslash\mathbb{H}) = 2g_0 - 2 + m_0 + \sum_{i=1}^{r'}(1 - 1/e_i'),$$

where g_0 is the genus of $(\Gamma_0(N) * W)\backslash\mathbb{H}$, m_0 is the number of its inequivalent cusps and e_1', e_2',... are the orders of its inequivalent elliptic points. The relations among m, m_0, e_i and e_i' were written out by Fricke ([Fr], p. 357–367). They are as follows. Assume $N > 4$. The involution W_N then matches pairs of distinct equivalence classes of cusps of $\Gamma_0(N)\backslash\mathbb{H}$; therefore, $m = 2m_0$. The equivalence classes of elliptic points of $\Gamma_0(N)\backslash\mathbb{H}$ are also paired by W_N, which at the same time introduces $\epsilon_N h(-4N)$ new elliptic points, all of order 2. Here

$$\epsilon_N = \begin{cases} 2 & \text{if } N \equiv 7 \bmod 8, \\ 4/3 & \text{if } N \equiv 3 \bmod 8, \\ 1 & \text{otherwise,} \end{cases} \tag{A.4.4}$$

and $h(-4N)$ is the number of equivalence classes of primitive, positive definite binary

quadratic forms of discriminant $-4N$. Hence

$$\sum_{i=1}^{r'}(1-1/e_i') = \frac{1}{2}\sum_{i=1}^{r}(1-1/e_i) + \frac{1}{2}\epsilon_N h(-4N).$$

For $k=2$, we have $s_k(\Gamma_0(N)) = g$ and $s_k(\Gamma_0(N) * W) = g_0$. Hence

$$\begin{aligned}
\mathrm{Tr}(W_N, S_2(N)) = 2g_0 - g &= \left(\frac{1}{2\pi}(\frac{1}{2}\,\mathrm{Vol}(\Gamma_0(N)\backslash\mathbb{H})) + 2 - m_0 - \sum_{i=1}^{r}(1-1/e_i)\right) \\
&\quad - \frac{1}{2}\left(\frac{1}{2\pi}\,\mathrm{Vol}(\Gamma_0(N)\backslash\mathbb{H}) + 2 - m - \sum_{i=1}^{r'}(1-1/e_i')\right) \\
&= 1 - \frac{1}{2}\epsilon_N h(-4N),
\end{aligned}$$

as was first pointed out by Fricke (op. cit.). For $k>2$, by Riemann-Roch,

$$\begin{aligned}
s_k(\Gamma_0(N)) &= (k-1)(g-1) + \left(\frac{k}{2}-1\right)m + \sum_{i=1}^{r}\lfloor k(e_i-1)/2e_i\rfloor \\
s_k(\Gamma_0(N) * W_N) &= (k-1)(g_0-1) + \left(\frac{k}{2}-1\right)m_0 + \sum_{i=1}^{r'}\lfloor k(e_i'-1)/2e_i'\rfloor
\end{aligned}$$

(see, e.g., [Shi], Thm 2.24). Hence

$$\begin{aligned}
\mathrm{Tr}(W_N, S_k(N)) &= 2s_k(\Gamma_0(N) * W_N) - s_k(\Gamma_0(N)) \\
&= (k-1)(2(g_0-1)-(g-1)) + \left(\frac{k}{2}-1\right)(2m_0-m) \\
&\quad + \left(2\sum_{i=1}^{r'}(1-1/e_i') - \sum_{i=1}^{r}(1-1/e_i)\right) \\
&= (k-1)(2g_0-g-1) + 2[k/4]\,\epsilon_N h(-4N) \\
&= (k-1)(-\frac{1}{2}\epsilon_N h(-4N)) + (k/2)(\epsilon_N h(-4N)) - 2k/4(\epsilon_N h(-4N)) \\
&= \begin{cases} \frac{1}{2}\epsilon_N h(-4N) & \text{if } 4|k \\ -\frac{1}{2}\epsilon_N h(-4N) & \text{if } 4\nmid k\ . \end{cases}
\end{aligned}$$

We invoke (A.4.3) and conclude that

$$\sum_{f\in H_k^*(N)} \eta_f = \sum_{R^2M=N} \mu(R)\cdot \begin{cases} (1-\frac{1}{2}\epsilon_M h(-4M)) & \text{if } k=2, \\ \frac{1}{2}\epsilon_M h(-4M) & \text{if } k>2,\ 4|k, \\ -\frac{1}{2}\epsilon_M h(-4M) & \text{if } k>2,\ 4\nmid k, \end{cases}$$

provided N is not of the form R^2, $2R^2$, $3R^2$ or $4R^2$ for some square-free integer R. Here, as usual, ϵ_N is as in (A.4.4).

It is a simple consequence of Dirichlet's formula for the class number that

$$h(d) \ll |d|^{1/2}\log|d|\log\log|d|$$

for any negative d (see, e.g., [Na], p. 254). Therefore

$$\begin{aligned} \left|\sum_{f\in H_k^*(N)} \eta_f\right| &\ll N^{1/2}\log N\log\log N\prod_{p^2|n}(1+1/p) \\ &\ll N^{1/2}\log N(\log\log N)^2. \end{aligned} \tag{A.4.5}$$

By Siegel's theorem,

$$h(d) \gg |d|^{1/2-\epsilon}.$$

Hence, for any square-free N,

$$\left|\sum_{f\in H_k^*(N)} \eta_f\right| \gg N^{1/2-\epsilon}. \tag{A.4.6}$$

We may finish by commenting on the special cases $N = R^2$, $2R^2$, $3R^3$, or, more precisely on the trace $\mathrm{Tr}(W_N, S_k(N))$ for $N = 1, 2, 3$. For those values of N, the genera of $\Gamma_0(N)\backslash\mathbb{H}$ and $(\Gamma_0(N) * W_N)\backslash\mathbb{H}$ are zero. An explicit computation by means

of Riemann-Roch gives

$$\begin{aligned}
\mathrm{Tr}(W_N, S_k(N)) &= \lfloor k/12 \rfloor - 1 && \text{if } N = 1,\ k \equiv 2 \bmod 12,\\
\mathrm{Tr}(W_N, S_k(N)) &= \lfloor k/12 \rfloor && \text{if } N = 1,\ k \not\equiv 2 \bmod 12,\\
\mathrm{Tr}(W_N, S_k(N)) &= 3\lfloor k/4 \rfloor - 1 && \text{if } N = 2,\\
\mathrm{Tr}(W_N, S_k(N)) &= 1 - 3\{k/3\} && \text{if } N = 3,
\end{aligned}$$

for $k > 2$. (The fact that the genera are zero gives us that $S_k(N)$ is empty for $k = 2$, $N = 1, 2, 3$.) For $N = R^2$, $2R^2$, there is a term of $\lfloor k/12 \rfloor$, resp. $3\lfloor k/4 \rfloor$, which dominates all other terms when k grows more rapidly than N. For all other N, including $N = 3R^2$, the bound is (A.4.5), which does not depend on k.

Appendix B

Addenda on the parity problem

B.1 The average of $\lambda(x^2 + y^4)$

We prove in this section that the Liouville function averages to zero over the integers represented by the polynomial $x^2 + y^4$. This is the same polynomial for which Friedlander and Iwaniec first broke parity ([FI1], [FI2]). As $x^2 + y^4$ is not homogeneous, the results in this section have no apparent bearings on the root numbers of elliptic curves. The interest in studying $x^2 + y^4$ resides mainly in the implied opportunity to test the flexibility of the basic Friedlander-Iwaniec framework.

As we will see, [FI1] can be used without any modifications; only [FI2] must be rewritten. We will let α be the Liouville function or the Moebius function: $\alpha = \lambda$ or $\alpha = \mu$.

B.1.1 Notation and identities

By n we shall always mean a positive integer, and by p a prime. As in [FI2], we define

$$f(n \leq y) = \begin{cases} f(n) & \text{if } n \leq y \\ 0 & \text{otherwise,} \end{cases}$$

$$f(n > y) = \begin{cases} f(n) & \text{if } n > y \\ 0 & \text{otherwise.} \end{cases}$$

Let

$$P(z) = \prod_{\substack{p \le z \\ p \text{ prime}}} p.$$

For any n,

$$f(n > y) = \sum_{\substack{bc|n \\ \gcd(n/c, P(z))=1}} \mu(b) f(c > y). \tag{B.1.1}$$

Write

$$\sum_{*} \cdots \quad \text{for} \quad \sum_{\substack{bc|n \\ \gcd(n/c, P(z))=1}} \cdots$$

Then

$$\begin{aligned} \sum_{*} \mu(b)\alpha(c > y) &= \sum_{*} \mu(b \le y)\alpha(c > y) + \sum_{*} \mu(b > y)\alpha(c > y) \\ &= \sum_{*} \mu(b \le y)\alpha(c) - \sum_{*} \mu(b \le y)\alpha(c \le y) + \sum_{*} \mu(b > y)\alpha(c > y). \end{aligned}$$

Let $w > y$. Proceed:

$$\begin{aligned} \sum_{*} \mu(b)\alpha(c > y) = &\sum_{*} \mu(b \le y)\alpha(c) - \sum_{*} \mu(b \le y)\alpha(c \le y) \\ &+ \sum_{*} \mu(y < b < w)\alpha(c > y) + \sum_{*} \mu(b > w)\alpha(y < c < w) \\ &+ \sum_{*} \mu(b \ge w)\alpha(c \ge w). \end{aligned}$$

We denote the summands on the right side of (B.1.1) by $\beta_1(n)$, $\beta_2(n)$, $\beta_3(n)$, $\beta_4(n)$ and $\beta_5(n)$.

If $\alpha = \mu$, then, by Möbius inversion,

$$\beta_1(n) = \sum_{*} \mu(b \le y)\alpha(c) = \mu(n/\gcd(n, P(z)^\infty) \le y)\, \mu(\gcd(n, P(z))^\infty), \tag{B.1.2}$$

whereas, if $\alpha = \lambda$,

$$\beta_1(n) = \sum_{*} \mu(b \le y)\alpha(c) = \mu(n/\gcd(n, P(z)^\infty) \le y)\, \lambda(\gcd(n, P(z))^\infty). \tag{B.1.3}$$

Clearly

$$\beta_2(n) = \sum_{\substack{b \le y \\ \gcd(b, P(z))=1}} \sum_{c \le y} \mu(b)\alpha(c) \sum_{\substack{d \\ bcd=n \\ \gcd(d, P(z))=1}} 1.$$

If $n < w^2 z$, then

$$\beta_5(n) = \sum_{\substack{bc|n \\ \gcd(n/c, P(z))=1}} \mu(b \ge w)\alpha(c \ge w) = \sum_{\substack{bc=n \\ \gcd(b, P(z))=1}} \mu(b \ge w)\alpha(c \ge w), \tag{B.1.4}$$

as $\gcd(n/c, P(z)) = 1$ implies that either $w = 1$ or $w > z$, and the latter possibility is invalidated by $bcd = n$, $b > w$, $c > w$, $n \le w^2 z$.

Let us be given a sequence $\{a_n\}_{n=1}^\infty$ of non-negative real numbers. For $j = 1, \cdots, 5$, we write

$$A(x) = \sum_{n=1}^{x} a_n, \quad A_d(x) = \sum_{\substack{1 \le n \le x \\ d|x}} a_n, \quad S_j(x) = \sum_{n=1}^{x} \beta_j(n) a_n. \tag{B.1.5}$$

We will regard y, w and z as functions of x to be set later. For now, we require that $w(x)^2 z(x) > x$. We have

$$\sum \alpha(n) a_n = \sum_{n=1}^{x} \alpha(n \le y) a_n + \sum_{j=1}^{5} S_j(x).$$

B.1.2 Axioms

Let $\{a_n\}_{n=1}^{\infty}$, a_n non-negative, be given. We let $A(x)$ and $A_d(x)$ be as in (B.1.5). We assume the crude bound

$$A_d(x) \ll d^{-1}\tau^{c_1}(d)A(x) \tag{B.1.6}$$

uniformly in $d \leq x^{1/3}$, where c_1 is a positive constant. We also assume we can express A_d in the form

$$A_d(x) = g(d)A(x) + r_d, \tag{B.1.7}$$

where

$$g : \mathbb{Z}^+ \to \mathbb{R}_0^+ \text{ is a multiplicative function,}$$

$$0 \leq g(p) < 1, \quad g(p) \ll p^{-1}, \tag{B.1.8}$$

$$\sum_{p \leq x} g(p) = \log\log x + c_2 + O((\log x)^{-1}), \tag{B.1.9}$$

$$\sum_{d \leq D(x)} |r_d(x)| \ll A(x)(\log x)^{-C_1}, \tag{B.1.10}$$

where

$$x^{2/3} < D(x) < x, \tag{B.1.11}$$

and C_1 is a sufficiently large constant ($C_1 \leq 65 \cdot 2^{c_1} + 4$). We also assume the following bilinear bound:

$$\sum_m \left| \sum_{\substack{N<n<2N \\ mn \leq x \\ \gcd(n, mP(z))=1}} \mu(n) a_{mn} \right| \leq A(x) \cdot (\log x)^{-C_2} \tag{B.1.12}$$

for every N with

$$y(x) < N < w(x),$$

where

$$y(x) \ll D^{1/2}(x)N^{-\epsilon}, \quad \log(x^{1/2}w^{-1}(x)) = o(\log x/C_3 \log\log x),$$

and C_2 and C_3 are sufficiently large constants. In [FI2], conditions (B.1.6)–(B.1.10) appear (sometimes in stricter forms) as (1.6), (1.9), (R) and (R1), respectively. Condition (B.1.12) is a special case of (B*) in [FI2] (the case corresponding to $C = 1$, in the notation of the said paper). All of these conditions are proven for

$$a_n = \{(x, y) \in \mathbb{Z}^2 : x^2 + y^4 = n\}$$

in [FI1]. Specifically, (B.1.6)–(B.1.10) are proven in [FI1], section 3, and the rest of [FI1] is devoted to proving (B*). The parameters $D(x)$ and $w(x)$ are given by

$$D \gg x^{2/3-\epsilon}, \quad w(x) \gg x^{1/2}(\log x)^{C_4}. \tag{B.1.13}$$

The constants $C_1, \ldots, C_4$ can be arbitarily large. Notice that

$$x^{3/4} \ll A(x) \ll x^{3/4}.$$

B.1.3 Estimates

We will bound each of $S_j(x)$, $1 \le j \le 5$. The term $S_1(x)$ can be bounded easily as in Lemma 3.6.3. Let us bound $S_2(x)$. Assume $\log z = O(\log x/(2C_3 \log\log x))$. Then

$$z^9 \ll Dy^{-2}, \quad \log D/\log z \gg 2C_3 \log\log x.$$

It follows that we can use a fundamental lemma (a standard formulation of a small sieve). We obtain:

$$\sum_{\substack{d \\ \gcd(d,P(z))=1}} a_{bcd} = g(bc)(1 + O((\log x)^{-2C_3})) + O\left(\sum_{\substack{d \le D \\ bc|d}} |r_d(x)|\right).$$

Hence, by (B.1.9) and (B.1.10),

$$\begin{aligned} S_2(n) &= \sum_{\substack{b \le y \\ \gcd(b,P(z))=1}} \sum_{c \le y} \mu(b)\alpha(c) \sum_{\substack{d \\ bcd=n \\ \gcd(d,P(z))=1}} 1 \\ &= \sum_{\substack{b \le y \\ \gcd(b,P(z))=1}} \sum_{c \le y} \mu(b)\alpha(c)g(bc)(1 + O((\log x)^{-2C_3}))A(x) \\ &+ O(\sum_d \tau_3(d)|r_d(x)|) \\ &= \sum_{\substack{b \le y \\ \gcd(b,P(z))=1}} \sum_{c \le y} \mu(b)\alpha(c)g(bc)A(x) + O(A(x)(\log x)^{-C_5}), \end{aligned}$$

where C_5 is a large constant. Note that (B.1.10) implies

$$\sum_{\substack{b \le y \\ \gcd(b,P(z))=1}} \sum_{c \le y} \mu(b)\alpha(c)g(bc) \ll A(x)(\log x)^{-5}.$$

See [FI2], (2.4).

To bound $S_3(x)$, a simple application of the bilinear condition (B.1.9) will suffice:

$$|S_3(x)| = \left| \sum_{\substack{b,c,d \\ \gcd(bd,P(z))=1}} \mu(y < b < w)\alpha(c > y) \right| \le \sum_m \tau(m) \left| \sum_{\substack{y<n<w \\ mn \le x \\ \gcd(n,P(z))=1}} \mu(n)a_{mn} \right|.$$

Since n has no small factors, the condition $\gcd(n, m) = 1$ may be added with a total

change of at most $O(A(x)(\log x)/z)$. The factor $\tau(m)$ may be extracted as in [FI2], p 1047. We obtain

$$S_3 \ll A(x)(\log x)^{-C_6} + A(x)/z.$$

The term S_4 can be treated in the same way, with the proviso that α must be replaced by μ. This replacement induces a total change of at most $O(A(x)(\log x)/z)$.

All terms up to now have contributed at most $O(A(x)((\log x)^{-5} + (\log x)/z)$. One term remains, namely, S_5. By (B.1.4),

$$S_5(n) = \sum_{\substack{bc=n \\ \gcd(b,P(z))=1}} \mu(b \le w)\alpha(c \le w).$$

Hence

$$\sum_{\substack{w \le x \le xw^{-1} \\ \gcd(b,P(z))=1 \\ bc=n}} 1 = \sum_{\substack{w \le b \le xw^{-1} \\ \gcd(b,P(z))=1}} g(b)A(x) + O\left(\sum_{d \le xw^{-1}} |r_d(x)|\right).$$

By (B.1.9) and a fundamental lemma,

$$\sum_{\substack{w \le b \le xw^{-1} \\ \gcd(b,P(z))=1}} g(b) \sim \frac{1}{\log z}(\log xw^{-1} - \log w) = \frac{\log xw^{-2}}{\log z} \ll \frac{\log\log x}{\log z}.$$

We are given $w(x) \gg x^{1/2}(\log x)^{-C_4}$; see (B.1.13). Set

$$z(x) = e^{\log x/C_3 \log\log x}.$$

Then

$$\sum_{\substack{w \le b \le xw^{-1} \\ \gcd(b,P(z))=1}} g(b) \ll \frac{(\log\log x)^2}{\log x} A(x).$$

Hence

$$\sum_n \alpha(n)a_n = \sum_{j=1}^{5} S_j(x) + O(A(y)) \ll \frac{(\log\log x)^2}{\log x} A(x),$$

as was desired. We have proven

Theorem B.1.1. *Let $\alpha = \mu$ or $\alpha = \lambda$. Then*

$$\sum_{\substack{a\geq 1\\ a^2+b^4\leq x}}\sum_{b\geq 1}\mu(a^2+b^4) \ll \left(\sum_{\substack{a\geq 1\\ a^2+b^4\leq x}}\sum_{b\geq 1} 1\right)\cdot\frac{(\log\log x)^2}{\log x} \ll x^{3/4}\frac{(\log\log x)^2}{\log x}.$$

Bibliography

[A] Apostol, T. M., *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer–Verlag, New York–Heidelberg, 1976.

[AL] Atkin, A., and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.

[Bl] Blanchard, A., *Initiation à la théorie analytique des nombres premiers*, *Travaux et Recherches Mathématiques*, No. 19, Dunod, Paris, 1969.

[BCDT] Breuil, C., Conrad, B., Diamond, F., and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), no. 4, 843–939.

[BG] Bateman, P. T., and E. Grosswald, On a theorem of Erdős and Szekeres, Illinois J. Math. **2** (1958) 88–98.

[BK] Brumer, A., and K. Kramer, The rank of elliptic curves, *Duke Math. J.* **44** (1977), 715–743.

[Bo] Bombieri, E., On the large sieve, *Mathematika* **12**, 1965, 201–225.

[C] Cassels, J. W. S., *Lectures on elliptic curves, London Mathematical Society student texts, 25*, Cambridge University Press, 1991.

[Ch] Chowla, S., *The Riemann hypothesis and Hilbert's tenth problem*, *Mathematics and Its Applications*, Vol. 4, Gordon and Breach Science Publishers, New York–London–Paris, 1965.

[Col] Coleman, M. D., A zero-free region for the Hecke L-functions, *Mathematika* **37** (1990) no. 2, 287–304.

[Col2] Coleman, M. D., The Rosser-Iwaniec sieve in number fields, with an application, *Acta Arith.* **65** (1993), no. 1, 53–83.

[Con] Connell, I., Calculating Root Numbers of Elliptic Curves over $\mathbb{Q}$, *Manuscr. Math.* **82**, 93–104.

[CS] Conway, J. H., and N. J. A. Sloane, *Sphere packings, lattices and groups, Grundlehren der Mathematischen Wissenschaften, 290*, Springer-Verlag, New York, 1988.

[Dav] Davenport, H., *Multiplicative number theory*, Markham, Chicago, 1967.

[DVP1] De la Vallée-Poussin, Ch. J., Recherches analytiques sur la théorie des nombres premiers, *Brux. S. sc.* **20** B, 363–397.

[DVP2] De la Vallée-Poussin, Ch. J., Recherches analytiques sur la théorie des nombres premiers, *Brux. S. sc.* **21** B, 351–342.

[De] Deligne, P., Les constantes des équations fonctionelles des fonctions L, *Modular Functions of One Variable, II, SLN* 349, Springer-Verlag, New York, 1973, 501–595.

[DR] Dwork, B., and P. Robba, On natural radii of p-adic convergence, *Trans. Amer. Math. Soc.* **256** (1979), 199–213.

[Es] T. Estermann, Einige Sätze über quadratfreie Zahlen, *Math. Ann.* **105** (1931), 653–662.

[Fo] Fogels, E., On the zeros of Hecke's L-functions I, *Acta Arith.*, **7** (1962), 87–106.

[FI1] Friedlander, J., and H. Iwaniec, The polynomial X^2+Y^4 captures its primes, *Ann. of Math. (2)* **148** (1998), no. 3, 945–1040.

[FI2] Friedlander, J., and H. Iwaniec, Asymptotic sieve for primes, *Ann. of Math. (2)* **148** (1998), no. 3, 1041–1065.

[Fr] Fricke, R., *Die elliptischen Funktionen und ihre Anwendungen, 2. Teil*, Teubner, Leipzig, 1922.

[GM] Gouvêa, F., and B. Mazur, The square-free sieve and the rank of elliptic curves, *J. Amer. Math. Soc.* **4** (1991), no. 1, 1–23.

[Gran] Granville, A., *ABC* allows us to count squarefrees, *Internat. Math. Res. Notices* **1998**, no. 19, 991-1009.

[Gre] Greaves, G., Power-free values of binary forms, *Quart. J. Math. Oxford* **43**(2) (1992), 45-65.

[Ha] Halberstadt, E., Signes locaux des courbes elliptiques en 2 et 3, *C. R. Acad. Sci. Paris Sér. I Math.* **326** (1998), no. 9, 1047–1052.

[HR] Halberstam, H., and H.-E. Richert, *Sieve Methods*, London Mathematical Society Monographs, No. 4., Academic Press, London-New York, 1974.

[H-B] Heath-Brown, D. R., Primes represented by x^3+2y^3, *Acta Math.* **186** (2001), no. 1, 1–84.

[HBM] Heath-Brown, D. R., and B. Z. Moroz, Primes represented by binary cubic forms, *Proc. London Math. Soc. (3)* **84** (2002), no. 2, 257–288.

[HBM2] Heath-Brown, D. R., and B. Z. Moroz, On the representation of primes by cubic polynomials in two variables, preprint.

[Hec] Hecke, E., Eine neue Art von Zetafunctionen und ihre Beziehung zur Verteilung der Primzahlen I, II, *Math. Z.* **1** (1918), 357–376; **6** (1920) 11–51.

[Hoo] Hooley, C., *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, Cambridge, 1976.

[ILS] Iwaniec, H., W. Luo and P. Sarnak, Low lying zeroes of families of L-functions, *Publ. Math. IHES* **91** (2000), 55–131.

[Iw] Iwaniec, H., *Topics in classical automorphic forms*, Grad. Studies in Mathematics, No. 17, AMS, Providence, RI, 1997.

[Iw2] Iwaniec, H., *Sieve methods*, unpublished.

[KL] Kabtjanskiĭ, G. A., and V. I. Levenšteĭn, Bounds for packings on the sphere and in space, *Problemy Peredači Informacii* **14** (1978), no. 1, 3–25.

[Kn] Knuth, D. E., Two notes on notation, *Amer. Math. Monthly* **99** (1992) no. 5, 403–422.

[Ku] Kubilius, J. P., On a problem in the n-dimensional analytic theory of numbers, *Vilniaus Valst. Univ. Mokslo Darbai. Mat. Fiz. Chem. Mokslu Ser.* **4** (1955) 5–43.

[La] Laska, M., An algorithm for finding a minimal Weierstrass equation for an elliptic curve, *Math. Comp.* **38** (1982), 257-260.

[Le] Levin, B. V., The "average" distribution of $\lambda(n)$ and $\Lambda_f(n)$ in progressions, *Topics in classical number theory, Vol. I, II,* Budapest, 1981, 995–1022, *Colloq. Math. Soc. J. Bolyai* **34**, North-Holland, Amsterdam, 1984.

[Man] Manduchi, E., Root numbers of fibers of elliptic surfaces, *Compositio Math.* **99** (1995) 33–58.

[Maz] Mazur, B., Rational points on modular curves, *Modular functions of one variable, V*, *Lecture Notes in Mathematics, 601*, Springer, Berlin, 1977.

[Na] Narkiewicz, W., *Classical problems in number theory*, Monografie Matematyczne, No. 62, PWN, Warsaw, 1986.

[Ne] Neukirch, J., *Algebraische Zahlentheorie*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1992.

[PT] Parson, A., and J. Tull, Asymptotic behavior of multiplicative functions, *J. Number Theory* **10** (1978), no. 4, 395–420.

[Pe] Petersson, H., Über die Entwicklungskoeffizienten der automorphen Formen, *Acta Math.* **58** (1932), 169–215.

[Pe2] Petersson, H., Über eine Metrisierung der automorphen Formen und die Theorie der Poincaréschen Reihen, *Math. Ann.* **117** (1940), 453–537.

[Pe3] Petersson, H., Über eine Metrisierung der ganzen Modulformen, *Jahresb. d. Deutschen Math. Verein.* **49** (1939), 49–75.

[Pr] Prachar, K., *Primzahlverteilung*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1957.

[Ra] Ramsay, K., personal communication.

[Ri1] Rieger, G. J., Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper. I. *J. reine angew. Math.* **199** (1958), 208–214.

[Ri2] Rieger, G. J., Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper. II. *J. reine angew. Math.* **201** (1959), 157–171.

[Ri3] Rieger, G. J., Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper. III. *J. reine angew. Math.* **208** (1961), 79–90.

[Riz1] Rizzo, O. G., Average root numbers in families of elliptic curves, *Proc. Amer. Math. Soc.* **127** (1999), no. 6, 1597–1603.

[Riz2] Rizzo, O. G., Average root numbers for a non-constant family of elliptic curves, Compositio Math. **136** (2003), 1–23.

[Ro] Rohrlich, D. E., Elliptic curves and the Weil-Deligne group, *Elliptic curves and related topics*, 125–157, *CRM Proc. Lecture Notes* **4** Amer. Math Soc., Providence, RI, 1994.

[Ro2] Rohrlich, D. E., Galois theory, elliptic curves, and root numbers, *Composition Math.* **100** (1996), no. 3, 311–349.

[Ro3] Rohrlich, D. E., Variation of the root number in families of elliptic curves, *Compositio Math.* **87** (1993), no. 2, 119–151.

[Se] Selberg, A., Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, *J. Indian Math. Soc. (N. S.)* **20** (1956), 47–87.

[Se2] Selberg, A., On elementary methods in primenumber-theory and their limitations, in Proc. 11th Scand. Math. Cong. Trondheim (1949), *Collected Works*, Vol. I, 388–397, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1989.

[ST] Serre, J.-P., and J. Tate, Good reduction of abelian varieties, *Ann. of Math. (2)* **88** (1968), no. 3, 492–517.

[Shi] Shimura, G., *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.

[Si] Silverman, J. H., *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1985.

[Si2] Silverman, J. H., The average rank of an algebraic family of elliptic curves, *J. reine angew. Math.* **504** (1998), 227–236.

[SW] Skinner, C. M., and A. J. Wiles, Nearly ordinary deformations of irreducible residual representations, *Ann. Fac. Sci. Toulouse Math.* (6) **8** (2001), no. 1, 185–215.

[Ta] Tate, J., Number theoretic background, *Automorphic Forms, Representations, and L-Functions*, *Proc. Symp. Pure Math.* Vol. 33 – Part 2, *Amer. Math. Soc.*, Providence, 1979, pp. 3–26.

[TW] Taylor, R., and A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* (2) **141** (1995), no. 3, 553–572.

[Vi] Vinogradov, I. M., *The method of trigonometrical sums in the theory of numbers*, translated and annotated by K. F. Roth and A. Davenport, Interscience Publishers, London and New York, 1954.

[Wa] Walfisz, A., *Weylsche Exponentialsummen in der neueren Zahlentheorie*, *Mathematische Forschungsberichte, XV*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1963.

[Wi] Wiles, A., Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (2) **141** (1995), no. 3, 443–551.

[Za] Zagier, D., The Eichler-Selberg trace formula on $\mathrm{SL}_2(\mathbb{Z})$, Appendix in S. Lang, *Introduction to Modular Forms*, Berlin-Heidelberg-New York and Correction, in *Modular Functions of One Variable VI*, Lect. Notes in Math. **627**, Berlin-Heidelberg-New York 1977.