# Existence and density problems in Diophantine geometry: From norm forms to Campana points

by

**Alec Shute**

September, 2022

*A thesis submitted to the*
*Graduate School*
*of the*
*Institute of Science and Technology Austria*
*in partial fulfillment of the requirements*
*for the degree of*
*Doctor of Philosophy*

Committee in charge:

Beatriz Vicoso, Chair
Tim Browning
Tamas Hausel
Damaris Schindler

The thesis of Alec Shute, titled *Existence and density problems in Diophantine geometry: From norm forms to Campana points*, is approved by:

**Supervisor**: Professor Tim Browning, ISTA, Klosterneuburg, Austria

Signature: _____

**Committee Member**: Professor Tamas Hausel, ISTA, Klosterneuburg, Austria

Signature: _____

**Committee Member**: Professor Damaris Schindler, Georg August University of Göttingen, Germany

Signature: _____

**Defense Chair**: Professor Beatriz Vicoso, ISTA, Klosterneuburg, Austria

Signature: _____

Signed page is on file

IST Austria Thesis, ISSN: 2663-337X

ISBN: 978-3-99078-023-7

I hereby declare that this thesis is my own work and that it does not contain other people's work without this being so stated; this thesis does not contain my previous work without this being stated, and the bibliography contains all the literature that I used in writing the dissertation.

I declare that this is a true copy of my thesis, including any final revisions, as approved by my thesis committee, and that this thesis has not been submitted for a higher degree to any other university or institution.

I certify that any republication of materials presented in this thesis has been approved by the relevant publishers and co-authors.

Signature: _____

Alec Shute
September, 2022

Signed page is on file

# Abstract

In this thesis, we study two of the most important questions in Arithmetic geometry: that of the existence and density of solutions to Diophantine equations. In order for a Diophantine equation to have any solutions over the rational numbers, it must have solutions everywhere locally, i.e., over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime $p$. The converse, called the *Hasse principle*, is known to fail in general. However, it is still a central question in Arithmetic geometry to determine for which varieties the Hasse principle does hold. In this work, we establish the Hasse principle for a wide new family of varieties of the form

$$f(t) = \mathbf{N}_{K/\mathbb{Q}}(\mathbf{x}) \neq 0,$$

where $f$ is a polynomial with integer coefficients and $\mathbf{N}_{K/\mathbb{Q}}$ denotes the norm form associated to a number field $K$. Our results cover products of arbitrarily many linear, quadratic or cubic factors, and generalise an argument of Irving [69], which makes use of the beta sieve of Rosser and Iwaniec. We also demonstrate how our main sieve results can be applied to treat new cases of a conjecture of Harpaz and Wittenberg on locally split values of polynomials over number fields, and discuss consequences for rational points in fibrations.

In the second question, about the density of solutions, one defines a height function and seeks to estimate asymptotically the number of points of height bounded by $B$ as $B \to \infty$. Traditionally, one either counts rational points, or integral points with respect to a suitable model. However, in this thesis, we study an emerging area of interest in Arithmetic geometry known as *Campana points*, which in some sense interpolate between rational and integral points. More precisely, we count the number of nonzero integers $z_1, z_2, z_3$ such that $\gcd(z_1, z_2, z_3) = 1$, and $z_1, z_2, z_3, z_1 + z_2 + z_3$ are all squareful and bounded by $B$. Using the circle method, we obtain an asymptotic formula which agrees in the power of $B$ and $\log B$ with a bold new generalisation of Manin's conjecture to the setting of Campana points, recently formulated by Pieropan, Smeets, Tanimoto and Várilly-Alvarado [96]. However, in this thesis we also provide the first known counterexamples to leading constant predicted by their conjecture.

# Acknowledgements

The last four years have been an incredible journey for me, with many ups and downs. I could not have undertaken this journey without the constant support and encouragement of my supervisor, Prof. Tim Browning. I would like to thank him for sharing many invaluable insights, and for his patience and understanding though some difficult times.

I am grateful to Prof. Damaris Schindler for the helpful feedback on an earlier version of this thesis, together with my other committee members Prof. Tamas Hausel and Prof. Beatriz Vicoso for being such friendly examiners at my thesis defence. I would also like to thank my mentor Prof. Max Jösch for helping me navigate my first year at ISTA and for chairing my qualifying exam.

Special thanks go to all the current and former group members – Kevin, Adelina, Nick, Francesa, Julian, Florian, Tal, Dante, Zhizhong, Margaret, and Jakob for countless lively mathematical and non-mathematical discussions, and for being such brilliant people to work with.

I'd like to acknowledge the many friendly and helpful support staff at ISTA, including Astrid Kober and Katja Rimpl for assistance with accommodation on campus, Birgit Oosthuizen-Noczil, Hanna Raszynska and Vlad Cozac for their administrative support, and IT services for assisting me on multiple occasions.

I have benefited greatly from the various activities at ISTA, including ultimate Frisbee, salsa dancing, the cycling group, the baking lab, and the chamber music group, and so I would like to extend my thanks to everyone I encountered in the ISTA community for making my time here so much more enjoyable. Thanks also go to Martin and my other climbing partners for their friendship and for introducing me to a sport which quickly became a new hobby. I'd like to thank Loki for always cheering me up on walks around ISTA, and Sinead and family for their food and warm hospitality.

Finally, thank you Jonathan, Mum and Dad for your constant support, and for patiently listening to the technical details of my mathematical travails even when you didn't understand a word.

**Funding:** I acknowledge the received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No. 665385  .

# About the Author

Alec Shute completed a Bsc at Imperial College London in 2017, and stayed there for a further year to complete a master's degree. He came to ISTA in September 2018, and joined the Browning group in 2019, where his research has been focused around analytic number theory and its application to problems in Diophantine geometry.

# List of Collaborators and Publications

Shute A. Sums of four squareful numbers. *arXiv:2104.06966*, 2021

Shute A. On the leading constant in the Manin-type conjecture for Campana points. *arXiv:2104.14946v2*, 2022

# Table of Contents

# Notation

## Geometry

We let $\mathbb{P}^n$ denote projective space of dimension $n$. The ring over which $\mathbb{P}^n$ is defined will be clear from the context, and will usually be $\mathbb{Q}$ or $\mathbb{Z}$. For a homogeneous polynomial $f \in \mathbb{Z}[x_1, \dots, x_n]$, we let $V(f)$ denote the zero locus of $f$, viewed as a closed subscheme of $\mathbb{P}^n$. By a *variety*, we mean a separated, geometrically integral scheme of finite type over a field. For a smooth variety $X$, we let $\omega_X$ denote the canonical line bundle on $X$.

## Analysis

For real functions $f$ and $g$, we write $f(x) = O(g(x))$ to mean that there exist real constants $C, x_0$ such that $|f(x)| \leqslant Cg(x)$ for all $x \geqslant x_0$. We also use the alternative notation $f(x) \ll g(x)$ to mean $f(x) = O(g(x))$ and $f(x) \gg g(x)$ to mean $g(x) = O(f(x))$. Estimates involving the parameter $\epsilon$ are assumed to hold for all sufficiently small $\epsilon > 0$, but with the implied constants $C, x_0$ allowed to depend on $\epsilon$. For example, we write $f(x) = O(x^\epsilon)$ to mean that for all $\epsilon > 0$, there exist constants $C, x_0$, depending on $\epsilon$, such that $f(x) \leqslant Cx^\epsilon$ for all $x \geqslant x_0$. Moreover, we adopt the convention that $\epsilon$ is allowed to take different values at different points in the argument, so that we do not have to keep track of coefficients of $\epsilon$ in our estimates. We indicate dependence of the implied constants $C, x_0$ on parameters other then $\epsilon$ with a subscript in the notation $O, \ll$ and $\gg$. We write $f(x) = o(g(x))$ to mean that $\lim_{x\to\infty}(f(x)/g(x)) = 0$, and $f(x) \sim g(x)$ to mean that $\lim_{x\to\infty}(f(x)/g(x)) = 1$. Unless otherwise stated, $|\cdot|$ denotes the supremum norm of a vector in $\mathbb{R}^n$.

## Number Theory

We take $\mathbb{N} = \mathbb{Z}_{\geqslant 1}$. We denote by $\mu : \mathbb{N} \to \{-1, 0, 1\}$ the Möbius function, which is $0$ on integers that are not squarefree, and $(-1)^r$ on integers with exactly $r$ distinct prime factors. We let $\tau(n)$ denote the number of divisors of an integer $n$. The letter $p$ will always denote a prime number unless otherwise stated. We denote by $(\mathbb{Z}^n_{\neq 0})_{\mathrm{prim}}$ the set of vectors $(a_1, \dots, a_n)$ such that $a_1, \dots, a_n$ are nonzero integers and $\gcd(a_1, \dots, a_n) = 1$. We write $n = \square$ to mean that

$n = m^2$ for some $m \in \mathbb{Z}$. We let $\nu_p$ denote the $p$-adic valuation, and $|\cdot|_p$ the $p$-adic norm. A field $K$ is assumed to be a number field unless otherwise stated. For a finite set of places $S$ of $K$, we let $\mathscr{O}_{K,S}$ denote the ring of $S$-integers of $K$.

CHAPTER 1

# Introduction

Given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with integer coefficients, what are its solutions over the integers or the rational numbers? Such equations are named *Diophantine equations* after Greek mathematician Diophantus of Alexandria, who lived in the 3rd Century A.D. Whilst extensively studied for more than two millennia, Diophantine equations remain a central and difficult topic in Number theory to this day, and have been the driving force behind the development of many new areas of mathematics.

In practice, it is often too ambitious to ask for an explicit list or parameterisation of all the solutions, and so we instead focus on counting the number of solutions. Some of the most natural questions, given a Diophantine equation $f(x_1, \ldots, x_n) = 0$ include

1. Are there any solutions?
2. Are there finitely or infinitely many solutions?
3. If there are infinitely many solutions, how are they distributed?

We remark that similar questions can be asked for systems of Diophantine equations $f_1 = \cdots = f_m = 0$. However, in this thesis, we shall focus on solutions to a single equation $f = 0$.

Suppose that the polynomial $f$ under consideration is homogeneous, i.e., all of its monomials have the same degree. In this case, $(0, \ldots, 0)$ is always a trivial solution to $f = 0$. Moreover, rational and integral solutions are essentially the same, in that any rational solution $(x_1, \ldots, x_n)$ can be transformed into an integral solution after scaling by an appropriate rational number $\lambda$. To formalise this, in the homogeneous case we consider the solutions not as

elements $(x_1, \dots, x_n)$ of $\mathbb{Z}^n$ or $\mathbb{Q}^n$, but as rational points $[x_1 : \cdots : x_n]$ in projective space $\mathbb{P}^{n-1}$, so that two solutions are viewed as the same if they are scalar multiples of each other, and the trivial solution $(0, \dots, 0)$ is automatically excluded.

In this introduction, we briefly summarise the main results of this thesis, leaving further comment of the context and surrounding literature to the relevant chapters.

## 1.1 Existence

Often, it is easy to see that $f = 0$ has no integer or rational solutions by showing that there are no solutions over some larger field or ring. For example, the polynomial $f(x, y) = x^2 + y^2$ has no nontrivial solutions over $\mathbb{R}$, and since $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, this implies there are no nontrivial solutions over $\mathbb{Q}$ or $\mathbb{Z}$ either. As another example, consider the polynomial $f(x, y) = x^2 - 3y^2 - 7$. Whilst $f = 0$ has solutions over $\mathbb{R}$, it has no solutions modulo $4$, and hence no solutions in the ring of $2$-adic integers $\mathbb{Z}_2$. Since $\mathbb{Z} \subseteq \mathbb{Z}_2$, this implies that $f = 0$ has no solutions over $\mathbb{Z}$.

For the remainder of this introduction, we consider for simplicity solutions to $f = 0$ over the rational numbers unless otherwise stated. We say that the equation $f = 0$ is *everywhere locally soluble* if it has solutions over $\mathbb{R}$ and over the $p$-adic fields $\mathbb{Q}_p$ for every prime $p$. (We recall that when $f$ is homogeneous, we require these solutions to be nontrivial.) Determining whether a given equation $f = 0$ is everywhere locally soluble is a relatively easy problem, thanks to tools such as Hensel's lemma. A natural question to therefore ask is whether $f = 0$ being everywhere locally soluble is enough to guarantee that $f = 0$ has solutions over $\mathbb{Q}$; in this case, we say that the *Hasse principle* holds.

The Hasse principle is known to hold for many important families of equations, including for example quadratic forms (i.e., $f$ is homogeneous of degree $2$) by the Hasse–Minkowski theorem [106, Theorem 8]. However, for higher degree forms, the Hasse principle can sometimes fail. One of the simplest counterexamples is due to Selmer [103], who demonstrated that the equation $3x^3 + 4y^3 + 5z^3 = 0$ has solutions everywhere locally but not over $\mathbb{Q}$. It therefore becomes an interesting question to determine under what circumstances the Hasse principle does still hold.

In Chapter 8, we consider the Hasse principle for a family of equations of the form

$$f(t) = \mathbf{N}_{K/\mathbb{Q}}(x_1, \dots, x_n) \neq 0, \tag{1.1.1}$$

where here, $f \in \mathbb{Z}[t]$ is a polynomial, and $\mathbf{N}_{K/\mathbb{Q}}(x_1, \dots, x_n)$ is the *norm form* associated to a number field $K/\mathbb{Q}$ of degree $n$, as we shall now define. We fix a

basis $\omega_1, \dots, \omega_n$ for $K$, viewed as an $n$-dimensional vector space over $\mathbb{Q}$. Then the norm form $\mathbf{N}_{K/\mathbb{Q}}(x_1, \dots, x_n)$ is a polynomial of degree $n$ in $n$ variables defined by the equation

$$\mathbf{N}_{K/\mathbb{Q}}(x_1, \dots, x_n) = N_{K/\mathbb{Q}}(\omega_1 x_1 + \cdots + \omega_n x_n), \tag{1.1.2}$$

where $N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ denotes the field norm. Whilst the norm form itself depends on the particular choice of basis $\omega_1, \dots, \omega_n$, the set of values it takes as $x_1, \dots, x_n$ range over $\mathbb{Q}$ does not. Therefore, for us the choice of basis will be unimportant.

A basic example is the number field $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$ is squarefree. A basis for $K$ is $\{1, \sqrt{d}\}$, and so the norm form is given by $\mathbf{N}(x, y) = x^2 - dy^2$.

Even in the family (1.1.1), the Hasse principle sometimes fails. The following counterexample was provided by Iskovskikh [70]. We make the choice $f(t) = (t^2 - 2)(-t^2 + 3)$ and $K = \mathbb{Q}(i)$, so that $\mathbf{N}(x, y) = x^2 + y^2$. Then Iskovskikh showed that (1.1.1) has solutions over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes $p$, but not over $\mathbb{Q}$.

Local to global questions for (1.1.1) have received much attention over the years, and several results have been obtained when $f$ and $K$ have relatively small degree. (A more detailed account is provided in the introduction of Chapter 8.) In this work, we establish the Hasse principle for (1.1.1) for a wide family of polynomials $f$, which may be a product of arbitrarily many linear, quadratic or cubic factors. This represents the first result of its kind where the polynomial $f$ can have arbitrarily large degree, besides a result of Browning and Matthiesen [19] in which all irreducible factors of $f$ are assumed to be linear.

Let $G$ denote the Galois group of the Galois closure of $K/\mathbb{Q}$, viewed as a permutation group acting on the $n$ roots of the minimum polynomial of $K/\mathbb{Q}$. We define

$$T(G) = \frac{1}{\#G}\#\{\sigma \in G : \text{ the cycle lengths of } \sigma \text{ are not coprime}\}. \tag{1.1.3}$$

Roughly speaking, the *Hasse norm principle* holds for $K/\mathbb{Q}$ if every element $c \in \mathbb{Q}^\times$ that is a local norm at every place of $K$ is also a norm of an element of $K$. Examples include when $[K : \mathbb{Q}]$ is prime [2], or $[K : \mathbb{Q}] = n$ and $G = S_n$ [76] or $G = A_n$ [83].

We now state the main results of Chapter 8 in a slightly simplified form, referring the reader to Theorems 8.1.1 and 8.1.2 for more general statements.

**Theorem A.** Suppose $K$ is a number field satisfying the Hasse norm principle. Let $f \in \mathbb{Z}[t]$ be a polynomial, all of whose irreducible factors have degree at most $2$. Suppose that $T(G) < \frac{0.39006\dots}{\deg f + 1}$. Then the Hasse principle holds for (1.1.1).

An interesting example of Theorem A is the case when $f$ is a product of two non-proportional quadratic polynomials and $G = S_n$. In Chapter 8, we obtain the following corollary.

**Corollary B.** Let $f \in \mathbb{Z}[t]$ be a product of two non-proportional irreducible quadratic polynomials. Let $K$ be a number field of degree $n$ with $G = S_n$. Let $L$ be the biquadratic number field generated by $f$, and $\widehat{K}$ the Galois closure of $K/\mathbb{Q}$. Suppose that $L \cap \widehat{K} = \mathbb{Q}$. Then the Hasse principle holds for (1.1.1), provided that

$$n \notin \{2, 3, \dots, 10, 12, 14, 15, 16, 18, 20, 22, 24, 26, 28, 30, 36, 42, 48\}.$$

In the Appendix, we show that Corollary B is consistent with what we know about the Brauer group for equations of the form (1.1.1). More precisely, we show that if $X$ is a smooth projective model of (1.1.1), and $(f, K)$ satisfy the hypotheses of Corollary B, then $\mathrm{Br}(X) = \mathrm{Br}(\mathbb{Q})$.

Our second main result allows $f$ to contain irreducible cubic factors, but requires a more restrictive assumption on the number field $K$.

**Theorem C.** Let $f \in \mathbb{Z}[t]$ be a polynomial, all of whose irreducible factors have degree at most $3$. Let $K$ be a number field of the form $\mathbb{Q}[x]/(x^q - r)$, where $q$ is a prime and $r$ is an integer such that the polynomial $x^q - r$ is irreducible in $\mathbb{Z}[x]$. Suppose that $q \geqslant (4.08825...) \deg f + 1$. Then the Hasse principle holds for (1.1.1).

We prove Theorems A and C by generalising an argument of Irving [69], which proceeds via an algebraic reduction to a sieve problem, followed by an application of the beta sieve of Rosser and Iwaniec [52, Chapter 11]. We introduce sieve methods in Chapter 5, as well as stating the main auxiliary sieve results which we use to prove Theorems A and C. In Section 8.4, we demonstrate a further application of these sieve results to a conjecture of Harpaz and Wittenberg on locally split values of polynomials over number fields, which has consequences for rational points in fibrations.

## 1.2 Density

We now turn to one of the other main questions stated at the beginning, namely the distribution of rational points. One way to interpret this is to fix a *height function* $H$, which assigns to each rational solution a non-negative real number measuring the "complexity" of the solution. For homogeneous polynomials $f \in \mathbb{Z}[x_1, \dots, x_n]$, where we view solutions as points $x = [x_1 : \cdots : x_n]$ in projective space, the most naive choice of height is given by scaling $x_1, \dots, x_n$

so that they are integers with $\gcd(x_1, \dots, x_n) = 1$, and then defining

$$H([x_1 : \cdots : x_n]) = \max_{1 \leqslant i \leqslant n} |x_i|. \tag{1.2.1}$$

However, there are many other possible height functions one can take. We discuss heights in more generality in Section 2.2. Let

$$N(B) = \#\{x \in \mathbb{P}^{n-1}(\mathbb{Q}) : f(x) = 0, H(x) \leqslant B\}.$$

A key feature of the height in (1.2.1) is the *Northcott property*, which states that $N(B)$ is finite for any given real number $B$. For a height satisfying the Northcott property, it makes sense to ask about the asymptotic behaviour of $N(B)$ as $B \to \infty$.

A more geometric way to set up the above problem is to consider a projective algebraic variety $X$ defined by a polynomial $f$. The nonzero rational solutions to $f = 0$ modulo scaling coincide with the set of rational points $X(\mathbb{Q})$, and we can view the height as a function $H : X(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$. In Chapter 2, we discuss Manin's conjecture [50], which, for a projective variety $X$, gives a prediction for the asymptotic behaviour of $N(B)$ in terms of the geometry of $X$. Manin's conjecture applies only to smooth *Fano varieties*, for which we expect $X(\mathbb{Q})$ to be infinite as soon as it is non-empty. For example, a smooth variety $X \subseteq \mathbb{P}^{n-1}$ defined by $f(x_1, \dots, x_n) = 0$ is Fano if $f$ homogeneous of degree $d < n$. Manin's conjecture [50], together with a refinement due to Peyre [92, Formule empirique 5.1] predicts an asymptotic formula for $N(B)$ of the shape

$$N(B) \sim cB^a(\log B)^{b-1}$$

for explicit constants $a, b \geqslant 1$ and $c > 0$. It turns out that in order for Manin's conjecture to hold, the contribution to $N(B)$ from certain accumulating sets (e.g. proper closed subvarieties and thin sets) must first be removed, since these have the potential to dominate the count.

Similar questions can be asked for integral points, although these are less well understood, even conjecturally. As already remarked, if $X$ is a projective variety (so $f$ is homogeneous), then rational and integral points coincide, but in other cases, we must fix a choice of integral model $\mathscr{X}$ for $X$ and try to count points in $\mathscr{X}(\mathbb{Z})$ of bounded height. To date, we have no analogue of Manin's conjecture in this setting, although partial conjectures do exist. Questions concerning the existence of integral points are also often more subtle than their counterparts for rational points.

In this work, we study the notion of *Campana points*, which is an area of growing interest in Arithmetic geometry thanks to its ability to interpolate between rational and integral points. Roughly speaking, Campana points on a projective variety $X$ are rational points which are integral with respect to a

weighted boundary divisor. We provide a more detailed discussion in Chapter 3. Arithmetically, Campana points correspond to powerful values of polynomials (see Example 3.0.5). We say that a nonzero integer $n$ is $m$-*full* if for any prime $p$ dividing $n$, we have that $p^m$ also divides $n$, and *squareful* if it is 2-full.

Similarly to rational and integral points, we can seek to understand Campana points quantitatively by studying asymptotically the number $N(B)$ of Campana points of height bounded by $B$ as $B \to \infty$. One of the motivating examples for the development of the theory is the counting problem

$$\#\mathscr{N}_k(B) = \#\left\{\mathbf{z} \in (\mathbb{Z}_{\neq 0})^k_{\mathrm{prim}} : |z_i| \leqslant B, z_i \text{ squareful for all } i, \sum_{i=1}^{k} z_i = 0\right\}, \tag{1.2.2}$$

where $(\mathbb{Z}_{\neq 0})^k_{\mathrm{prim}}$ denotes the condition that $\mathbf{z} = (z_1, \dots, z_k) \in \mathbb{Z}^k$ should satisfy $z_i \neq 0$ for all $i$ and $\gcd(z_1, \dots, z_k) = 1$. We remark that if we remove the equation $\sum_{i=1}^{k} z_i = 0$ from (1.2.2), then the resulting counting problem can be treated using elementary methods. We demonstrate this in Section 3.3.

The counting problem in (1.2.2) generalises a question posed by Poonen in 2006 [98], who asked for an asymptotic formula for $\#\mathscr{N}_3(B)$. This corresponds to counting Campana points on $X = \mathbb{P}^1$ with a divisor $\frac{1}{2}[1:0] + \frac{1}{2}[1:1] + \frac{1}{2}[0:1]$ and with the naive height defined in (1.2.1). Whilst Poonen's question seems out of reach at the moment, an asymptotic formula for $\#\mathscr{N}_k(B)$ when $k \geqslant 5$ was found by Van Valckenborgh [117]. In Chapter 6, we treat the case $k = 4$.

For an integer $n$, we write $n = \square$ to mean that $n = m^2$ for some $m \in \mathbb{Z}$. A new feature that appears when $k = 4$ is the presence of an accumulating set of the form

$$\mathscr{T} = \{(z_1, \dots, z_4) \in (\mathbb{Z}_{\neq 0})^4_{\mathrm{prim}} : z_1 \cdots z_4 = \square\}. \tag{1.2.3}$$

We remove the contribution from this set by considering the counting problem

$$N(B) = \#(\mathscr{N}_4(B) \backslash \mathscr{T}). \tag{1.2.4}$$

In Chapter 6, we prove the following theorem.

**Theorem D.** We have

$$N(B) = cB + O(B^{734/735+\epsilon}), \tag{1.2.5}$$

where the implied constant depends only on $\epsilon$. The constant $c$ is positive and is given explicitly in (6.5.9) and Lemma 6.6.1.

The proof of Theorem D proceeds via an application of circle method. Whilst a classical form of the circle method was employed by Van Valckenbourgh to treat (1.2.2) for $k \geqslant 5$, for $k = 4$ this is not sufficient. We instead appeal to a more modern formulation known as the *delta method*, which was introduced by Duke,

Friedlander and Iwaniec in 1993 [46], and further developed by Heath–Brown in 1995 [61]. In Chapter 4, we introduce the circle method and indicate how it can be applied to study $\#\mathscr{N}_k(B)$.

In 2019, Pieropan, Smeets, Tanimoto and Várilly-Alvarado formulated a bold new prediction for the density of Campana points in the Fano case, which provides a vast generalisation of Manin's conjecture [96]. Henceforth, we shall refer to their conjecture as the *PSTV-A conjecture*. We give the precise statement in Conjecture 3.0.8, and summarise the main known cases in Section 3.1.

In Chapter 6, we demonstrate that the power of $B$ and $\log B$ obtained in Theorem D are consistent with the PSTV-A conjecture. However, the leading constant $c$ seems more problematic. In Chapter 7, we carry out a detailed investigation of the leading constant in the PSTV-A conjecture, and obtain the following counterexample. For odd, squarefree and coprime integers $a$ and $b$, let

$$N(B) = \frac{1}{2}\#\left\{(x,y) \in \mathbb{Z}^2_{\mathrm{prim}} : |x|, |y| \leqslant B, ax^2 + by^2 \text{ squareful}\right\}.$$

**Theorem E.** Let $a = 37$ and $b = 109$. Then the PSTV-A conjecture does not hold for $N(B)$.

In fact, we demonstrate that there are infinitely many choices of $a$ and $b$ for which the conjecture does not hold, and in Theorem 7.1.5 we find an asymptotic formula for $N(B)$ for any $a$ and $b$.

CHAPTER 2

# Manin's conjecture

## 2.1 Geometry determines arithmetic

A key principle in Arithmetic geometry is that the existence and density of rational solutions to polynomial equations should be governed by geometric properties of the corresponding algebraic variety. Perhaps one of the most striking demonstrations of this principle is the effect the anticanonical line bundle $\omega_X^\vee$ can have on the density of rational points on a smooth projective variety $X$.

At one extreme, we have *Fano varieties*, which are smooth varieties with $\omega_X^\vee$ ample. Here, if the set of rational points $X(\mathbb{Q})$ is non-empty, we expect it to be infinite. In fact, a far-reaching conjecture of Colliot-Thélène [31] predicts that if $X$ is rationally connected (a more general notion than that of being Fano) and $X(\mathbb{Q}) \neq \emptyset$, then $X(\mathbb{Q})$ is Zariski dense in $X$, and so in particular, $X(\mathbb{Q})$ is infinite.

At the other extreme, we have varieties of *general type*, where $\omega_X$ is ample. Here, we expect very few rational points. In the case of curves, Mordell's conjecture, proved by Faltings in 1983, states that if $X$ is of general type, then $X(\mathbb{Q})$ is finite [48]. Very little is known about higher-dimensional cases, although it is conjectured by Bombieri and Lang that if $X$ is of general type, then $X(\mathbb{Q})$ is not Zariski dense, i.e., $X(\mathbb{Q})$ is contained in a proper closed subvariety of $X$ [66, Section F.5.2].

Varieties that do not fit into either of the above categories are called *intermediate type*. This very rich class of varieties can exhibit a wide range of different behaviours, and here $X(\mathbb{Q})$ is sometimes Zariski dense, and sometimes not. However, even when $X(\mathbb{Q})$ is infinite, rational points are typically much more "sparse" compared to Fano varieties, in the sense that the number of points of height bounded by $B$ grows very slowly as we increase $B$.

For example, suppose that $X \subseteq \mathbb{P}^n$ is a hypersurface of degree $d$. Then $\omega_X^\vee \cong \mathscr{O}_X(n+1-d)$ [59, Example II.8.20.3]. Since $\mathscr{O}_X(k)$ is very ample if and only if $k \geqslant 1$, we see that $X$ is Fano if $d \leqslant n$, general type if $d \geqslant n+2$, and intermediate type if $d = n+1$. We collect together some further examples in Table 5.2.

| | Definition | Curves | Surfaces | Hypersurfaces in $\mathbb{P}^n$ of degree $d$ |
|---|---|---|---|---|
| Fano | $\omega_X^\vee$ ample | $\mathbb{P}^1$, conics | del Pezzo surfaces | $d \leqslant n$ |
| Intermediate type | $\omega_X, \omega_X^\vee$ not ample | elliptic curves | $K3$ surfaces, abelian surfaces | $d = n+1$ |
| General type | $\omega_X$ ample | curves of genus $\geqslant 2$ | | $d \geqslant n+2$ |

Table 2.1: Examples of Fano, intermediate type and general type varieties

## 2.2 Heights

When $X(\mathbb{Q})$ is infinite, we can seek to understand the distribution of rational points more quantitatively using the notion of heights. We recall from the introduction that a height function on $X$ is a map $H : X(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$. If we are given an embedding $X \subseteq \mathbb{P}^n$, the most obvious choice of height is the one from (1.2.1), which we recall is given by

$$H(x) = \max_{0 \leqslant i \leqslant n} |x_i| \tag{2.2.1}$$

for $(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}_{\text{prim}}$ representing $x$. For a given height $H$, we seek an asymptotic formula for the quantity

$$N(B) = \#\{x \in X(\mathbb{Q}) : H(x) \leqslant B\}. \tag{2.2.2}$$

As a first example, it is easy to show using Möbius inversion that when $X = \mathbb{P}^n$ and $H$ is given by (2.2.1), we have

$$N(B) \sim \frac{2^n}{\zeta(n+1)} B^{n+1}. \tag{2.2.3}$$

We consider again the example of a smooth hypersurface $X \subseteq \mathbb{P}^n$ of degree $d$. By the above example, there are up to a constant $B^{n+1}$ choices for $x \in \mathbb{P}^n(\mathbb{Q})$

with $H(x) \leqslant B$. We represent each such $x$ by a vector $\mathbf{x} = (x_0, \dots, x_n) \in \mathbb{Z}^{n+1}_{\text{prim}}$. Let $f$ be the polynomial defining $X$. Since $|x_i| \leqslant B$ for each $i$, we know that $f(\mathbf{x}) = O(B^d)$, where the implied constant depends only on $f$. We might therefore expect the probability $f(\mathbf{x})$ is zero to be roughly $B^{-d}$, and hence $N(B)$ to have size roughly $B^{n+1-d}$. This naive heuristic suggests that Fano hypersurfaces, where $d \leqslant n$, should contain infinitely many rational points, whilst intermediate and general type hypersurfaces should contain far fewer rational points.

All known asymptotic formulas for $N(B)$ take the shape

$$N(B) \sim cB^a(\log B)^b \tag{2.2.4}$$

for some constants $a, b, c \geqslant 0$. For varieties of intermediate type, the growth of $N(B)$ is often logarithmic. This holds true, for example, if $X$ is an abelian variety [104, Section 5.4]. In contrast, for Fano varieties, we expect that whenever $X(\mathbb{Q}) \neq \emptyset$, there are many rational points, in the sense that (2.2.4) holds for some $a, c > 0$.

The choice of embedding $X \subseteq \mathbb{P}^n$ significantly impacts the asymptotic behaviour of $N(B)$. We now explain how to keep track of this dependence by relating embeddings $X \subseteq \mathbb{P}^n$ to very ample line bundles $\mathscr{L}$ on $X$. This has the advantage of making our counting problems more intrinsic to the variety, and paves the way for more precise conjectures about the growth rate of $N(B)$.

Suppose that $X$ is a projective variety and $\mathscr{L}$ is a line bundle on $X$. By a cohomological result of Serre [59, Theorem III.5.2], the global sections of $\mathscr{L}$ form a finite dimensional vector space over $\mathbb{Q}$, which we denote by $\Gamma(X, \mathscr{L})$. Let $(s_0, \dots, s_n)$ be a generating set for $\Gamma(X, \mathscr{L})$. Suppose that $s_0, \dots, s_n$ never simultaneously vanish at any point $x$ of $X$ (in this case, we say that $\mathscr{L}$ is *basepoint-free*). Then we have a well-defined map

$$\begin{aligned} \varphi : X &\to \mathbb{P}^n \\ x &\mapsto [s_0(x) : \cdots : s_n(x)]. \end{aligned}$$

In fact, as shown in [59, Theorem II.7.1], we can recover $\mathscr{L}$ and $(s_0, \dots, s_n)$ up to isomorphism from $\varphi$ via the pullbacks $\mathscr{L} = \varphi^*\mathscr{O}(1)$ and $s_i = \varphi^*(x_i)$, where $x_0, \dots, x_n$ are coordinates on $\mathbb{P}^n$. Consequently, there is a bijective correspondence between ismorphism classes of basepoint-free line bundles $\mathscr{L}$ on $X$ with a choice of generating set $(s_0, \dots, s_n)$, and morphisms $\varphi : X \to \mathbb{P}^n$.

We could already define the height of $x \in X(\mathbb{Q})$ to be $H(\varphi(x))$, where $H$ is given in (2.2.1). However, in order to ensure that our height satisfies the Northcott property, we would like $\varphi$ to be an embedding. We say that $\mathscr{L}$ is *very ample* if it is basepoint-free, and the map $\varphi$ is an embedding for some choice of generating set $(s_0, \dots, s_n)$.

We denote a height function resulting from the above construction by $H_{\mathscr{L}}$; typically, we suppress the dependence on $s_0, \dots, s_n$ in our notation. We say that $\mathscr{L}$ is *ample* if some tensor power $\mathscr{L}^{\otimes k}$ for $k \geqslant 1$ is very ample. For ample line bundles $\mathscr{L}$, it is natural to define a height function $H_{\mathscr{L}} : X(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$ by $H_{\mathscr{L}}(x) = (H_{\mathscr{L}^{\otimes k}}(x))^{1/k}$.

For example, let $X = \mathbb{P}^n$ with coordinates $x_0, \dots, x_n$ and $\mathscr{L} = \mathscr{O}_X(d)$. Then the global sections of $\mathscr{L}$ are generated by the set of all monomials of degree $d$ in $x_0, \dots, x_n$. With this generating set, the corresponding morphism $\varphi : \mathbb{P}^n \to \mathbb{P}^N$ is the Veronese embedding of degree $d$, with $N = \binom{n+d}{n} - 1$. The height function we obtain is

$$H_{\mathscr{L}}(x) = \max_{\substack{(\alpha_0,\dots,\alpha_n) \in \mathbb{N}^{n+1} \\ \alpha_0 + \cdots + \alpha_n = d}} |x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_n^{\alpha_n}| = \max_{0 \leqslant i \leqslant n} |x_i|^d,$$

where $\mathbf{x} = (x_0, \dots, x_n) \in \mathbb{Z}^{n+1}_{\mathrm{prim}}$. However, there are many other generating sets we could choose. For example, in Chapter 7, we consider $X = \mathbb{P}^1, \mathscr{L} = \mathscr{O}(1)$, and the generating set $(x_0, x_1, x_0 + x_1)$ for $\Gamma(X, \mathscr{L})$. This gives rise to the height $H_{\mathscr{L}}(x) = \max(|x_0|, |x_1|, |x_0 + x_1|)$, where $(x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}$ represents $x$.

### 2.2.1 Local heights

In some situations, it is convenient to express a height function $H : X(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$ as a product of local heights at the places of $\mathbb{Q}$. For example, consider the naive height from (1.2.1). Let $v$ denote a place of $\mathbb{Q}$, and let $|\cdot|_v$ denote the $p$-adic metric if $v = p$ is prime, or the usual Euclidean metric if $v = \infty$. Then $H$ can be expressed as $H(x) = \prod_v H_v(x)$, where

$$H_v(x) = \max_{0 \leqslant i \leqslant n} |x_i|_v.$$

Whilst the individual heights $H_v$ depend on the representative $[x_0 : \cdots : x_n]$ of $x$, their product does not, thanks to the product formula [72, Fact 1.8].

In the more general setting of heights $H_{\mathscr{L}}$ for a line bundle $\mathscr{L}$ on $X$, we can define local heights by fixing an *adelic metrization* on $\mathscr{L}$, which is a system of metrics $\|\cdot\|_v$ on the line bundles $\mathscr{L} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}_v}$ of $X(\overline{\mathbb{Q}_v})$ satisfying certain properties [94, Definition 2.5]. However, for our purposes, it will be sufficient to consider local heights of the form

$$H_{\mathscr{L},v}(x) = \max_{0 \leqslant i \leqslant n} \left| \frac{s_i(x)}{s(x)} \right|_v, \tag{2.2.5}$$

where $s_0, \dots, s_n$ is the choice of generating set for $\Gamma(X, \mathscr{L})$ and $s$ is a section of $\mathscr{L}$ satisfying $s(x) \neq 0$. Again, by the product formula, we recover the global height $H_{\mathscr{L}}$ defined above (at least away from the zero locus of $s$) when taking the product of the local heights over all places $v$.

## 2.3 Manin's conjecture

In 1989, Batyrev and Manin [50] formulated a major conjecture on the asymptotic behaviour of $N(B)$ for Fano varieties admitting a rational point, which is commonly referred to as *Manin's conjecture*. In this section, we introduce Manin's conjecture and discuss various known cases and refinements.

Sometimes, the count $N(B)$ from (2.2.2) may be dominated by rational points on a proper closed subvariety of $X$. Such subvarieties are called *accumulating*. For example, consider a cubic surface $X \subseteq \mathbb{P}^3$. The naive heuristic from Section 2.2 would suggest that (2.2.4) should hold with exponent $a = 1$. However, it is a classical fact that $X$ contains 27 lines over $\overline{\mathbb{Q}}$ [59, Theorem V.4.9]. If some of these lines happen to be defined over $\mathbb{Q}$, they will each contain $B^2$ rational points up to a constant, by (2.2.3). It is natural to ask how $N(B)$ behaves after removing all accumulating subvarieties. For a Zariski open subset $U \subseteq X$, we therefore define a new counting function

$$N_{U,\mathscr{L}}(B) = \#\{x \in U(\mathbb{Q}) : H_{\mathscr{L}}(x) \leqslant B\}. \tag{2.3.1}$$

Let $\mathrm{Pic}(X)$ denote the Picard group, which is the abelian group of isomorphism classes of line bundles on $X$, with multiplication given by the tensor product. Below, we freely make use of the isomorphism between $\mathrm{Pic}(X)$ and the group $\mathrm{Cl}(X)$ of Weil divisors on $X$ modulo linear equivalence (see [59, Corollary II.6.16]). For a divisor $D$, we denote by $[D]$ its class in $\mathrm{Cl}(X)$, and we write $D \geqslant 0$ to mean that $D$ is effective. The *real cone of effective divisors* $\Lambda_{\mathrm{eff}}$ is defined as

$$\Lambda_{\mathrm{eff}} = \{[D] \in \mathrm{Cl}(X) \otimes_{\mathbb{Z}} \mathbb{R} : D \geqslant 0\}. \tag{2.3.2}$$

Let $[K_X] \in \mathrm{Cl}(X)$ be the canonical divisor class, which corresponds to the canonical line bundle $\omega_X$, and let $[L]$ be the divisor class corresponding to $\mathscr{L}$. We define

$$a = \inf\{t \in \mathbb{R} : t[L] + [K_X] \in \Lambda_{\mathrm{eff}}\}, \tag{2.3.3}$$

and we define $b$ to be the codimension of the minimal supported face of $\Lambda_{\mathrm{eff}}$ which contains $a[L] + [K_X]$.

**Example 2.3.1.** We consider once more the case of a smooth hypersurface $X \subseteq \mathbb{P}^n$ of degree $d$, and $\mathscr{L} = \mathscr{O}_X(1)$. We have $\omega_X \cong \mathscr{O}(d - n - 1)$ [59, Example 8.20.3], and so $t[L] + [K_X]$ is effective if and only if $t \geqslant n + 1 - d$. Therefore, $a = n + 1 - d$. We observe that this agrees with the exponent of $B$ predicted by the naive heuristic from Section 2.2. Moreover, we have $a[L] + [K_X] = 0$, and so the minimal supported face of $\Lambda_{\mathrm{eff}}$ containing $a[L] + [K_X]$ is $\{0\}$. Therefore, $b$ is equal to the dimension of $\Lambda_{\mathrm{eff}}$, which is the rank of the Picard group $\mathrm{Pic}(X)$, commonly referred to as the *Picard number* $\varrho(X)$. When $n \geqslant 4$, so $X$ has dimension at least 3, it turns out that $b = 1$. This is because for smooth

complete intersections of dimension at least $3$, the Picard number is $1$ by a version of the Lefschetz hyperplane theorem [79, Example 3.1.25].

We now come to the statement of Manin's conjecture. We begin by stating the conjecture in its classical form, before discussing a refinement due to Peyre which allows for the removal of thin accumulating sets (see Conjecture 2.3.4).

**Conjecture 2.3.2** (Manin's conjecture [50])**.** *Let $X$ be a Fano variety and let $\mathscr{L}$ be an ample line bundle on $X$, with a corresponding height function $H_{\mathscr{L}}$. Suppose that $X(\mathbb{Q})$ is Zariski dense in $X$. Then there exists a constant $c > 0$ and a Zariski open subset $U \subseteq X$ such that*

$$N_{U,\mathscr{L}}(B) \sim cB^a(\log B)^{b-1}, \tag{2.3.4}$$

*where $a$ and $b$ are given by (2.3.3).*

The leading constant $c$ has also been given a conjectural interpretation by Peyre [92, Formule empirique 5.1]. It should be noted that the exponents $a$ and $b$ depend on the choice of line bundle $\mathscr{L}$, but not the generating set $s_0, \dots, s_n$ used to define $H_{\mathscr{L}}$. In contrast, the leading constant $c$ does depend on the particular choice of generating set. We remark also that Manin's conjecture is commonly stated with the choice $[L] = [-K_X]$, so that $H_{\mathscr{L}}$ is an anticanonical height. In this case, it is clear from (2.3.3) that $a = 1$ and $b$ is the Picard number $\varrho(X)$.

When the variety $X$ has a very large dimension compared to its degree, the Hardy–Littlewood circle method is an effective tool to count rational points. The seminal work of Birch [7] establishes that if $f \in \mathbb{Z}[x_0, \dots, x_n]$ is a non-singular homogeneous polynomial of degree $d \geqslant 2$ satisfying $n \geqslant (d-1)2^d$, then there exists a constant $c$ such that $N(B) \sim cB^{n+1-d}$. This is consistent with Conjecture 2.3.2 (which Birch's result predates), since by Example 2.3.1, we have $a = n+1-d$ and $b = 1$ in this setting. Whilst Birch's result represents a major step forward, we note that it assumes a much stronger condition on the size of $n$ compared to the Fano range $n \geqslant d$ where we expect Manin's conjecture to hold. We discuss Birch's result and the circle method further in Chapter 4.

A very different approach is to study the *height zeta function* associated to an open subset $U \subseteq X$, which is defined as

$$Z_U(s) = \sum_{x \in U(\mathbb{Q})} H(x)^{-s}. \tag{2.3.5}$$

A Tauberian theorem can then be used to relate analytic properties of $Z(s)$ with the counting problem $N(B)$. This method has has been successfully employed by Franke, Manin and Tschinkel to establish Manin's conjecture for

flag varieties [50], Batyrev and Tschinkel for toric varieties [5], and Chambert-Loir and Tschinkel for smooth equivariant compactifications of vector groups [28].

Fano varieties of dimension $2$ are known as *del Pezzo surfaces*. Del Pezzo surfaces are either isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ or the blowup of $\mathbb{P}^2$ at $9-d$ points in general position. The quantity $d$ is called the *degree* of the del Pezzo surface. The study of rational points on del Pezzo surfaces becomes much more challenging as the degree decreases. For $d \geqslant 6$, Manin's conjecture is known to hold as a special case of [5], since these del Pezzo surfaces are toric. There are very few known cases of Manin's conjecture for $d \leqslant 5$, with notable exceptions including split del Pezzo surfaces of degree $5$ [42], and a quartic del Pezzo surface with a conic fibration [43]. However, there are many known upper and lower bounds, as well as results for singular del Pezzo surfaces. A survey can be found in [9].

It turns out that Manin's conjecture, as stated in Conjecture 2.3.2, is false. Whilst we have stated Manin's conjecture over $\mathbb{Q}$, in [50] it is formulated over an arbitrary number field. The first known counterexamples were found by Batyrev and Tschinkel in 1996 [4], over the number field $\mathbb{Q}(\sqrt{-3})$. Let $X$ be a Fano cubic bundle in $\mathbb{P}^3 \times \mathbb{P}^3$, defined by the equation

$$\sum_{i=0}^{3} x_i y_i^3 = 0. \tag{2.3.6}$$

Batyrev and Tschinkel [4, Corollary 2.4] demonstrate that whenever $a_0, \dots, a_3$ are all cubes in $\mathbb{Q}(\sqrt{-3})^*$, the rational points on the hypersurface $Y_{\mathbf{a}}$ defined by $\sum_{i=0}^{3} a_i y_i^3$ grow more quickly than predicted by (2.3.4). Moreover, the infinite union over all such hypersurfaces is not a Zariski closed subset of $X$. Thanks to the work of Loughran [82], we now have counterexamples over any number field, including $\mathbb{Q}$ itself. Later, Browning and Heath-Brown [17] studied rational points on the quadric bundle $X \subseteq \mathbb{P}^3 \times \mathbb{P}^3$ given by the equation

$$\sum_{i=0}^{3} x_i y_i^2 = 0. \tag{2.3.7}$$

Here, rational points for which $x_0 x_1 x_2 x_3$ is a square of a rational number are shown to dominate, providing a further counterexample to Conjecture 2.3.2.

Whilst Conjecture 2.3.2 is false, all hope is not lost. Peyre has introduced several reformulations of the conjecture. For example, Peyre [92] suggests adapting Manin's conjecture to allow for the removal of *thin* accumulating sets, which we discuss in more detail below. More recently, in [94, Section 4], Peyre formulates a way to consider not just a single height associated to some ample line bundle, but all the heights simultaneously. Another idea introduced in [93] is to allow for the removal of rational points with a small *freeness*. Roughly

speaking, freeness measures how large the slopes of the lattice defined by the tangent bundle $T_xX$ are compared to the height of the point $x$. However, it was shown by Sawin [100] that Manin's conjecture still does not hold in this setting.

Thin sets arise from the following two geometric constructions:

1. Proper Zariski closed subsets $Z \subsetneq X$ (as encountered already in Conjecture 2.3.2),
2. Images of dominant morphisms $\varphi : V \to X$ of degree at least $2$ from an integral projective variety $V$ with $\dim V = \dim X$.

**Definition 2.3.3.** Let $Z$ and $\varphi : V \to X$ be as in (1) and (2) above, and let $K$ be a number field. A subset $A \subset X(K)$ is *type I* if $A = Z(K)$, and *type II* if $A = \varphi(V(K))$. A *thin set* is a subset of $X(K)$ which is contained in a finite union of type I and type II sets.

As a basic example, let $K = \mathbb{Q}, X = V = \mathbb{P}^1$, and let $\varphi : V \to X$ be the morphism sending $[x_0 : x_1]$ to $[x_0^2 : x_1^2]$. Then $\varphi(V(\mathbb{Q}))$ is a type II thin set, consisting of the point $[0 : 1]$ and all points of the form $[1 : t]$, where $t$ is the square of a rational number.

We now state a modified version of Manin's conjecture allowing for the removal of thin sets.

**Conjecture 2.3.4** (Manin–Peyre conjecture [92])**.** *Let $X$ and $\mathscr{L}$ be as in Conjecture 2.3.2. Then there exists a constant $c > 0$ and a thin subset $A \subseteq X(\mathbb{Q})$ such that*

$$\#\{x \in X(\mathbb{Q}) \backslash A : H_{\mathscr{L}}(x) \leqslant B\} \sim cB^a(\log B)^{b-1}, \tag{2.3.8}$$

*where $a$ and $b$ are given by (2.3.3).*

To date, Conjecture 2.3.4 remains consistent with all known results about the density of rational points on Fano varieties. In the counterexample (2.3.6) considered by Batyrev and Tschinkel, the union of the cubic hypersurfaces $Y_{\mathbf{a}}$ is a thin subset of $X(\mathbb{Q}(\sqrt{-3}))$, coming from the morphism

$$\begin{gathered} \pi : V \to X \\ ([x_0 : x_1 : x_2 : x_3], \mathbf{y}) \mapsto ([x_0^3 : x_1^2 : x_2^3 : x_3^3], \mathbf{y}), \end{gathered}$$

where $V \subseteq \mathbb{P}^3 \times \mathbb{P}^3$ is the variety defined by $\sum_{i=0}^3 x_i^3 y_i^3 = 0$. In the context of the quadric bundle (2.3.7) considered by Browning and Heath-Brown, the set of rational points such that $x_0x_1x_2x_3$ is a square also forms a thin set. This follows from a very similar argument to Lemma 6.2.1, which we prove later

in this work. Moreover, the authors were able to count rational points on the complement of this thin set, thus establishing Conjecture 2.3.4 for this quadric bundle.

Whilst Conjecture 2.3.4 does not stipulate which thin set should be removed, we would in general expect there to be a choice which somehow reflects the geometry of $X$. Lehmann, Sengupta and Tanimoto [81] have pursued this idea, formulating an explicit geometric prediction for a choice of thin exceptional set $A$ such that the asymptotic (2.3.8) should hold. Their work also provides geometric evidence that thin sets are the correct notion of exceptional sets to consider when studying rational points on Fano varieties [81, Theorem 1.3].

CHAPTER 3

# Campana points

The notion of *Campana points*, first discussed by Campana [25], [26], and Abramovich [1], is receiving increasing attention in the field of Arithmetic geometry. Campana points can be viewed as rational points on a variety $X$ which are integral with respect to a weighted boundary divisor $D$, and thus provide a way to interpolate between integral and rational points. In this chapter we define Campana points, and discuss a Manin-type conjecture for the quantitative arithmetic of Campana points developed by Pieropan, Smeets, Tanimoto and Várilly-Alvarado [96, Conjecture 1.1]. In this thesis, we primarily work over $\mathbb{Q}$, but below we state the definitions for an arbitrary number field $K$.

**Definition 3.0.1.** Let $\mathscr{A}$ denote a finite set of indices. A *Campana orbifold* is a pair $(X, D)$, where $X$ is a smooth variety over $K$ and

$$D = \sum_{\alpha \in \mathscr{A}} \epsilon_\alpha D_\alpha$$

is an effective Weil $\mathbb{Q}$-divisor of $X$ over $K$ (where the $D_\alpha$ are prime divisors) such that

1. For all $\alpha \in \mathscr{A}$, either $\epsilon_\alpha = 1$ or $\epsilon_\alpha$ takes the form $1 - 1/m_\alpha$ for some integer $m_\alpha \geqslant 2$.

2. The support $D_{\mathrm{red}} := \sum_{\alpha \in \mathscr{A}} D_\alpha$ of $D$ has strict normal crossings on $X$. (This means that for any $1 \leqslant r \leqslant |\mathscr{A}|$, the intersection of any $r$ of the divisors $D_\alpha$ is either empty of smooth of codimension $r$ in $X$.)

We say that a Campana orbifold is *klt* if $\epsilon_\alpha \neq 1$ for all $\alpha \in \mathscr{A}$.

Let $(X, D)$ be a Campana orbifold. Campana points will be defined as points $P \in X(K)$ satisfying certain conditions. These conditions are dependent on a finite set $S$ of places of $K$, which contains all archimedean places, and a choice of *good integral model* of $(X, D)$ over $\mathscr{O}_{K,S}$. This model is defined to be a pair $(\mathscr{X}, \mathscr{D})$, where $\mathscr{X}$ is a flat, proper model of $X$ over $\mathscr{O}_{K,S}$, with $\mathscr{X}$ regular, and

$$\mathscr{D} = \sum_{\alpha \in \mathscr{A}} \epsilon_\alpha \mathscr{D}_\alpha,$$

where $\mathscr{D}_\alpha$ denotes the Zariski closure of $D_\alpha$ in $\mathscr{X}$.

**Definition 3.0.2.** Let $P \in (X \backslash D_{\mathrm{red}})(K)$. For a place $v \notin S$, let $\mathscr{P}_v$ denote the induced point in $\mathscr{X}(\mathscr{O}_v)$ obtained via the valuative criterion for properness, as stated in [59, Theorem II.4.7]. For $\alpha \in \mathscr{A}$, we define the *intersection multiplicity* $n_v(\mathscr{D}_\alpha, P)$ of $\mathscr{D}_\alpha$ and $P$ at $v$ to be the colength of the ideal $\mathscr{P}_v^* \mathscr{D}_\alpha$ in $\mathscr{O}_v$. The *intersection number* of $P$ and $\mathscr{D}$ at $v$ is defined to be

$$n_v(\mathscr{D}, P) = \sum_{\alpha \in \mathscr{A}} \epsilon_\alpha n_v(\mathscr{D}_\alpha, P).$$

**Definition 3.0.3.** Let $(X, D)$ be a Campana orbifold with a good integral model $(\mathscr{X}, \mathscr{D})$ over $\mathscr{O}_{K,S}$. A point $P \in (X \backslash D_{\mathrm{red}})(K)$ is a *Campana $\mathscr{O}_{K,S}$-point* of $(\mathscr{X}, \mathscr{D})$ if for all $v \notin S$ and all $\alpha \in \mathscr{A}$, we have

1. If $\epsilon_\alpha = 1$, then $n_v(\mathscr{D}_\alpha, P) = 0$.
2. If $\epsilon_\alpha \neq 1$, so that $\epsilon_\alpha = 1 - 1/m_\alpha$ for some integer $m_\alpha \geqslant 2$, then either $n_v(\mathscr{D}_\alpha, P) = 0$ or $n_v(\mathscr{D}_\alpha, P) \geqslant m_\alpha$.

We denote the set of Campana $\mathscr{O}_{K,S}$-points of $(\mathscr{X}, \mathscr{D})$ by $(\mathscr{X}, \mathscr{D})(\mathscr{O}_{K,S})$.

**Example 3.0.4.** In this example, we demonstrate how Campana points interpolate between integral and rational points. Let $K = \mathbb{Q}$ and $X = \mathbb{P}^1$, with coordinates $x_0, x_1$, and take the obvious model over $\mathbb{Z}$. We have $X(\mathbb{Q}) = X(\mathbb{Z})$. In fact, as discussed in the Introduction, rational and integral points coincide for any proper variety, by clearing denominators, or more formally, by the valuative criterion for properness [59, Theorem II.4.7]. However, when we consider rational and integral points on $X \backslash D$ for a boundary divisor $D$, the situation is very different. We suppose for convenience that $D$ is given by the point $[0 : 1]$. Again, by the valuative criterion for properness, we have $(X \backslash D)(\mathbb{Q}) = X(\mathbb{Q}) \backslash D(\mathbb{Q}) = X(\mathbb{Z}) \backslash D(\mathbb{Z})$, which we can identify with the set $\mathbb{A}^1(\mathbb{Q}) = \mathbb{Q}$ using the affine chart $x_0 \neq 0$. In contrast, $(\mathscr{X} \backslash \mathscr{D})(\mathbb{Z})$ is not equal to $X(\mathbb{Z}) \backslash D(\mathbb{Z})$. Indeed, in a morphism $\operatorname{Spec} \mathbb{Z} \to \mathscr{X} \backslash \mathscr{D}$, the image of every prime ideal $(p) \in \operatorname{Spec} \mathbb{Z}$ must not be contained in $\mathscr{D}$. In other words, we require $[x_0 : x_1] \notin \mathscr{D}(\mathbb{Z}/p\mathbb{Z})$ for every prime $p$, so $(\mathscr{X} \backslash \mathscr{D})(\mathbb{Z})$ corresponds to coprime integers $(x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}$ such that $x_0 \in \mathbb{Z}^\times = \{\pm 1\}$.

We now consider the weighted boundary divisor $(1-1/m)D$ for an integer $m \geqslant 2$. Suppose that $[x_0 : x_1]$ is a rational point of $\mathbb{P}^1$, with $(x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}$. For a prime $p$, the intersection multiplicity of $[x_0 : x_1]$ and $[0 : 1]$ at $p$ is $\nu_p(x_0)$, the $p$-adic valuation of $x_0$. Indeed, the pullback $\mathscr{P}_v^*(\mathscr{D})$ is the ideal in $\mathbb{Z}_p$ generated by $p^{\nu_p(x_0)}$, which has colength $\nu_p(x_0)$. Consequently, $[x_0 : x_1]$ is a Campana point in $(\mathscr{X}, \mathscr{D})(\mathbb{Z})$ if $\nu_p(x_0) = 0$ or $\nu_p(x_0) \geqslant m$ for all primes $p$. In other words, we require that $x_0$ is $m$-full.

The larger the integer $m$, the closer we get to the set of integral points $(\mathscr{X}\backslash\mathscr{D}_{\mathrm{red}})(\mathbb{Z})$. If we take the intersection over all $m \geqslant 2$, we recover the integral points, since $\pm 1$ are the only integers that are $m$-full for arbitrarily large $m$. The situation is summarised in the following diagram.

$$
\begin{aligned}
(X\backslash D)(\mathbb{Q}) = X(\mathbb{Q})\backslash D(\mathbb{Q}) =& \{x_1/x_0 : (x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}\} \\
& \cup| \\
(\mathscr{X}, (1-\tfrac{1}{2})\mathscr{D})(\mathbb{Z}) =& \{x_1/x_0 : (x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}, p \mid x_0 \implies p^2 \mid x_0\} \\
& \cup| \\
(\mathscr{X}, (1-\tfrac{1}{3})\mathscr{D})(\mathbb{Z}) =& \{x_1/x_0 : (x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}, p \mid x_0 \implies p^3 \mid x_0\} \\
& \cup| \\
& \vdots \\
& \cup| \\
\textstyle\bigcap_{m\in\mathbb{Z}_{\geqslant 2}}(\mathscr{X}, (1-\tfrac{1}{m})\mathscr{D})(\mathbb{Z}) =& \{x_1/x_0 : (x_0, x_1) \in \mathbb{Z}^2_{\mathrm{prim}}, x_0 = \pm 1\} \\
& \| \\
& (\mathscr{X}\backslash\mathscr{D})(\mathbb{Z}).
\end{aligned}
$$

**Example 3.0.5.** More generally, when $K = \mathbb{Q}$, Campana points are related to $m$-full values of polynomials. We consider projective space $X = \mathbb{P}^n$, and a strict normal crossings divisor

$$D = \sum_{i=0}^{k} \left(1 - \frac{1}{m_i}\right) D_i,$$

where $m_i \geqslant 2$ are integers, and $D_i$ are prime divisors on $X$ defined by irreducible polynomials $f_i$ with integral coefficients. Choosing the obvious good integral model $(\mathscr{X}, \mathscr{D})$, a rational point $z \in (X \setminus \bigcup_{i=0}^{k} D_i)(\mathbb{Q})$, represented by $(z_0, \ldots, z_n) \in \mathbb{Z}^{n+1}_{\mathrm{prim}}$, is a Campana $\mathbb{Z}$-point of $(\mathscr{X}, \mathscr{D})$ if and only if $f_i(z_0, \ldots, z_n)$ is $m_i$-full for all $i \in \{0, \ldots, k\}$.

**Definition 3.0.6.** We recall the notion of a thin subset of rational points from Definition 2.3.3. We define a *thin set of Campana $\mathscr{O}_{K,S}$-points* to be the intersection of a thin set of $X(K)$ with the set of Campana points $(\mathscr{X}, \mathscr{D})(\mathscr{O}_{K,S})$.

We conclude this section by introducing the Manin-type conjecture for Campana points as stated in [96, Conjecture 1.1]. Let $(X, D)$ be a Campana orbifold over $K$ with a good integral model $(\mathscr{X}, \mathscr{D})$ over $\mathscr{O}_{K,S}$. Let $(\mathscr{L}, \|\cdot\|)$ be an adelically metrized ample line bundle on $X$ with associated divisor class $[L]$. Let $H_{\mathscr{L}}\colon X(K) \to \mathbb{R}_{\geqslant 0}$ denote the corresponding height function, as defined in [91, Section 1]. We recall the definition of the cone of effective divisors $\Lambda_{\text{eff}}$ from (2.3.2).

**Definition 3.0.7.** Let $[K_X]$ denote the canonical divisor class. In analogy to (2.3.3), we define

$$a = \inf\{t \in \mathbb{R} : t[L] + [K_X] + [D] \in \Lambda_{\text{eff}}\},$$

and we define $b$ to be the codimension of the minimal supported face of $\Lambda_{\text{eff}}$ which contains $a[L] + [K_X] + [D]$.

**Conjecture 3.0.8** (Pieropan, Smeets, Tanimoto, Várilly-Alvarado)**.** *Suppose that $(X, D)$ is a klt Campana orbifold, with $-(K_X + D)$ ample (in this case we say that the orbifold is Fano). Assume that the set of Campana points $(\mathscr{X}, \mathscr{D})(\mathscr{O}_{K,S})$ is not itself thin. Then there is a thin set $\mathscr{T}$ of Campana $\mathscr{O}_{K,S}$-points such that*

$$\#\{P \in (\mathscr{X}, \mathscr{D})(\mathscr{O}_{K,S}) \backslash \mathscr{T} : H_{\mathscr{L}}(P) \leqslant B\} \sim c_{PSTV\text{-}A} B^a (\log B)^{b-1}$$

*as $B \to \infty$, where $a, b$ are as in Definition 3.0.7, and $c_{PSTV\text{-}A} > 0$ is an explicit constant described in Section 3.2 and [96, Section 3.3].*

Henceforth, we refer to Conjecture 3.0.8 as the *PSTV-A conjecture* for brevity.

**Remark 3.0.9.** The hypothesis that the Campana points themselves are not thin is discussed by Nakahara and Streeter in [90]. The authors establish in [90, Theorem 1.1] a connection between thin sets of Campana points and weak approximation, in the spirit of Serre's arguments in [105, Theorem 3.5.7]. Combining this with [90, Corollary 1.4], it can be shown that this hypothesis holds for the orbifolds we consider in Chapter 6 and 7.

## 3.1 Known results

The arithmetic study of Campana points is still in its early stages. Initial results in [22], [117] and [23], which predate the formulation of the PSTV-A conjecture, concern squareful and $m$-full values of hyperplanes of $\mathbb{P}^{n+1}$. Following discussions in the Spring 2006 MSRI program on rational and integral points on higher-dimensional varieties, Poonen [98] posed the problem of finding the number of coprime integers $z_0, z_1$ such that $z_0, z_1$ and $z_0 + z_1$ are all squareful

and bounded by $B$. In the language of the PSTV-A conjecture, this corresponds to counting Campana points on the orbifold $(\mathbb{P}^1, D)$, where $D$ is the divisor $\frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[\infty]$. Upper and lower bounds for this problem were obtained by Browning and Van Valckenborgh [22], but finding an asymptotic formula remains wide open. Van Valckenborgh [117] considers a higher-dimensional analogue of this problem by defining a Campana orbifold $(\mathbb{P}^n, D)$, where

$$D_i = \begin{cases} \{z_i = 0\}, & \text{if } 0 \leqslant i \leqslant n, \\ \{z_0 + \cdots + z_n = 0\}, & \text{if } i = n+1. \end{cases}$$

Let $H : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$ be the height function defined by

$$H(z) = \max(|z_0|, \ldots, |z_n|, |z_0 + \cdots + z_n|) \tag{3.1.1}$$

for a representative $(z_0, \ldots, z_n) \in \mathbb{Z}^{n+1}_{\text{prim}}$ of $z$. Then we have

$$\#\{P \in (\mathscr{X}, \mathscr{D})(\mathbb{Z}) : H(P) \leqslant B\} = \frac{1}{2}\#\mathscr{N}_{n+2}(B),$$

where $\mathscr{N}_{n+2}(B)$ is as defined in (1.2.2). Van Valckenborgh [117, Theorem 1.1] proves that for any $n \geqslant 3$, we have $\#\mathscr{N}_{n+2}(B) \sim cB^{n/2}$ as $B \to \infty$, for an explicit constant $c > 0$, and the main aim of Chapter 6 will be to handle the case $n = 2$. The work of Browning and Yamagishi [23] treats a more general orbifold $(\mathbb{P}^n, D)$, where the $D_i$ are as above, and $D = \sum_{i=0}^{n+1}(1 - \frac{1}{m_i})D_i$ for integers $m_0, \ldots, m_{n+1} \geqslant 2$. Their main result is an asymptotic formula for the number of Campana points on this orbifold (with the same height as in (3.1.1)), under the assumption that there exists some $j \in \{0, \ldots, n+1\}$ such that

$$\sum_{\substack{0 \leqslant i \leqslant n+1 \\ i \neq j}} \frac{1}{m_i(m_i+1)} \geqslant 1.$$

The general approach in all the aforementioned results is summarised in Section 4.5, and makes use of a unique representation of squareful numbers given in Lemma 3.3.1 (or a generalisation of it to $m$-full numbers) in order to parameterise the problem as a sum of counting problems over a family of projective varieties.

Following the formulation of the PSTV-A conjecture, several further cases have been treated. In the same paper that the PSTV-A conjecture is introduced, the authors establish their conjecture for vector group compactifications [96, Theorem 1.2]. This formed an ideal testing ground for the PSTV-A conjecture, since both integral and rational points on vector group compactifications had previously been studied by Chambert-Loir and Tschinkel using the height zeta function method [28], [29]. Pieropan and Schindler [95] establish the PSTV-A conjecture for complete smooth split toric varieties satisfying an additional technical assumption, by developing a very general version of the hyperbola

method. Xiao [119] treats the case of biequivariant compactifications of the Heisenberg group over $\mathbb{Q}$, using the height zeta function method. Finally, Streeter [115] studies $m$-full values of norm forms by counting Campana points on the orbifold $(\mathbb{P}^{d-1}_K, (1-\frac{1}{m})V(\mathbf{N}_{E/K}))$, where $K$ is a number field, $V(\mathbf{N}_{E/K})$ is the divisor cut out by a norm form associated to a degree-$d$ Galois extension $E/K$, and $m \geqslant 2$ is an integer which is coprime to $d$ if $d$ is not prime.

In [96], [95] and [119], the leading constants for the counting problems considered were reconciled with the prediction from the PSTV-A conjecture. In the case of Campana points for norm forms, Streeter [115, Section 7.3] provides an example where the leading constant in [115, Theorem 1.4] differs from the constant defined in the PSTV-A conjecture. It remains unclear whether this could be explained by the removal of a thin set. For the papers [22], [117] and [23], however, no subsequent attempts to compare the leading constants have been made. In Chapter 7, we make a detailed study of the leading constant for $\#\mathscr{N}_3(B)$ in the context of Conjecture 3.0.8.

## 3.2 The leading constant $c_{\text{PSTV-A}}$

We now turn our attention to the definition of the leading constant $c_{\text{PSTV-A}}$. For a description of $c_{\text{PSTV-A}}$ in full generality, we refer the reader to [96, Section 3.3]. Here, for simplicity, we define $c_{\text{PSTV-A}}$ in the case when $X$ is a smooth projective variety over $\mathbb{Q}$ satisfying $a[L]+[K_X]+[D]=0$ (this latter hypothesis in particular holds when $\mathrm{Pic}(X) \cong \mathbb{Z}$, see Example 2.3.1). The constant $c_{\text{PSTV-A}}$ is given by the formula

$$c_{\text{PSTV-A}} = \frac{\alpha\beta\tau}{a(b-1)!}, \tag{3.2.1}$$

and we proceed to discuss each of the factors $\alpha, \beta, \tau$ in turn.

Let $\varrho$ denote the Picard number of $X$, i.e., the rank of $\mathrm{Pic}(X)$. The *dual effective cone* $\Lambda^*_{\text{eff}}$ is defined as

$$\Lambda^*_{\text{eff}} = \{y \in (\mathrm{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{R})^* : \langle y, r\rangle \geqslant 0 \text{ for all } r \in \Lambda_{\text{eff}}\}.$$

Here $(\mathrm{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{R})^* \cong (\mathbb{R}^\varrho)^* = \mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^\varrho, \mathbb{R})$ is the usual vector space dual, and $\langle \cdot, \cdot \rangle$ is the tautological pairing defined by $\langle y, r\rangle = y(r)$.

The definition of $\alpha$ from [96, Section 3.3] is closely related to the $\alpha$-constant from the classical Manin conjecture. In general, the definition involves a rigid effective divisor $E$ which is $\mathbb{Q}$-linearly equivalent to $aL + K_X + D$. However, if $(X, D)$ is any Campana orbifold with $E = 0$ and we write $D = \sum_{i=0}^k \epsilon_i D_i$ for prime divisors $D_i$, then the definition of $\alpha$ simplifies to

$$\alpha = \prod_{i=0}^{k}(1-\epsilon_i) \int_{\Lambda^*_{\text{eff}}} e^{-\langle [L], x\rangle} \mathrm{d}x. \tag{3.2.2}$$

When $a[L] + [K_X] + [D] = 0$, the constant $\beta$ from [96, Section 3.3] agrees with the definition of $\beta$ in Manin's conjecture. We have $\beta = 1$ whenever $\mathrm{Pic}(X_{\overline{\mathbb{Q}}}) \cong \mathbb{Z}$ [72, Definition 5.12, Remark 5.13]. In this work, we shall only consider examples where $\mathrm{Pic}(X_{\overline{\mathbb{Q}}}) \cong \mathbb{Z}$, and so the $\beta$-constant will not play a role.

We now describe the Tamagawa number $\tau$. Again, we do not give the definition in full generality, but assume for simplicity that $a[L] + [K_X] + [D] = 0$. It follows from [96, Section 3.3] that

$$\tau = \int_{\mathscr{U}(\mathbb{A}_{\mathbb{Q}})} H_D(x)\, \mathrm{d}\tau_X. \tag{3.2.3}$$

We explain the notation used in this equation. In [96, Section 3.3], two alternative definitions of $\mathscr{U}(\mathbb{A}_{\mathbb{Q}})$ are given. The first is as a topological closure of the Campana points $(\mathscr{X}, \mathscr{D})(\mathscr{O}_{K,S})$ in the adelic points $X(\mathbb{A}_{\mathbb{Q}})$, and the second is in terms of the Brauer–Manin pairing. In general, it is not known whether the two definitions coincide, but in all examples we consider in this thesis, the definitions do agree since there will be no Brauer–Manin obstruction. The notation $H_D$ represents a height function associated to $D$, defined as follows. We write $D = \sum_{i=0}^{k} \epsilon_i D_i$ for prime divisors $D_i$. We fix an adelic metrization on the line bundles $\mathscr{O}_X(D_i)$ associated to each of the divisors $D_i$. This induces a height $H_{D_i}$ as described in [91, Définition 1.2]. We then define

$$H_D = \prod_{i=1}^{k} H_{D_i}^{\epsilon_i}. \tag{3.2.4}$$

Finally, the measure $\tau_X$ is defined to be the usual Tamagawa measure appearing in Manin's conjecture, as defined in [91, Section 2].

## 3.3 A basic example

We now study in detail a particular example of Conjecture 3.0.8. Let $X = \mathbb{P}^n$, with coordinates $z_0, \dots, z_n$, and let $D$ be the divisor $D = \sum_{i=0}^{n} \{z_i = 0\}$. We choose the usual height on $\mathbb{P}^n(\mathbb{Q})$, as given in (1.2.1). We take the obvious smooth proper model over $\mathbb{Z}$. The resulting counting problem is

$$N(B) = \frac{1}{2} \# \left\{ (z_0, \dots, z_n) \in (\mathbb{Z}_{\neq 0})^{n+1}_{\mathrm{prim}} : |z_i| \leqslant B, z_i \text{ squareful for all } i \right\}. \tag{3.3.1}$$

An asymptotic formula for $N(B)$ is known thanks to the much more general work of Pieropan and Schindler, in which the authors develop a version of the hyperbola method in order to establish the PSTV-A conjecture for certain split toric varieties [95]. However, in this section, we give a self-contained proof of an asymptotic formula for $N(B)$ and demonstrate the consistency with the

PSTV-A conjecture. We begin with some basic facts about $m$-full numbers which we shall also use in Chapters 6 and 7.

**Lemma 3.3.1.** *Every nonzero squareful integer $z$ can be written uniquely in the form $z = x^2y^3$, for a positive integer $x$ and a squarefree integer $y$.*

*Proof.* Clearly, the sign of $y$ is uniquely determined by the sign of $z$. For a prime $p$, let $\nu_p(x) = r_p, \nu_p(y) = s_p$ and $\nu_p(z) = t_p$. Then the equation $z = y^3x^2$ is equivalent to the equations $t_p = 2r_p + 3s_p$ for all primes $p$. The property that $z$ is squareful is equivalent to $t_p = 0$ or $t_p \geqslant 2$ for all primes $p$, and the property that $y$ is squarefree is equivalent to $s_p \in \{0, 1\}$ for all primes $p$. The result now follows from the fact that for a fixed integer $t_p = 0$ or $t_p \geqslant 2$, there is a unique solution to the equation $t_p = 2r_p + 3s_p$ with $s_p \in \{0, 1\}$ and $r_p \in \mathbb{Z}_{\geqslant 0}$. □

**Lemma 3.3.2.** *Let $F(B)$ denote the number of squareful positive integers bounded by $B$. Then $F(B) = cB^{1/2} + O(B^{1/3})$, where*

$$c = \prod_p (1 + p^{-3/2}) = \frac{\zeta(3/2)}{\zeta(3)}. \tag{3.3.2}$$

*Proof.* Suppose that $z$ is a positive squareful integer bounded by $B$. Using Lemma 3.3.1, we write $z = x^2y^3$ for positive integers $x, y$ with $y$ squarefree. We obtain

$$F(B) = \sum_{y \leqslant B^{1/3}} \mu^2(y) \sum_{x \leqslant (B/y^3)^{1/2}} 1 = \sum_{y \leqslant B^{1/3}} \mu^2(y) \left( \frac{B^{1/2}}{y^{3/2}} + O(1) \right).$$

The error term in the above expression is $O(B^{1/3})$. We may also extend the summation over $y$ to an infinite sum with an error term $O(B^{1/3})$. We conclude that $F(B) = cB^{1/2} + O(B^{1/3})$, where

$$c = \sum_{y=1}^{\infty} \frac{\mu^2(y)}{y^{3/2}}.$$

The summand is multiplicative in $y$, and can be expressed as the Euler product in (3.3.2). □

**Remark 3.3.3.** With a more refined analysis, it is possible to find a secondary main term for $F(B)$. Bateman and Grosswald prove in [3, Theorem 3] that

$$F(B) = \frac{\zeta(3/2)}{\zeta(3)} B^{1/2} + \frac{\zeta(2/3)}{\zeta(2)} B^{1/3} + O_A(B^{1/6} (\log B)^{-A})$$

for any $A \geqslant 1$. They remark that an improvement of the error term to $O(B^\theta)$ for some $\theta < 1/6$ would imply the quasi-Riemann hypothesis that there

exists a $\delta > 0$ such that $\zeta(s) \neq 0$ whenever $Re(s) > 1 - \delta$. Assuming the Riemann hypothesis, the exponent $\theta$ has undergone a series of improvements, which are summarised in [118, Table 1]. The current record, due to Wang, is $\theta = 328/2333 + \epsilon$ for any $\epsilon > 0$ [118, Theorem 1].

A similar parameterisation to Lemma 3.3.1 can be found for $m$-full numbers for any $m \geqslant 2$. Using this, we obtain the following generalisation of Lemma 3.3.2, first proved by Erdös and Szekeres [47].

**Lemma 3.3.4.** *For an integer $m \geqslant 2$, let $F_m(B)$ denote the number of $m$-full positive integers bounded by $B$. Then $F_m(B) = C_m B^{1/m} + O(B^{1/(m+1)})$, where*

$$C_m = \prod_p \left(1 + \sum_{j=m+1}^{2m-1} p^{-j/m}\right). \tag{3.3.3}$$

### 3.3.1 The asymptotic formula

We proceed to find an asymptotic formula for the quantity $N(B)$ from (3.3.1). Below, all implied constants are allowed to depend on a small parameter $\epsilon > 0$, which for convenience we allow to take different values at different points in the argument.

By Möbius inversion, we have

$$N(B) = 2^n \sum_{d \leqslant B^{1/2}} \mu(d)(N_d(B))^{n+1}, \tag{3.3.4}$$

where

$$N_d(B) = \#\{z \in \mathbb{N} : z \leqslant B, z \text{ squareful}, d \mid z\}. \tag{3.3.5}$$

The factor $2^n$ in (3.3.4) comprises of a factor $2^{n+1}$ coming from counting over $\mathbb{N}$ rather than $\mathbb{Z}$ in (3.3.5), and the factor $1/2$ in the definition of $N(B)$ from (3.3.1). We can write $z$ uniquely in the form $z = y^3x^2$ for positive integers $x, y$ with $y$ squarefree using Lemma 3.3.1. Define $d_2 = \gcd(y, d), d_1 = d/d_2, y' = y/d_2$, and $x' = x/d_1$. Then

$$\begin{aligned} N_d(B) &= \sum_{d_2 \mid d} \sum_{\substack{y \leqslant B^{1/3} \\ \gcd(y,d)=d_2}} \mu^2(y) \sum_{\substack{x \leqslant \left(B/y^3\right)^{1/2} \\ d_1 \mid x}} 1 \\ &= \sum_{d_2 \mid d} \sum_{\substack{y' \leqslant B^{1/3}/d_2 \\ \gcd(y',d)=1}} \mu^2(y'd_2) \left(\left(\frac{B}{y'^3 d_2^3 d_1^2}\right)^{1/2} + O(1)\right). \end{aligned}$$

Note that $\gcd(y', d) = 1$ may be replaced by $\gcd(y', d_1) = 1$ in the last line above, because the factor $\mu^2(y'd_2)$ takes care of the condition $\gcd(y', d_2) = 1$.

We deal with the coprimality condition $\gcd(y', d_1) = 1$ by a further application of Möbius inversion. Below, we make the substitution $y'' = y'/e$. We obtain

$$N_d(B) = \sum_{d_2|d} \sum_{e|d_1} \mu(e) \sum_{y'' \leqslant B^{1/3}/d_2 e} \mu^2(y'' d_2 e) \left( \left( \frac{B}{y''^3 e^3 d_2^3 d_1^2} \right)^{1/2} + O(1) \right). \tag{3.3.6}$$

The error term coming from the $O(1)$ factor in (3.3.6) can be bounded by

$$\sum_{d_2|d} \sum_{e|d_1} \sum_{y'' \leqslant B^{1/3}/d_2 e} O(1) \ll B^{1/3} \sum_{d_2|d} \sum_{e|d_1} 1 \ll B^{1/3+\epsilon},$$

where we have applied the trivial estimate for the divisor function to the sums over $d_2$ and $e$ [56, Section 18.1]. Similarly, we may extend the $y''$-sum in (3.3.6) to an infinite sum with an error term bounded by

$$B^{1/2} \sum_{d_2|d} \frac{1}{d_2^{3/2}} \sum_{e|d_1} \frac{1}{e^{3/2}} \sum_{y'' > B^{1/3}/d_2 e} \frac{1}{(y'')^{3/2}} \ll B^{1/3} \sum_{d_2|d} \frac{1}{d_2} \sum_{e|d_1} \frac{1}{e} \ll B^{1/3+\epsilon}.$$

Changing notation from $y''$ back to $y$, we conclude that

$$N_d(B) = \left( \frac{B^{1/2}}{d} \sum_{d_2|d} \frac{1}{d_2^{1/2}} \sum_{e|d_1} \frac{\mu(e)}{e^{3/2}} \sum_{y=1}^{\infty} \frac{\mu^2(y d_2 e)}{y^{3/2}} \right) + O(B^{1/3+\epsilon}). \tag{3.3.7}$$

We shall use (3.3.7) when $d \leqslant B^\delta$, for some $\delta > 0$ to be determined later. For larger values of $d$, we require a separate estimate. Below, we allow $\epsilon$ to depend on $\delta$.

**Lemma 3.3.5.** *Suppose that $d \geqslant B^\delta$. Then*

$$N_d(B) \ll \frac{B^{1/2}}{d^{1-\epsilon}}.$$

*Proof.* Every squareful number $1 \leqslant z \leqslant B$ with $d \mid z$ can be written in the form $z = uv$, where $u, v$ are squareful, $\gcd(v, d) = 1$, and $uv \leqslant B$. (Explicitly, we take $u = \prod_{p|d} p^{\nu_p(z)}$.) All primes dividing $u$ also divide $d$; we write this condition as $u \mid d^\infty$. We claim that the number of choices for $u$ is

$$\#\{u \leqslant B : u \mid d^\infty\} \ll (Bd)^\epsilon. \tag{3.3.8}$$

To see this, we fix $\epsilon > 0$ and note that

$$\#\{u \leqslant B : u \mid d^\infty\} \leqslant B^\epsilon \sum_{\substack{u \leqslant B \\ p|u \implies p|d}} u^{-\epsilon} \leqslant B^\epsilon \prod_{p|d} \left( \frac{1}{1 - p^{-\epsilon}} \right) \leqslant B^\epsilon \prod_{p|d} C_\epsilon,$$

where $C_\epsilon = (1-2^{-\epsilon})^{-1}$. Using the fact that the number of prime divisors $p \mid d$ is $O(\log d/\log\log d)$, which is a consequence of the divisor bound in [56, Section 18.1], we obtain

$$\#\{u \leqslant B : u \mid d^\infty\} \ll B^\epsilon C_\epsilon^{O(\log d/\log\log d)} \ll B^\epsilon d^{O(C_\epsilon/\log\log d)}.$$

For $d$ sufficiently large, the exponent $O(C_\epsilon/\log\log d)$ is less than $\epsilon$. Therefore, we obtain the bound $O(B^\epsilon d^\epsilon)$ claimed in (3.3.8).

Since $u$ is squareful and $d$ is squarefree, we have $d^2 \mid u$, and so $v \leqslant B/d^2$. By Lemma 3.3.2, the number of choices for $v$ is therefore $O(B^{1/2}/d)$. Overall, we have $O(B^{1/2+\epsilon}/d^{1-\epsilon})$ choices for $u, v$, and since $d \geqslant B^\delta$, we may remove the $B^\epsilon$ factor by redefining $\epsilon$. □

Combining (3.3.4) with (3.3.7) and Lemma 3.3.5, we obtain

$$\begin{aligned} N(B) &= B^{(n+1)/2} \sum_{d<B^\delta} (c_d + O(B^{-1/6+\epsilon})) + O\left(B^{(n+1)/2} \sum_{d\geqslant B^\delta} d^{-(n+1)+\epsilon}\right) \\ &= B^{(n+1)/2}\left(\sum_{d<B^\delta} c_d + O(B^{\delta-1/6+\epsilon}) + O(B^{-n\delta+\epsilon})\right), \end{aligned} \tag{3.3.9}$$

where

$$c_d = 2^n \frac{\mu(d)}{d^{n+1}} \left(\sum_{d_2\mid d} \frac{1}{d_2^{1/2}} \sum_{e\mid d_1} \frac{\mu(e)}{e^{3/2}} \sum_{y=1}^{\infty} \frac{\mu^2(yd_2e)}{y^{3/2}}\right)^{n+1}. \tag{3.3.10}$$

By applying once more the trivial bound for the divisor function to the sum over $d_2$, and $e$, we see that $c_d = O(d^{-n-1+\epsilon})$. Therefore, the sum in (3.3.9) can be extended to an infinite sum over $d$, with an error term $O(B^{-n\delta+\epsilon})$ which can be absorbed into the error term already present in (3.3.9). Choosing $\delta = \frac{1}{6(n+1)}$, we conclude that

$$N(B) = cB^{(n+1)/2} + O\left(B^{\frac{n+1}{2}-\frac{n}{6(n+1)}}\right), \tag{3.3.11}$$

where $c = \sum_{d=1}^{\infty} c_d$.

We now realise $c$ as an Euler product. The inner summand of (3.3.10) is a multiplicative function of $y$, and we recall that $\gcd(d_2, e) = 1$. Therefore,

$$\begin{aligned} \sum_{y=1}^{\infty} \frac{\mu^2(yd_2e)}{y^{3/2}} &= \prod_{p\nmid d_2e} \left(1+p^{-3/2}\right) \\ &= \prod_{p\mid d_2} (1+p^{-3/2})^{-1} \prod_{p\mid e} (1+p^{-3/2})^{-1} \prod_{p} (1+p^{-3/2}). \end{aligned}$$

Hence

$$\begin{aligned}
&\prod_p (1+p^{-3/2})^{-1} \sum_{d_2|d} \frac{1}{d_2^{1/2}} \sum_{e|d_1} \frac{\mu(e)}{e^{3/2}} \sum_{y=1}^{\infty} \frac{\mu^2(yd_2e)}{y^{3/2}} \\
&= \sum_{d_2|d} d_2^{-1/2} \left( \prod_{p|d_2} (1+p^{-3/2})^{-1} \sum_{e|d_1} \left( \frac{\mu(e)}{e^{3/2}} \prod_{p|e} (1+p^{-3/2})^{-1} \right) \right) \\
&= \sum_{d_2|d} d_2^{-1/2} \left( \prod_{p|d_2} (1+p^{-3/2})^{-1} \prod_{p|d_1} \left(1 - p^{-3/2}(1+p^{-3/2})^{-1}\right) \right) \\
&= \prod_{p|d} (1+p^{-3/2})^{-1} \sum_{d_2|d} d_2^{-1/2}.
\end{aligned}$$

Substituting this into (3.3.10), we conclude that

$$\begin{aligned}
c &= 2^n \prod_p (1+p^{-3/2})^{n+1} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^{n+1}} \left( \prod_{p|d} (1+p^{-3/2}) \sum_{d_2|d} d_2^{-1/2} \right)^{n+1} \\
&= 2^n \prod_p (1+p^{-3/2})^{n+1} \sum_{d=1}^{\infty} \frac{\mu(d)}{d^{n+1}} \left( \prod_{p|d} \frac{1}{1-p^{-1/2}+p^{-1}} \right)^{n+1} \\
&= 2^n \prod_p (1+p^{-3/2})^{n+1} \left( 1 - \frac{1}{(1-p^{1/2}+p)^{n+1}} \right). \qquad (3.3.12)
\end{aligned}$$

### 3.3.2 Consistency with the PSTV-A conjecture

We conclude this section by proving that the asymptotic formula from (3.3.11) and the Euler product for the leading constant from (3.3.12) agree with the asymptotic predicted by the PSTV-A conjecture, without the removal of any thin sets being required.

We recall the divisor is $D = \sum_{i=0}^{n} \frac{1}{2}\{z_i = 0\}$, which has degree $(n+1)/2$. We have $\mathrm{Pic}(\mathbb{P}^n) \cong \mathbb{Z}$, with the isomorphism given by $n \mapsto n[H]$ where $[H]$ denotes the hyperplane class. Under this isomorphism, the cone of effective divisors is $\Lambda_{\mathrm{eff}} = \mathbb{R}_{\geqslant 0}$. The canonical line bundle is $\omega_{\mathbb{P}^n} \cong \mathscr{O}_{\mathbb{P}^n}(-n-1)$, so the canonical divisor is $[K_X] = -(n+1)[H]$. The line bundle used to define the height (1.2.1) is $\mathscr{L} = \mathscr{O}_{\mathbb{P}^n}(1)$, and so corresponds to the divisor $L = [H]$.

We now work out the constants $a$ and $b$ which are the exponents of $B$ and $\log B$ in the PSTV-A conjecture. We have

$$\begin{aligned}
a &= \inf\{t \in \mathbb{R} : t[L] + [K_X] + [D] \in \Lambda_{\mathrm{eff}}\} \\
&= \inf\left\{ t \in \mathbb{R} : t - (n+1) + \frac{n+1}{2} \geqslant 0 \right\} \\
&= \frac{n+1}{2}.
\end{aligned}$$

The minimal supported face of $\Lambda_{\text{eff}}$ which contains $a[L] + [K_X] + [D] = 0$ is $\{0\}$, which has codimension $1$ in $\Lambda_{\text{eff}}$, and so $b = 1$. Therefore, the powers of $B$ and $\log B$ in (3.3.11) agree with the PSTV-A conjecture. Substituting into (3.2.1), we obtain

$$c_{\text{PSTV-A}} = \frac{\alpha\beta\tau}{ab!} = \frac{2\alpha\beta\tau}{n+1}. \tag{3.3.13}$$

From (3.2.2), we have

$$\alpha = \prod_{i=0}^{n}\left(1-\frac{1}{2}\right)\int_{\Lambda_{\text{eff}}^*} e^{-\langle [L],x\rangle}\,\mathrm{d}x = \frac{1}{2^n}\int_{\mathbb{R}_{\geqslant 0}} e^{-x}\,\mathrm{d}x = \frac{1}{2^n}.$$

As remarked in Section 3.2, since $\mathrm{Pic}(\mathbb{P}^n) \cong \mathbb{Z}$, we have $\beta = 1$. Therefore,

$$c_{\text{PSTV-A}} = \frac{\tau}{2^n(n+1)}. \tag{3.3.14}$$

It remains to compute the Tamagawa number $\tau$, for which we need to compute $H_D$ from (3.2.4). Each component $D_i = \{z_i = 0\}$ of $D$ gives rise to the height $H_{D_i}(z) = \max_{0\leqslant i\leqslant n}|z_i|$ for $(z_0,\dots,z_n) \in (\mathbb{Z}_{\neq 0})^{n+1}_{\text{prim}}$ representing $z$. In view of (3.2.4), this means that

$$H_D(z) = \max_{0\leqslant i\leqslant n}|z_i|^{(n+1)/2}.$$

As a product of local heights over places $v$ of $\mathbb{Q}$, we have $H_D = \prod_v H_{D,v}$, where $H_{D,v} : \mathbb{P}^n(\mathbb{Q}_p) \to \mathbb{R}_{\geqslant 0}$ sends $z$ to $\max_{0\leqslant i\leqslant n}|z_i|_p^{(n+1)/2}$ for a representative $(z_0,\dots,z_n)$ of $z$. We note that $2D$ has degree $n+1$ so corresponds to the line bundle $\mathscr{O}_{\mathbb{P}^n}(n+1)$. Hence there is a rational section $s$ on the line bundle $\mathscr{L}$ associated to $D$ defined by $s(\mathbf{x}) = (\prod_{i=0}^{n+1} x_i)^{1/2}$.

We can now write $\tau$ as a product $\tau_\infty \prod_p \tau_p$. Below, we use the notation $(\mathbb{Z}_p^{n+1})_{\text{prim}}$ to denote $p$-adic integers $x_0,\dots,x_n$ such that $\nu_p(x_i) = 0$ for some $i \in \{0,\dots,n\}$, and $d_{x_i,p}$ to denote the usual $p$-adic measure of the variable $x_i$. We have

$$\tau_p = \int_{\substack{(x_0\dots,x_n)\in(\mathbb{Z}_p^{n+1})_{\text{prim}}\\ \nu_p(x_i)\neq 1 \text{ for all } i}} \prod_{i=0}^{n}|x_i|^{-1/2}\cdot\frac{d_{x_0,p}\cdots d_{x_n,p}}{\max_{0\leqslant i\leqslant n}(|x_i|_p^{n+1})}.$$

If $(x_0,\dots,x_n) \in (\mathbb{Z}_p^{n+1})_{\text{prim}}$ then $\nu_p(x_i) = 0$ for some $i$, and so the integrand is $\prod_{i=0}^n |x_i|^{-1/2}$. We have $\tau_p = I_1 - I_2$, where

$$I_1 = \int_{\substack{(x_0\dots,x_n)\in\mathbb{Z}_p^{n+1}\\ \nu_p(x_i)\neq 1 \text{ for all } i}} \prod_{i=0}^{n}|x_i|^{-1/2}\cdot d_{x_0,p}\cdots d_{x_n,p},$$

$$I_2 = \int_{\substack{(x_0\dots,x_n)\in\mathbb{Z}_p^{n+1}\\ \nu_p(x_i)\geqslant 2 \text{ for all } i}} \prod_{i=0}^{n}|x_i|^{-1/2}\cdot d_{x_0,p}\cdots d_{x_n,p}.$$

To compute $I_2$, we change variables from $x_i$ to $p^{-2}x_i$ to obtain

$$I_2 = p^{-(n+1)} \prod_{i=0}^{n+1} \int_{x_i \in \mathbb{Z}_p} |x_i|_p^{-1/2} d_{x_i,p}.$$

The measure of the set $\nu_p(x_i) = j$ with respect to $d_{x_i,p}$ is $(1-p^{-1})p^{-j}$, and so

$$\begin{aligned} I_2 &= p^{-(n+1)} \left( \sum_{j=0}^{\infty} (1-p^{-1}) p^{-j/2} \right)^{n+1} \\ &= p^{-(n+1)} \left( \frac{1-p^{-1}}{1-p^{-1/2}} \right)^{n+1}. \end{aligned}$$

A similar computation yields

$$\begin{aligned} I_1 &= \prod_{i=0}^{n+1} \int_{\substack{x_i \in \mathbb{Z}_p \\ \nu_p(x_i) \neq 1}} |x_i|_p^{-1/2} d_{x_i,p} \\ &= \left( \sum_{\substack{j=0 \\ j \neq 1}}^{\infty} (1-p^{-1}) p^{-j/2} \right)^{n+1} \\ &= (1-p^{-1})^{n+1} \left( \frac{1}{1-p^{-1/2}} - p^{-1/2} \right)^{n+1}. \end{aligned}$$

Therefore,

$$\begin{aligned} \tau_p &= (1-p^{-1})^{n+1} \left( \frac{1}{1-p^{-1/2}} - p^{-1/2} \right)^{n+1} - p^{-(n+1)} \left( \frac{1-p^{-1}}{1-p^{-1/2}} \right)^{n+1} \\ &= (1+p^{-3/2})^{n+1} \left( 1 - \left( \frac{p^{-1}(1+p^{-1/2})}{1+p^{-3/2}} \right)^{n+1} \right) \\ &= (1+p^{-3/2})^{n+1} (1-(1-p^{1/2}+p)^{-n+1}), \end{aligned}$$

which agrees with the Euler factor computed in (3.3.12).

Finally, we compute $\tau_\infty$. We can consider the affine charts $U_i = \{x \in \mathbb{P}^n(\mathbb{R}) : |x_i| = \max_{j=0,\dots,n} |x_j|\}$ where $i$ runs from $0$ to $n$. These charts cover $\mathbb{P}^n(\mathbb{R})$, and their intersections have measure zero. Using the maps $f_i : [x_0 : \cdots : x_{i-1} : 1 : x_{i+1} : \cdots x_n] \mapsto (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$, the measure on $U_i$ is given by

$$\frac{\prod_{j\neq i} dx_j}{\max_{j\neq i}(1,|x_j|)} = \prod_{j\neq i} dx_j,$$

where $dx_j$ denotes the usual Lebesgue measure. Therefore

$$\begin{aligned}\tau_\infty &= \sum_{i=0}^{n} \int_{\substack{(x_0,\ldots,\widehat{x_i},\ldots,x_n)\in\mathbb{R}^n \\ |x_j|\leqslant 1 \text{ for all } j}} \prod_{\substack{j=0,\ldots,n \\ j\neq i}} |x_j|^{-1/2} dx_j \\ &= (n+1)\left(\int_{|x|\leqslant 1} |x|^{-1/2} dx\right)^n \\ &= (n+1)4^n.\end{aligned}$$

Combining with (3.3.14), we conclude that $c_{\text{PSTV-A}} = c$.

CHAPTER 4

# The circle method

In this section, we introduce the circle method in its classical form, and discuss various refinements, including the delta method of Duke, Friedlander and Iwaniec [46], which was further developed by Heath-Brown [61]. This latter version is particularly well suited to counting points on quadratic forms, and we shall apply it in this context in Chapter 6. The expository material in this chapter is based on [11] and [12]. Let

$$\delta(n) = \begin{cases} 1, & \text{if } n = 0, \\ 0, & \text{if } n \in \mathbb{Z}_{\neq 0}. \end{cases} \tag{4.0.1}$$

The genesis of the Hardy–Littlewood circle method lies in the simple observation that for any integer $n$,

$$\int_0^1 e(\alpha n) \mathrm{d}\alpha = \delta(n). \tag{4.0.2}$$

Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree $d$. Let $\mathbf{x} = (x_1, \ldots, x_n)$, and define $|\mathbf{x}| = \max_{1 \leqslant i \leqslant n} |x_i|$. We consider the counting function

$$N(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : F(\mathbf{x}) = 0, |\mathbf{x}| \leqslant B\}. \tag{4.0.3}$$

In order to compare $N(B)$ with Manin's conjecture for the corresponding projective hypersurface $X \subseteq \mathbb{P}^{n-1}$ and the naive height (1.2.1), we must reinsert the coprimality condition $\gcd(x_1, \ldots, x_n) = 1$ into (4.0.3). This is a straightforward application of Möbius inversion provided we can prove an asymptotic formula for $N(B)$ whose exponent in $B$ is larger than $1$. In this case, the coprimality condition will only affect $N(B)$ by a constant factor.

Using (4.0.2), we have

$$N(B) = \int_0^1 S(\alpha) \mathrm{d}\alpha, \tag{4.0.4}$$

where

$$S(\alpha) = \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n \\ |\mathbf{x}|\leqslant B}} e(\alpha F(\mathbf{x})). \tag{4.0.5}$$

Heuristically, for "typical" choices of $\alpha \in (0,1)$ and for large values of $B$, we would expect the quantities $e(F(\mathbf{x}))$ to be distributed uniformly at random on the unit circle $\{z \in \mathbb{C} : |z| = 1\}$ as $\mathbf{x} \in \mathbb{Z}^n$ ranges over vectors with $|\mathbf{x}| \leqslant B$. If this were true, then the central limit theorem would suggest that $S(\alpha)$ has size approximately $B^{n/2}$. (This is the idea underpinning *square-root cancellation*, which is a commonly used heuristic in Analytic number theory.) However, this heuristic breaks down if $\alpha$ is very close to a rational number with a small denominator. In this case, the values of $e(\alpha F(\mathbf{x}))$ are concentrated near a small number of points on the unit circle, and less cancellation occurs in the sum $S(\alpha)$.

In view of the above discussion, it is natural to consider the decomposition

$$N(B) = \int_{\mathfrak{M}} S(\alpha)\mathrm{d}\alpha + \int_{\mathfrak{m}} S(\alpha)\mathrm{d}\alpha,$$

where $\mathfrak{M}$ consists of those $\alpha \in (0,1)$ which are suitably close to a rational number with small denominator, and $\mathfrak{m} = (0,1)\backslash\mathfrak{M}$. We refer to $\mathfrak{M}$ as the *major arcs* and $\mathfrak{m}$ as the *minor arcs*. We recall from Chapter 2 that we expect the exponent of $B$ in the asymptotic formula for $N(B)$ to be $n-d$. Therefore, according to the principle of square-root cancellation, if $n/2 < n-d$ (i.e., $n > 2d$), then we might hope that $\int_{\mathfrak{m}} |S(\alpha)|\mathrm{d}\alpha$ makes a negligible contribution to $N(B)$. However, this is very difficult to establish rigorously, and we are usually forced to make much stronger assumptions on the size of $n$ than this. We discuss further the treatment of the minor arcs in Section 4.2.

In the groundbreaking work "forms in many variables" from 1962, Birch used the circle method to establish the following very general result.

**Theorem 4.0.1** ([7]). *Let $F_1, \dots, F_R \in \mathbb{Z}[x_1, \dots, x_n]$ be homogeneous forms of degree $d \geqslant 2$. Let*

$$N(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| \leqslant B, F_1(\mathbf{x}) = \cdots = F_R(\mathbf{x}) = 0\}.$$

*Let $\sigma$ denote the dimension of the variety in $\mathbb{P}^{n-1}$ defined by the condition that the Jacobian $\left(\frac{\partial F_i(\mathbf{x})}{\partial x_j}\right)_{ij}$ has rank $< R$, with the convention $\dim\emptyset = -1$. Suppose that*

$$n - 1 - \sigma > (d-1)2^{d-1}R(R+1). \tag{4.0.6}$$

*Then there is a constant $c$ such that*

$$N(B) \sim cB^{n-dR}.$$

The constant $c$ comes out of the treatment of the major arcs, and can be written as a product of a *singular integral* and a *singular series*, which we discuss further in Section 4.1. In fact, this constant is consistent with Peyre's prediction for the leading constant in Manin's conjecture [92, Formule empirique 5.1], and in particular is strictly positive provided that the system $F_1 = \cdots = F_R$ has non-singular solutions everywhere locally.

We remark that when $R = 1$, the quantity $\sigma$ is the dimension of the singular locus of $F_1 = 0$. In the case of non-singular cubic forms ($R = 1, d = 3, \sigma = -1$), Theorem 4.0.1 provides an asymptotic formula for $N(B)$ provided that $n \geqslant 17$. Birch's result therefore generalises and improves on earlier work of Davenport, which treats non-singular cubic forms in at least $32$ variables [41].

We briefly mention some directions in which Theorem 4.0.1 has been generalised. Birch's results have been extended to number fields by Skinner [109], and function fields by Lee [80]. Schindler [101] studied bihomogeneous forms in many variables. Browning and Heath-Brown [15] generalised Theorem 4.0.1 to the setting where $F_1, \ldots, F_R$ may have differing degrees. In this chapter, we shall focus our discussion around the case $R = 1$ of a single homogeneous form $F$. However, the behaviour in terms of $R$ is also interesting, and we remark that Rydin Myerson has improved the dependence on $R$ in (4.0.6) from quadratic to linear [99].

It seems intrinsic to methods based on Weyl differencing discussed in Section 4.2 that increasing the degree by one should at least double the number of variables required, so that $n$ has to grow exponentially with $d$ in order for the circle method to work. Indeed, for general values of $d$, very few improvements to Theorem 4.0.1 have been found, a notable exception being the work of Browning and Prendiville [20], which replaces the factor $(d-1)$ appearing in (4.0.6) with $d - \frac{\sqrt{d}}{2}$ in the case $R = 1$.

However, by restricting to particular small values of $d$ (namely $d \leqslant 4$), substantial improvements to the bounds provided in Theorem 4.0.1 have been found. These results typically rely on some form of the *Kloosterman circle method*, which we discuss in Section 4.3. For example, Heath-Brown [60] uses this approach to treat non-singular cubic forms in $n \geqslant 10$ variables. By further developing the delta method of Duke, Friedlander and Iwaniec [46], Heath-Brown [61], demonstrated for the first time that the circle method can handle the case $d = 2$ of quadratic forms even for $n = 3$ and $n = 4$. The current record for non-singular quartic forms is $n \geqslant 29$ (compared to $n \geqslant 49$ obtained from Theorem 4.0.1), which was recently established by Marmon and Vishe [84] by a delicate refinement of the aforementioned ideas.

## 4.1 The major arcs

To analyse the integral over the major arcs $\mathfrak{M}$, we replace each $\alpha \in \mathfrak{M}$ with the rational number $a/q$ with small denominator that it approximates. With an appropriate choice of $\mathfrak{M}$, the error in doing so is negligible, since by continuity, $S(\alpha)$ is close to $S(a/q)$.

Let $\eta > 0$. A common choice for the major arcs is

$$\mathfrak{M} = \bigcup_{q<B^\eta} \bigcup_{\substack{0\leqslant a<q \\ \gcd(a,q)=1}} \mathfrak{M}(a,q), \tag{4.1.1}$$

where

$$\mathfrak{M}(a,q) = \left\{\alpha \in [0,1) : \left|\alpha - \frac{a}{q}\right| < B^{-d+\eta}\right\}.$$

We choose $\eta$ sufficiently small that these major arcs are non-overlapping. It is immediate from the definition of $\mathfrak{M}$ that

$$\int_{\mathfrak{M}} S(\alpha)\mathrm{d}\alpha = \sum_{q<B^\eta} \sum_{\substack{0\leqslant a<q \\ \gcd(a,q)=1}} \int_{|\theta|<B^{-d+\eta}} S(a/q+\theta)\,\mathrm{d}\theta. \tag{4.1.2}$$

Suppose that $\alpha \in \mathfrak{M}(a,q)$, and write $\alpha = a/q+\theta$. Since the quantity $e(aF(\mathbf{x}))$ only depends on the value of $\mathbf{x}$ modulo $q$, we have

$$S(\alpha) = \sum_{\mathbf{x} \pmod q} e_q(aF(\mathbf{x})) \sum_{\substack{\mathbf{y}\in\mathbb{Z}^n \\ |\mathbf{y}|\leqslant B \\ \mathbf{y}\equiv\mathbf{x} \pmod q}} e(\theta F(\mathbf{y})). \tag{4.1.3}$$

Using [11, Lemma 8.1], we can smooth out the inner sum of (4.1.3) by replacing it with the corresponding integral. Let

$$S_{a,q} = \sum_{\mathbf{x} \pmod q} e_q(aF(\mathbf{x})).$$

We obtain

$$S(\alpha) \sim \frac{S_{a,q}}{q^n} \int_{|\mathbf{y}|\leqslant B} e(\theta F(\mathbf{y}))\mathrm{d}\mathbf{y} = \frac{B^n S_{a,q}}{q^n} \int_{|\mathbf{y}|\leqslant 1} e(\theta B^d F(\mathbf{y}))\mathrm{d}\mathbf{y}, \tag{4.1.4}$$

where in the last line we have made a change of variables from $\mathbf{y}$ to $B\mathbf{y}$. The purpose of the above manipulations is that we have now completely separated the dependence of $S(\alpha)$ on $a/q$ from its dependence on $\theta$. Returning to (4.1.2), and changing variables from $B^d\theta$ to $\theta$, we deduce that

$$\int_{\mathfrak{M}} S(\alpha)\mathrm{d}\alpha \sim B^{n-d} \left( \sum_{q<B^\eta} \sum_{\substack{0\leqslant a<q \\ \gcd(a,q)=1}} \frac{S_{a,q}}{q^n} \right) \left( \int_{|\theta|<B^\eta} \int_{|\mathbf{y}|\leqslant 1} e(\theta F(\mathbf{y}))\mathrm{d}\mathbf{y}\mathrm{d}\theta \right). \tag{4.1.5}$$

When $n$ is sufficiently large in terms of $d$, we may complete the sum over $q$ and the integral over $\theta$ to obtain

$$\int_{\mathfrak{M}} S(\alpha)\mathrm{d}\alpha \sim B^{n-d}\mathfrak{S}_F\mathfrak{J}_F, \tag{4.1.6}$$

where

$$\mathfrak{S}_F = \sum_{q=1}^{\infty} \sum_{\substack{0\leqslant a<q \\ \gcd(a,q)=1}} \frac{S_{a,q}}{q^n}, \tag{4.1.7}$$

$$\mathfrak{J}_F = \int_{\theta\in\mathbb{R}} \int_{|\mathbf{y}|\leqslant 1} e(\theta F(\mathbf{y}))\mathrm{d}\mathbf{y}\mathrm{d}\theta. \tag{4.1.8}$$

The quantities $\mathfrak{S}_F$ and $\mathfrak{J}_F$ are called the *singular series* and *singular integral* respectively, and when $F$ is non-singular they are compatible with the leading constant predicted by Peyre's refinement of Manin's conjecture [91, Section 4.2]. Assuming $\mathfrak{S}_F$ is absolutely convergent, it follows from multiplicativity of $S_{a,q}$ that

$$\mathfrak{S}_F = \prod_p \sigma_p,$$

where

$$\sigma_p = \lim_{t\to\infty} p^{-t(n-1)}\#\{\mathbf{x} \pmod{p^t} : F(\mathbf{x}) \equiv 0 \pmod{p^t}\}.$$

If the equation $F = 0$ has non-singular solutions everywhere locally, then by Hensel's lemma, we see that $\sigma_p > 0$ for all $p$, and in fact, assuming in addition that the product is absolutely convergent, we have $\mathfrak{S}_F > 0$. The typical approach to analyse the singular series is discussed in more detail in [12, Section 2.3].

## 4.2 The minor arcs

A basic approach in order to tackle the minor arcs is to use *Weyl differencing*, which is a technique that can be applied iteratively to reduce the degree of the polynomial $F$ under consideration. This leads to a key lemma known as *Weyl's inequality*. Below, we sketch the main ideas behind Weyl's inequality, leaving a more precise statement and proof to [12, Lemma 2.4]. In this section, boldface

letters will always denote vectors in $\mathbb{Z}^n$. We have

$$\begin{aligned}|S(\alpha)|^2 &= S(\alpha)\overline{S(\alpha)}\\ &= \sum_{|\mathbf{x}_1|,|\mathbf{x}_2|\leqslant B} e(\alpha(F(\mathbf{x}_1)-F(\mathbf{x}_2)))\\ &= \sum_{|\mathbf{x}_1|\leqslant 2B}\ \sum_{\substack{|\mathbf{x}_2|\leqslant B\\ |\mathbf{x}_1+\mathbf{x}_2|\leqslant B}} e(\alpha(F(\mathbf{x}_1+\mathbf{x}_2)-F(\mathbf{x}_2)))\\ &\leqslant \sum_{|\mathbf{x}_1|\leqslant 2B}\left|\sum_{\substack{|\mathbf{x}_2|\leqslant B\\ |\mathbf{x}_1+\mathbf{x}_2|\leqslant B}} e(\alpha(F(\mathbf{x}_1+\mathbf{x}_2)-F(\mathbf{x}_2)))\right|. \qquad (4.2.1)\end{aligned}$$

We denote the inner sum in (4.2.1) by $T(\alpha;\mathbf{x}_1)$. Now $F(\mathbf{x}_1+\mathbf{x}_2)-F(\mathbf{x}_2)$ is a polynomial of degree $d-1$ in the variables $\mathbf{x}_2$. Therefore, the quantity $T(\alpha;\mathbf{x}_1)$ is similar to $S(\alpha)$ but for a polynomial with degree one lower. To continue the process, we apply the Cauchy–Schwarz inequality to obtain

$$|S(\alpha)|^4 \leqslant (4B)^n \sum_{|\mathbf{x}_1|\leqslant 2B} |T(\alpha;\mathbf{x}_1)|^2.$$

The quantity $|T(\alpha;\mathbf{x}_1)|^2$ may be treated analogously to (4.2.1) to obtain

$$|S(\alpha)|^4 \leqslant (4B)^n \sum_{|\mathbf{x}_1|\leqslant 2B}\sum_{|\mathbf{x}_2|\leqslant 2B}\ \sum_{\substack{|\mathbf{x}_3|\leqslant B\\ |\mathbf{x}_2+\mathbf{x}_3|\leqslant B\\ |\mathbf{x}_1+\mathbf{x}_3|\leqslant B\\ |\mathbf{x}_1+\mathbf{x}_2+\mathbf{x}_3|\leqslant B}} e(\alpha(F(\mathbf{x}_1,\mathbf{x}_2;\mathbf{x}_3)),$$

where

$$F(\mathbf{x}_1,\mathbf{x}_2;\mathbf{x}_3) = F(\mathbf{x}_1+\mathbf{x}_2+\mathbf{x}_3)-F(\mathbf{x}_2+\mathbf{x}_3)-F(\mathbf{x}_1+\mathbf{x}_3)+F(\mathbf{x}_3)$$

is a polynomial of degree $d-2$ in the variables $\mathbf{x}_3$.

Iterating this process $d-1$ times yields an estimate for $|S(\alpha)|^{2^{d-1}}$ in terms of sums of exponentials $e(\alpha L(\mathbf{x}_1,\dots,\mathbf{x}_{d-1};\mathbf{x}_d))$, where $L(\mathbf{x}_1,\dots,\mathbf{x}_{d-1};\mathbf{x}_d)$ are linear polynomials in the variables $\mathbf{x}_d$. Writing $\mathbf{x}_d = (x_d^{(1)},\dots,x_d^{(n)})$, it can be checked that

$$e(\alpha L(\mathbf{x}_1,\dots,\mathbf{x}_{d-1};\mathbf{x}_d)) = e(h)\prod_{i=1}^{n} e(\beta_i x_d^{(i)}), \qquad (4.2.2)$$

where $h = h(\mathbf{x}_1,\dots,\mathbf{x}_{d-1})$ is independent of $\mathbf{x}_d$ and $\beta_i = \beta_i(\mathbf{x}_1,\dots,\mathbf{x}_{d-1})$ is multilinear in $\mathbf{x}_1,\dots,\mathbf{x}_{d-1}$. We must now take a sum of (4.2.2) over $\mathbf{x}_d\in\mathbb{Z}^n$ lying in some box which depends on $\mathbf{x}_1,\dots,\mathbf{x}_{d-1}$. This sum splits into a product of geometric series, which can be treated using the elementary fact that

$$\left|\sum_{x\leqslant X} e(\beta x)\right| \ll \frac{1}{\|\beta\|} \qquad (4.2.3)$$

for any $X \geqslant 1$, where $\|\beta\|$ denotes the distance of $\beta$ to the nearest integer. If $\|\beta\|$ is extremely small, this estimate is not useful, so we resort to the trivial bound $|\sum_{x \leqslant X} e(\beta x)| \leqslant X$. Applying this for all $i \in \{1, \dots, n\}$ would recover the trivial estimate $S(\alpha) \leqslant B^n$. In order to do better than this, the task is now to show that the quantities $\|\beta_1\|, \dots, \|\beta_n\|$ are very rarely this small as we average over $\mathbf{x}_1, \dots, \mathbf{x}_{d-1}$.

## 4.3 The Kloosterman circle method

Given the difficulties in finding good estimates for the minor arcs, a more ambitious approach is to do away with the minor arcs completely, and instead try to find an asymptotic formula for $S(\alpha)$ for all $\alpha$. This is the idea behind Kloosterman's version of the circle method. Typically, the major arcs are defined using *Farey dissection*. For a parameter $Q \geqslant 1$, we define the *Farey sequence* to be the sequence of all reduced fractions $a/q$ with $0 \leqslant a \leqslant q \leqslant Q$, arranged in ascending order. We then divide $[0, 1)$ into a disjoint union of intervals $\mathfrak{M}_{a,q} = [b, c)$, where $b, c$ are the medians of the consecutive terms $\frac{a'}{q'} < \frac{a}{q} < \frac{a''}{q''}$ of the Farey sequence. This results in the expression

$$\delta(n) = \sum_a \sum_q \int_{\mathfrak{M}_{\mathfrak{a},\mathfrak{q}}} e(n\alpha) \mathrm{d}\alpha,$$

where the summation is over all reduced fractions $a/q$ in the Farey sequence. An elementary manipulation [71, Proposition 20.7] yields

$$\delta(n) = 2 \operatorname{Re} \int_0^1 \sum_{\substack{q \leqslant Q < b \leqslant q+Q \\ \gcd(b,q)=1}} \sum (bq)^{-1} e\left(\frac{n\bar{b}}{q} - \frac{n\theta}{bq}\right) \mathrm{d}\theta,$$

where $\bar{b}$ denotes the multiplicative inverse of $b$ modulo $q$.

A major advantage of this approach over the Hardy–Littlewood circle method is that there is potential to exploit cancellation in the sums over $a$ and $q$. (The ability to do this in the Hardy–Littlewood method is lost when we take modulus signs in $\int_{\mathfrak{m}} |S(\alpha)| \mathrm{d}\alpha$.) Cancellation in the sum over $a$ was first exploited by Kloosterman [75], who gave a complete classification of the integers $a, b, c, d$ for which $ax^2 + by^2 + cz^2 + dt^2$ represents every sufficiently large integer, a problem just out of reach of the classical Hardy–Littlewood circle method. Such a cancellation in $a$ is now referred to as a *Kloosterman refinement*. In rare cases, a cancellation in both the $a$ and $q$ sums has been achieved (known as a *double Kloosterman refinement*). This idea was first used by Hooley when studying Waring's problem for cubes in 7 variables [67].

One disadvantage of the Kloosterman circle method is the presence of exponential sums involving $\bar{b}$, which in practice are often awkward to analyse. In

the next section, we introduce the delta method, which provides a way to circumvent this issue.

## 4.4 The delta method

We now discuss the delta method, as introduced by Duke, Friedlander and Iwaniec [46] and further developed by Heath-Brown [61]. Let $g : \mathbb{R} \to \mathbb{R}_{\geqslant 0}$ be a function which is normalised so that $\sum_{q=1}^{\infty} g(q) = 1$ and $g(0) = 0$. Then for any integer $n$, we have

$$\delta(n) = \sum_{q \mid n} \left\{ g(q) - g\left(\frac{|n|}{q}\right) \right\}.$$

We can detect the condition $q \mid n$ using the fact that $\frac{1}{q} \sum_{a \pmod q} e_q(an)$ is equal to $1$ if $q \mid n$ and $0$ otherwise. Therefore,

$$\delta(n) = \sum_{q=1}^{\infty} \frac{1}{q} \left\{ g(q) - g\left(\frac{|n|}{q}\right) \right\} \sum_{a \pmod q} e_q(an).$$

Finally, we convert the fractions $a/q$ that feature in the expressions $e_q(an)$ into reduced fractions by extracting a sum over $j \mid \gcd(a, q)$. We obtain the following identity, first considered by Duke, Friedlander and Iwaniec [46].

$$\delta(n) = \sum_{q=1}^{\infty} \sum_{\substack{a \pmod q \\ \gcd(a,q)=1}} e_q(an) \sum_{j=1}^{\infty} \frac{1}{jq} \left\{ g(jq) - g\left(\frac{|n|}{jq}\right) \right\}. \tag{4.4.1}$$

In practice, $g$ is often taken to be an infinitely differentiable function supported on $[Q/2, Q]$. With such a choice, the $q$-sum in (4.4.1) can be restricted to $q \ll \max(Q, 2|n|/Q)$, and so it seems natural to take $Q = |n|^{1/2}$.

Heath-Brown's variant of (4.4.1) replaces the condition $\sum_{q=1}^{\infty} g(q) = 1$ with the smooth analogue $\int_{-\infty}^{\infty} g(x)\mathrm{d}x = 1$. In order to apply estimates involving repeated integration by parts, it is desirable to also have good control over the derivatives of $g$. This can be achieved by building $g$ out of the *standard bump function* $\psi : \mathbb{R} \to \mathbb{R}_{\geqslant 0}$ given by

$$\psi(t) = \begin{cases} \exp(\frac{1}{t^2-1}), & \text{if } |t| < 1, \\ 0, & \text{otherwise}, \end{cases} \tag{4.4.2}$$

which is an infinitely differentiable function supported on $[-1, 1]$, all of whose derivatives are $O(1)$. More precisely, we let $w_0(x) = c\psi(4x - 3)$, where $c$ is the constant such that $\int_{-\infty}^{\infty} w_0(x)\mathrm{d}x = 1$, and then define $g(x) = w_0(x/Q)$. We note that this makes $g$ supported on $[Q/2, Q]$ as before. It can be shown by

applying Poisson summation and repeated integration by parts that $\sum_{q=1}^{\infty} g(q) = C_Q$, where $C_Q = 1 + O_N(Q^{-N})$. We therefore almost recover the assumption $\sum_{q=1}^{\infty} g(q) = 1$ used in the formulation of (4.4.1). Proceeding as above, we deduce the following estimate for $\delta(n)$ [61, Theorem 1].

$$\delta(n) = \frac{C_Q}{Q^2} \sum_{q=1}^{\infty} \sum_{\substack{0 \leqslant a < q \\ \gcd(a,q)=1}} e_q(an) h\left(\frac{q}{Q}, \frac{n}{Q^2}\right), \tag{4.4.3}$$

where

$$h(x,y) = \sum_{j=1}^{\infty} \frac{1}{xj} \left\{ w_0(xj) - w_0\left(\frac{|n|}{xj}\right) \right\}. \tag{4.4.4}$$

We now apply (4.4.3) to count zeros of a polynomial $F \in \mathbb{Z}[x_1, \dots, x_n]$. Let $w : \mathbb{R}^n \to \mathbb{R}_{\geqslant 0}$ be a compactly supported infinitely differentiable function. We define

$$N(w, B) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ F(\mathbf{x})=0}} w(B^{-1}\mathbf{x}),$$

which is a smoothly weighted analogue of the counting function $N(B)$ from (4.0.3). Typically, we let $w$ be a smooth approximation to the characteristic function $1_{[-1,1]^n}$ so that $N(w, B)$ approximates $N(B)$. We have

$$\begin{aligned} N(w,B) &= \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ |\mathbf{x}| \leqslant B}} w(B^{-1}\mathbf{x}) \delta(F(\mathbf{x})) \\ &= \frac{C_Q}{Q^2} \sum_{q=1}^{\infty} \sum_{\substack{a \pmod q \\ \gcd(a,q)=1}} \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ |\mathbf{x}| \leqslant B}} e_q(aF(\mathbf{x})) w(B^{-1}\mathbf{x}) h\left(\frac{q}{Q}, \frac{F(\mathbf{x})}{Q^2}\right) \\ &= \frac{C_Q}{Q^2} \sum_{q=1}^{\infty} \sum_{\substack{a \pmod q \\ \gcd(a,q)=1}} \sum_{\boldsymbol{b} \pmod q} e_q(aF(\boldsymbol{b})) \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ \mathbf{x} \equiv \boldsymbol{b}(q)}} w(B^{-1}\mathbf{x}) h\left(\frac{q}{Q}, \frac{F(\mathbf{x})}{Q^2}\right). \end{aligned} \tag{4.4.5}$$

The $n$-dimensional Poisson summation formula [114, Theorem VII.2.4] states that for a smooth compactly supported function $f : \mathbb{R}^n \to \mathbb{R}$, we have

$$\sum_{\mathbf{y} \in \mathbb{Z}^n} f(\mathbf{y}) = \sum_{\mathbf{c} \in \mathbb{Z}^n} \int_{\mathbb{R}^n} f(\mathbf{y}) e(-\mathbf{c} \cdot \mathbf{y}) \mathrm{d}\mathbf{y}.$$

Applying this to the inner summand of (4.4.5), with the change of variables $\mathbf{x} = q\mathbf{y} + \boldsymbol{b}$, we obtain the following result.

**Theorem 4.4.1** ([61, Theorem 2]). *We have*

$$N(w,B) = \frac{C_Q}{Q^2} \sum_{\mathbf{c}\in\mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(\mathbf{c}) I_q(\mathbf{c}), \tag{4.4.6}$$

*where*

$$\begin{aligned} S_q(\mathbf{c}) &= \sum_{\substack{a \pmod q \\ \gcd(a,q)=1}} \sum_{\mathbf{b} \pmod q} e_q(aF(\boldsymbol{b}) + \mathbf{b}\cdot\mathbf{c}), \\ I_q(\mathbf{c}) &= \int_{\mathbb{R}^n} w(B^{-1}\mathbf{x}) h\left(\frac{q}{Q}, \frac{F(\mathbf{x})}{Q^2}\right) e_q(-\mathbf{c}\cdot\mathbf{x})\,\mathrm{d}\mathbf{x}. \end{aligned} \tag{4.4.7}$$

Thinking of $w$ as an approximation for $1_{[-1,1]^n}$, we expect $F(\mathbf{x})$ to typically have size $B^d$ for $\mathbf{x}\in\mathbb{Z}^n$ satisfying $w(B^{-1}\mathbf{x}) \neq 0$. Recalling the discussion after (4.4.1), it is therefore natural to take $Q = B^{d/2}$. However, it turns out in some cases to be beneficial to choose $Q$ smaller than this. For example, in their study of quartic forms in $n \geqslant 29$ variables, Marmon and Vishe make the choice $Q = B^{8/5+\epsilon}$ [84] by applying a level lowering trick of Munshi [89].

Usually when applying Theorem 4.4.1, the main term comes from the case $\mathbf{c} = \mathbf{0}$, and we aim to show that the sum over all other values $\mathbf{c} \neq \mathbf{0}$ is negligible. This intuitively makes sense, since $S_q(\mathbf{c})$ and $I_q(\mathbf{c})$ exhibit greater oscillation for larger values of $\mathbf{c}$. A basic way to exploit this is via the *first derivative test*, which is essentially repeated integration by parts for $I_q(\mathbf{c})$, where we integrate the factor $e_q(\mathbf{c}\cdot\mathbf{x})$. We combine this idea with some more refined estimates in Section 6.4.

## 4.5 Application to counting Campana points

In this section, we indicate how the delta method is applied to count Campana points in Chapter 6, thus providing a sketch proof of Theorem D. We recall from the introduction the definition

$$\mathscr{N}_k(B) = \left\{ \mathbf{z} \in (\mathbb{Z}_{\neq 0})^k_{\mathrm{prim}} : |z_i| \leqslant B, z_i \text{ squareful for all } i, \sum_{i=1}^k z_i = 0 \right\}. \tag{4.5.1}$$

Using Lemma 3.3.1, we may write each $z_i$ uniquely in the form $z_i = x_i^2 y_i^3$ for $x_i$ positive integers and $y_i$ squarefree integers. The resulting equation $\sum_{i=1}^k y_i^3 x_i^2 = 0$ defines a quadric for each fixed choice of $\mathbf{y} = (y_1,\dots,y_k)$. Therefore,

$$\#\mathscr{N}_k(B) = \frac{1}{2^k} \sum_{\substack{\mathbf{y}\in(\mathbb{Z}_{\neq 0})^k \\ y_1,\dots,y_k \text{ squarefree}}} N_{\mathbf{y}}(B), \tag{4.5.2}$$

where

$$N_{\mathbf{y}}(B) = \#\left\{\mathbf{x} \in (\mathbb{Z}_{\neq 0})^k : \sum_{i=1}^{k} x_i^2 y_i^3 = 0, \begin{array}{l} \gcd(x_1 y_1, \dots, x_k y_k) = 1 \\ \max_{1 \leqslant i \leqslant k} |y_i^3 x_i^2| \leqslant B \end{array}\right\}.$$

The factor $1/2^k$ comes from the fact that for each $i \in \{1, \dots, k\}$, there are two choices for the sign of $x_i$ corresponding to the same choice of $z_i$.

Non-singular quadrics conform to Manin's conjecture (Conjecture 2.3.2). This is because such quadrics are examples of flag varieties, for which Manin's conjecture is known to hold by the work of Franke, Manin and Tschinkel [50]. In fact, the Picard number $\varrho$ of the quadric $\sum_{i=1}^{4} y_i^3 x_i^2$ is 2 if $y_1 \cdots y_4 = \square$, and 1 otherwise. Therefore, we have asymptotic formulas of the shape

$$N_{\mathbf{y}}(B) \sim \begin{cases} c_{\mathbf{y}} B, & \text{if } y_1 \cdots y_4 \neq \square, \\ c_{\mathbf{y}} B \log B, & \text{if } y_1 \cdots y_4 = \square, \end{cases} \tag{4.5.3}$$

for explicit constants $c_{\mathbf{y}} \geqslant 0$ depending on $\mathbf{y}$. This explains why we need to remove the thin set defined by the condition $z_1 \cdots z_4 = \square$ from $\mathscr{N}_4(B)$ in order to compare our count with the PSTV-A conjecture (Conjecture 3.0.8). We therefore consider (4.5.2) with the added condition $y_1 \cdots y_4 \neq \square$, which is equivalent to $z_1 \cdots z_4 \neq \square$.

Whilst (4.5.3) provides an asymptotic formula for each individual $N_{\mathbf{y}}(B)$, crucially, we need enough uniformity in our estimates that we can take a sum over $\mathbf{y}$ and still maintain sufficient control over the error terms. For $k \geqslant 5$, Van Valckenborgh demonstrated that sufficient uniformity can be obtained by applying the classical circle method as introduced at the beginning of this chapter to each $N_{\mathbf{y}}(B)$. In the case $k = 4$, we require a better dependence of the error terms on $\mathbf{y}$ than the classical circle method can provide, so we instead apply the delta method as discussed in Section 4.4. We consider a slightly more general counting function

$$N_{\mathbf{a}}(B) = \#\left\{\mathbf{x} \in (\mathbb{Z}_{\neq 0})^4 : \sum_{i=1}^{4} a_i x_i^2 = 0, \max_{1 \leqslant i \leqslant 4} |a_i x_i^2| \leqslant B\right\}, \tag{4.5.4}$$

where we have removed the coprimality condition and replaced $(y_1^3, \dots, y_4^3)$ with an arbitrary vector $\mathbf{a} = (a_1, \dots, a_4) \in (\mathbb{Z}_{\neq 0})^4$. We conclude this section by stating the main result of Section 6.4, which is an estimate for $N_{\mathbf{a}}(B)$ obtained from the delta method in which the dependence of the error terms on $\mathbf{a}$ is made completely explicit. Our result features the quantities

$$\Delta = \prod_{i=1}^{4} \gcd\left(a_i, \prod_{j \neq i} a_j\right), \quad A = a_1 \cdots a_4,$$

as well as a *singular series* $\mathfrak{G}_{\mathbf{a}}$ and a *singular integral* $\sigma_\infty(\boldsymbol{\epsilon})|A|^{-1/2}$, defined respectively in (6.4.1) and (6.4.2). Note that $\sigma_\infty(\boldsymbol{\epsilon})$ only depends on the signs $\boldsymbol{\epsilon} = (\epsilon_1, \dots, \epsilon_4)$ of $(a_1, \dots, a_4)$.

**Theorem 4.5.1.** *Let* $\mathbf{a} \in (\mathbb{Z}_{\neq 0})^4$ *be such that* $A \neq \square$ *and* $|A| \leqslant B^{4/7}$. *Then*

$$N_{\mathbf{a}}(B) = \frac{\mathfrak{G}_{\mathbf{a}}\sigma_\infty(\boldsymbol{\epsilon})B}{|A|^{1/2}} + O\left(\frac{B^{41/42+\epsilon}\Delta^{1/3}}{|A|^{11/24}}\right), \tag{4.5.5}$$

*where the implied constant depends only on* $\epsilon$.

To complete the proof of Theorem D, in Section 6.5, we apply Theorem 4.5.1 together with an inclusion-exclusion argument in order to reinsert the coprimality condition $\gcd(x_1y_1, \dots, x_4y_4) = 1$ and obtain an estimate for $N_{\mathbf{y}}(B)$. Returning to (4.5.2), we can take a sum over these estimates for $N_{\mathbf{y}}(B)$ in the range $\max_{1\leqslant i\leqslant 4}|y_i| \leqslant D$, where $D$ is a small power of $B$. The contribution from the remaining range $\max_{1\leqslant i\leqslant 4}|y_i| > D$ is dealt with in Section 6.3 using an elementary argument, and forms part of the error term in Theorem D.

CHAPTER 5

# Sieves

Sieve theory is an ancient but continually evolving area of mathematics, which has traditionally been used as a way to estimate the distribution of primes in sets of arithmetic interest. In this chapter, we give an account of the development of combinatorial sieves. We begin with the Legendre–Eratosthenes sieve in Section 5.1, which is based on the inclusion-exclusion principle. In Sections 5.2-5.6 (which are based on [52, Chapters 1,4,6,11] and [116]), we discuss various refinements and generalisations, eventually arriving in Section 5.6 at a powerful result known as the beta sieve, first introduced by Rosser and Iwaniec. We discuss these developments through the lens of two main examples, namely the prime counting function $\pi(x)$, and the twin prime conjecture. However, modern applications of sieve theory are extremely diverse. In Section 5.7, we state the main sieve results we prove in Chapter 8 in order to study the Hasse principle for polynomials represented by norm forms. These results concern values of binary forms which avoid prime factors belonging to certain sifting sets. The density of the sifting sets we consider is governed by the Chebotarev density theorem, which we introduce in Section 5.8. Finally, in Section 5.9, we prove a level of distribution result which is an essential ingredient in the application of the beta sieve in Chapter 8.

## 5.1 The Legendre–Eratosthenes sieve

One of the first sieves was the *sieve of Eratosthenes* from the 3rd century BC, which provides a way to list all the prime numbers up to a given integer $x$. The algorithm can be stated as follows:

1. Begin with the list of integers $(2, \dots, x)$.

2. Find the first integer $k$ in the list which is not circled or crossed out, and circle it. Cross out all integers up to $x$ of the form $nk$, where $n \geqslant 2$.

3. Repeat $(2)$ iteratively until an integer greater than or equal to $\sqrt{x}$ has been circled.

4. Circle all remaining integers which have not been crossed out.

The list of circled integers obtained from this algorithm is the list of prime numbers up to $x$, due to the fact that every composite integer $m \leqslant x$ contains a prime factor $p \leqslant \sqrt{x}$.

Often, we do not want to list prime numbers explicitly, but instead want estimates for the density of primes in a given interval. Let $\pi(x)$ denote the number of primes $p \leqslant x$. The *Legendre–Eratosthenes sieve* is a quantitative version of the sieve of Eratosthenes, and provides an estimate for $\pi(x)$.

Let $A = [1, x] \cap \mathbb{N}$, let $P$ denote the set of all primes, and let $z > 1$ be a parameter, which is called the *sifting level*. We define a *sifting function*

$$S(A, P, z) = \#\{n \in A : p \nmid n \text{ for all } p \in P, p < z\}. \tag{5.1.1}$$

It is also convenient to define

$$P(z) = \prod_{\substack{p \in P \\ p < z}} p. \tag{5.1.2}$$

Then the condition in (5.1.1) can be rewritten as $\gcd(n, P(z)) = 1$. We observe that

$$S(A, P, \sqrt{x}) = \pi(x) - \pi(\sqrt{x}) + O(1). \tag{5.1.3}$$

Finally, we define

$$V(z) = \prod_{p < z} \left(1 - \frac{1}{p}\right). \tag{5.1.4}$$

We begin with a simple heuristic. The probability that a randomly chosen integer $n$ in the interval $[1, x]$ is a multiple of a given prime $p \leqslant \sqrt{x}$ is roughly $1 - \frac{1}{p}$. If we believe that the properties $p_1 \mid n$ and $p_2 \mid n$ are independent for distinct primes $p_1$ and $p_2$, then we might guess that $S(A, P, \sqrt{x})$, has size comparable to $xV(\sqrt{x})$. The Legendre–Eratosthenes sieve attempts to make this heuristic more precise by keeping track of the error terms produced when comparing $S(A, P, z)$ with $xV(z)$.

When using the sieve of Eratosthenes to count primes, we begin with the number $x = |A|$, and subtract the number of even numbers in $A$, and then the number of multiples of $3$ in $A$, and the number of multiples of $5$ in $A$ and so on. We

then note that some numbers have been discarded twice, like $6$ for example, so we must add back in the number of multiples of $6$ in $A$ and so on. More generally, let $A_d = \{n \in A : d \mid n\}$, where here, and for the remainder of this chapter, we always assume that $d$ is a squarefree positive integer. The above process is formalised by the *inclusion-exclusion principle*, which states that

$$S(A,P,z) = |A| - \sum_{p_1|P(z)} |A_{p_1}| + \sum_{p_1p_2|P(z)} |A_{p_1p_2}| - \sum_{p_1p_2p_3|P(z)} |A_{p_1p_2p_3}| + \cdots . \tag{5.1.5}$$

The inclusion-exclusion process can also be stated in terms of the Möbius function $\mu$.

**Lemma 5.1.1** (Legendre)**.** *We have*

$$S(A,P,z) = \sum_{d|P(z)} \mu(d)|A_d|. \tag{5.1.6}$$

*Proof.* Fix an integer $d|P(z)$. The term $|A_d|$ appears exactly once in (5.1.5), in the form $|A_{p_1\cdots p_r}|$ where $p_1 \cdots p_r$ is the prime factorisation of $d$. The coefficient of $|A_d|$ in (5.1.5) is $(-1)^r$, which is equal to $\mu(d)$. □

We now apply the estimate $|A_d| = \frac{x}{d} + O(1)$. Substituting this into Lemma 5.1.1, we obtain

$$S(A,P,z) = x \sum_{d|P(z)} \frac{\mu(d)}{d} + \sum_{d|P(z)} O(1). \tag{5.1.7}$$

The number of divisors $d \mid P(z)$ is $2^{\pi(z)}$, and the function $\frac{\mu(d)}{d}$ is multiplicative. Therefore,

$$S(A,P,z) = xV(z) + O(2^{\pi(z)}). \tag{5.1.8}$$

By Mertens' theorem [71, Equation (2.16)], the main term in (5.1.8) is

$$xV(z) = x \prod_{p<z} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}x}{\log z} \left(1 + O\left(\frac{1}{\log z}\right)\right), \tag{5.1.9}$$

where $\gamma$ denotes the Euler–Mascheroni constant, so that numerically, we have $e^{-\gamma} = 0.561459....$

Unfortunately, the error term $O(2^{\pi(z)})$ has a very bad dependence on the sifting level $z$, and in order for this error term to be smaller than our main term, we must choose $z$ very small, around size $\log x$. Recalling (5.1.3), the resulting estimate for $\pi(x)$ is

$$\begin{aligned} \pi(x) &= S(A,P,\sqrt{x}) + \pi(\sqrt{x}) + O(1) \\ &\leqslant S(A,P,\log x) + O(\sqrt{x}) \\ &= O\left(\frac{x}{\log\log x}\right). \end{aligned} \tag{5.1.10}$$

Whilst we have obtained a nontrivial estimate for $\pi(x)$ from this method, the bound (5.1.10) does not seem very impressive. After all, we actually know from the Prime number theorem that $\pi(x) \sim \frac{x}{\log x}$ [71, pp.31]. With more care, the error term $O(2^{\pi(z)})$ can be significantly improved; we discuss some refinements in Sections 5.3-5.6. However, we observe that if we just ignore the remainder term in (5.1.7) and plug $z = \sqrt{x}$ into (5.1.9), we would obtain $\pi(x) \sim \frac{2e^{-\gamma}x}{\log x}$, which has the wrong leading constant. Hence the naive heuristic discussed above does not capture the correct leading constant, and the remainder term $\sum_{d|P(z)} \mu(d) \left(|A_d| - \frac{x}{d}\right)$ must actually have size comparable to the main term.

Despite the above shortcomings, sieve theory has proven to be a powerful tool in the study of prime numbers. A major advantage of sieve theory lies in its flexibility–it can be applied in very general settings in which the techniques from complex analysis underpinning results such as the Prime number theorem are no longer available. We now proceed to discuss sieves in a more general framework.

## 5.2 Sieving in more generality

Let $x \geqslant 1$ be a parameter. Let $P$ be an arbitrary set of prime numbers. Let $\mathscr{A} = (a_n)_{n\in\mathbb{Z}}$ be a sequence of non-negative real numbers, supported on $[-x, x]$. Let $P(z)$ be as defined in (5.1.2). For each $p \mid P(z)$, let $E_p \subseteq \mathbb{Z}$ be an associated set. We would like to find estimates for the sums

$$S(\mathscr{A}, P, z) := \sum_{n\in\mathbb{Z}} a_n 1_{n\notin\bigcup_{p|P(z)} E_p}. \tag{5.2.1}$$

For a squarefree integer $d$, let $E_d = \bigcap_{p|d} E_p$, and let $E_1 = \mathbb{Z}$. we can adapt the proof of Lemma 5.1.1 to this more general setting to show that

$$\sum_{n\in\mathbb{Z}} 1_{n\notin\bigcup_{p|P(z)} E_p} = \sum_{d|P(z)} \mu(d) \sum_{n\in E_d} a_n, \tag{5.2.2}$$

which is known as the *Legendre sieve identity*. We denote by $\mathscr{A}_d$ the sequence $(a_n 1_{E_d}(n))$. By an abuse of notation, we let $|\mathscr{A}_d| = \sum_{n\in E_d} a_n$, and we let $X = |\mathscr{A}| = |\mathscr{A}_1|$.

Whilst $E_p$ may be arbitrary, in applications it is often taken to be the integers belonging to some set of residue classes modulo $p$, and this will be the case for all examples we consider in this work. Let $g(d)$ be a multiplicative function, supported on squarefree integers. We write

$$|\mathscr{A}_d| = g(d)X + r(d), \tag{5.2.3}$$

where $r(d)$ is a remainder term. We require that $r_d$ is small, at least on average over $d$. Such an estimate is known as a *level of distribution result*, which we

discuss more in Section 5.3. We also generalise the definition of $V(z)$ from (5.1.4) by setting

$$V(z) = \prod_{p|P(z)} (1 - g(p)). \tag{5.2.4}$$

**Example 5.2.1.** To recover the sifting function $S(A, P, z)$ from (5.1.1) used to estimate $\pi(x)$, we take $A = [1, x]$, $a_n = 1_{n\in A}$, $P = \{\text{all primes}\}$, and $E_p = \{n \in \mathbb{Z} : p \mid n\}$. Then $X = |A_1| = x$ and $|\mathscr{A}_d| = |A_d| = \#\{n \leqslant x : d \mid n\}$. We used the estimate $|A_d| = \frac{x}{d} + O(1)$ in Section 5.1, which corresponds to the choice $g(d) = 1/d$, and the estimate $r(d) = O(1)$.

**Example 5.2.2** (Twin primes)**.** A famous open problem in Prime number theory is the *twin prime conjecture*, which states that there exist infinitely many primes $p$ such that $p + 2$ is also prime. There are several ways to recast this as a sieve problem. For example, we can define

$$\mathscr{A} = 1_{[1,x-2]}, \quad P = \{\text{all primes}\}, \quad E_p = \{n \in \mathbb{Z} : n \equiv 0 \text{ or } -2 \pmod p\}. \tag{5.2.5}$$

If one of $n$ or $n + 2$ is not prime, then it must have a prime factor $\leqslant \sqrt{x}$, and so we would have $n \in \bigcup_{p\leqslant\sqrt{x}} E_p$. Therefore, the twin prime conjecture would follow from unboundedness of $S(\mathscr{A}, P, \sqrt{x})$ as $x \to \infty$.

An alternative formulation, which turns out to provide stronger partial results towards the twin prime conjecture, is to take

$$A = \{q + 2 : q \in P, q \leqslant x\}, \quad P = \{\text{odd primes}\}, \quad E_p = \{n \in \mathbb{Z} : p \mid n\},$$

and $a_n = 1_A, z = \sqrt{x}$.

In a breakthrough result in 2013, Zhang proved that there are infinitely many pairs of primes with a gap bounded by $70$ million by combining the Selberg sieve with other analytic tools [120]. This bound was subsequently improved by Maynard to $600$ [86], and then further to $246$ by the combined efforts of the Polymath project [97].

**Example 5.2.3** (Goldbach conjecture)**.** The Goldbach conjecture states that every even integer $x \geqslant 4$ can be expressed as the sum of two primes. For such an $x$, we define

$$A = \{x - q : q < x \text{ prime }, q \nmid x\}, \quad a_n = 1_A, \quad E_p = \{n \in \mathbb{Z} : p \mid n\},$$

and aim to show that $(5.2.1)$ is nonzero for $z = \sqrt{x}$, so that the set $A$ contains at least one prime.

Whilst the Goldbach conjecture remains wide open, Chen used sieve theory to prove that every sufficiently large even integer is a sum of a prime and a number with at most two prime factors [30].

## 5.3 Upper and lower bound sieve coefficients

We recall that in the Legendre–Eratosthenes sieve discussed in Section 5.1, we may only take the sifting level $z$ of order of magnitude $\log x$, due to the exponential error term $O(2^{\pi(z)})$ coming from (5.1.7). In contrast, we would like to take a sifting level of $\sqrt{x}$. For larger values of $z$, the Legendre sieve is very wasteful, because many of the divisors $d \mid P(z)$ are much larger than $x$, and for each of these, the Legendre sieve produces a $O(1)$ term, whereas we actually know trivially that $|A_d| = 0$. Therefore, it is natural to truncate the sum in (5.1.6) by considering sums of the form

$$\sum_{\substack{d \mid P(z) \\ d < D}} \mu(d)|A_d|. \tag{5.3.1}$$

More generally, we may replace the Möbius function $\mu$ by some other function $f : \mathbb{N} \to \mathbb{R}$, supported on squarefree integers less than $D$ dividing $P(z)$. Of course, for this to be useful, we would like to choose $f$ in such a way that $\sum_{d|P(z)} f(d)|\mathscr{A}_d|$ provides a good approximation to our original sifting function $S(\mathscr{A}, P, z) = \sum_{d|P(z)} \mu(d)|\mathscr{A}_d|$.

**Definition 5.3.1.** We say that the real numbers $(\mu^+(d))_{d|P(z)}$ are *upper bound sieve coefficients* (or an *upper bound sieve*) for the sifting function $S(\mathscr{A}, P, z)$ from (5.2.1) if $\mu^+(1) \geqslant 1$ and $\sum_{d|n} \mu^+(d) \geqslant 0$ for all $n \mid P(z)$. Similarly, $(\mu^-(d))_{d|P(z)}$ are *lower bound sieve coefficients* for $S(\mathscr{A}, P, z)$ if $\mu^-(1) \leqslant 1$ and $\sum_{d|n} \mu^-(d) \leqslant 0$ for all $n \mid P(z)$. We say that $\mu^+$ or $\mu^-$ have *level* $D$ if they are supported on positive squarefree integers less than $D$.

**Lemma 5.3.2.** *Suppose that $(\mu^+(d))_{d|P(z)}$ and $(\mu^-(d))_{d|P(z)}$ are upper and lower bound sieve coefficients for $S(\mathscr{A}, P, z)$ respectively. Then*

$$\sum_{d|P(z)} \mu^-(d)|\mathscr{A}_d| \leqslant S(\mathscr{A}, P, z) \leqslant \sum_{d|P(z)} \mu^+(d)|\mathscr{A}_d|. \tag{5.3.2}$$

*Proof.* Define functions $\nu^+, \nu^- : \mathbb{N} \to \mathbb{R}$ by

$$\nu^+(n) = \sum_{d|P(z)} \mu^+(d)1_{E_d}(n), \quad \nu^-(n) = \sum_{d|P(z)} \mu^-(d)1_{E_d}(n).$$

Then for all $n \mid P(z)$, we have

$$\nu^-(n) \leqslant 1_{n \notin \bigcup_{p|P(z)} E_p} \leqslant \nu^+(n), \tag{5.3.3}$$

as we shall now explain. Suppose that $n \notin \bigcup_{p|P(z)} E_p$. Then $1_{E_d}(n) = 0$ for all $d \mid P(z)$, except for $1_{E_1}(n)$, which is 1. Therefore $\nu^+(n) = \mu^+(1) \geqslant 1$, and $\nu^-(n) = \mu^-(1) \leqslant 1$. Now suppose that $n \in \bigcup_{p|P(z)} E_p$. Let $\{p_1, \dots, p_r\}$ be

the (non-empty) list of primes $q \mid P(z)$ for which $n \in E_q$, and let $m = p_1 \cdots p_r$. Then $\nu^+(n) = \sum_{d|m} \mu^+(d) \geqslant 0$. Therefore, $1_{n \notin \bigcup_{p|P(z)} E_p} \leqslant \nu^+(n)$. Similarly, $\nu^-(n) = \sum_{d|m} \mu^-(d) \leqslant 0$, and so we have established (5.3.3).

Substituting (5.3.3) into the definition of $S(\mathscr{A}, P, z)$, we obtain

$$S(\mathscr{A}, P, z) = \sum_{n \in \mathbb{Z}} a_n 1_{n \notin \bigcup_{p|P(z)} E_p} \leqslant \sum_{n \in \mathbb{Z}} a_n \nu^+(n) = \sum_{n \in \mathbb{Z}} a_n \sum_{d|P(z)} \mu^+(d) 1_{E_d}(n).$$

After switching the order of summation, the last expression can be rewritten as $\sum_{d|P(z)} \mu^+(d)|\mathscr{A}_d|$. We similarly deduce the required lower bound for $S(\mathscr{A}, P, z)$. □

Suppose that $\mu^+, \mu^-$ are upper and lower bound sieve coefficients of level $D$. Recalling (5.2.3), we have found from Lemma 5.3.2 that

$$S(\mathscr{A}, P, z) \leqslant XV^+(z) + R^+(D, z), \tag{5.3.4}$$

where

$$V^+(z) = \sum_{d|P(z)} \mu^+(d) g(d), \quad R^+(D, z) = \sum_{d|P(z)} \mu^+(d) r_d, \tag{5.3.5}$$

and similarly for the lower bound sieve $\mu^-$. We would like to compare $V^+(z)$ and $V^-(z)$ with the quantity

$$V(z) = \sum_{d|P(z)} \mu(d) g(d) = \prod_{p|P(z)} (1 - g(p))$$

defined in (5.2.4).

Usually, there is a natural choice of $g(p)$ such that we expect $S(\mathscr{A}, P, z)$ to have order of magnitude $XV(z)$. We recall from Example 5.2.1 that when estimating $\pi(x)$, the natural choice of multiplicative function is given by $g(d) = \frac{1}{d}$. However, as we saw in Section 5.1, $S(\mathscr{A}, P, z)$ and $XV(z)$ can disagree asymptotically by a constant factor.

In order to effectively compare $XV^+(z)$ and $XV(z)$, we would like $\mu^+$ to be a good approximation for $\mu$, and so in particular for the support $D$ to be as large as possible. In practice, the quality of the bounds for $S(\mathscr{A}, P, z)$ that many sieve methods produce is directly influenced by the size we can take $D$ whilst still maintaining control over the remainder term $R^+(D, z)$; such a bound for $R^+(D, z)$ is called a *level of distribution*. The sieves themselves are not sensitive to the method used to obtain a level of distribution result, and so a wide variety of analytic techniques can be used here. Common approaches involve the theory of exponential sums, tools from harmonic analysis, and the Bombieri–Vinogradov inequality and its variants. A discussion of some of these

techniques can be found in [52, Chapter 22]. In this work, we shall prove a level of distribution result using some ideas from the geometry of numbers. We give more details in Sections 5.7 and 5.9.

Whilst in principle there is scope to exploit cancellation in the sum $R^+(D,z)$, this is often very challenging, so the most common first step is to apply the trivial bound

$$R^+(D,z) \leqslant \sum_{d|P(z)} |\mu^+(d) r_d|.$$

The beta sieve, which we apply in Chapter 8, is an example of a *combinatorial sieve*, which means that $\mu^+(d) \in \{-1,0,1\}$ for all $d$ and $\mu^+$ is supported on squarefree integers $d \leqslant D$. We therefore have

$$R^+(D,z) \leqslant \sum_{\substack{d \leqslant D \\ \mu^2(d)=1}} |r_d|. \tag{5.3.6}$$

## 5.4 Combinatorial sieves

Combinatorial sieves are based on repeated applications of the *Buchstab identity*, which states that

$$1_{n \notin \bigcup_{p<z} E_p} = 1 - \sum_{p<z} 1_{E_p(n)} 1_{n \notin \bigcup_{q<p} E_q}. \tag{5.4.1}$$

This identity comes from the simple observation that for every $n \in \bigcup_{p<z} E_p$, there is a unique choice of $p$ for which $n \in E_p$ but $n \notin E_q$ for any $q < p$. Using the Buchstab identity, we can obtain a variant of the inclusion-exclusion process from (5.1.5), which has the advantage of being easier to truncate. Below, we suppress the set of primes $P$ from the notation for brevity. We have

$$\begin{aligned} S(\mathscr{A},z) &= |\mathscr{A}| - \sum_{p_1<z} S(\mathscr{A}_{p_1},z) \\ &= |\mathscr{A}| - \sum_{p_1<z} |\mathscr{A}_{p_1}| + \sum_{p_2<p_1<z} S(\mathscr{A}_{p_1p_2},z) \\ &= |\mathscr{A}| - \sum_{p_1<z} |\mathscr{A}_{p_1}| + \sum_{p_2<p_1<z} |\mathscr{A}_{p_1p_2}| - \sum_{p_3<p_2<p_1<z} S(\mathscr{A}_{p_1p_2p_3},z) \\ &= \cdots. \end{aligned} \tag{5.4.2}$$

We have a great deal of flexibility as to how to terminate this process. If we require an upper (resp. lower) bound sieve for $S(\mathscr{A},z)$, then at any stage we may remove any of the terms which appear with a coefficient $-1$ (resp. $1$), and only continue to apply Buchstab iterations to the remaining terms.

**Example 5.4.1.** In the Legendre sieve identity from (5.2.2), we have not performed any truncation, instead keeping all terms $S(\mathscr{A}_d,z)$ for any $d \mid P(z)$.

**Example 5.4.2** (Brun pure sieve)**.** The Brun pure sieve terminates the Buchstab iterations after $r+1$ steps, and replaces all remaining sifting functions with $0$. When $r$ is odd, this produces a lower bound for $S(\mathscr{A}, z)$ and when $r$ is even, it produces an upper bound for $S(\mathscr{A}, z)$. Let $\omega(d)$ denote the number of prime factors of $d$. In the abstract framework of Definition 5.3.1, the Brun pure sieve is given by the sieve coefficients

$$\lambda_d = \begin{cases} \mu(d), & \text{if } \omega(d) \leqslant r, \\ 0, & \text{otherwise,} \end{cases}$$

which are upper bound sieve coefficients for $S(\mathscr{A}, z)$ if $r$ is even and a lower bound sieve coefficients if $r$ is odd.

The Brun pure sieve represents the first major improvement of the Legendre–Eratosthenes sieve. In 1915, Brun pushed this idea further by choosing truncation parameters that depend not only on the number of prime factors of $d$, but also on their size. This lead to a remarkable result known as the *Fundamental lemma of sieve theory*, the proof of which was essentially given by Brun in [24]. We give a modern formulation in Section 5.5. Brun's choice of sieve coefficients remains to this day a popular choice in a wide variety of applications. This motivated Rosser and Iwaniec to undertake a delicate optimisation of Brun's arguments, resulting in the main theorem of the beta sieve, which we discuss in Section 5.6.

Let $D, \beta \geqslant 1$ be parameters. We define functions $\mu^+, \mu^- : \mathbb{N} \to \{-1, 0, 1\}$, supported on integers dividing $P(z)$, as follows. We define

$$\mu^{\pm}(d) = \begin{cases} \mu(d), & \text{if } d \in \mathscr{D}^{\pm}, \\ 0, & \text{otherwise,} \end{cases} \tag{5.4.3}$$

where

$$\begin{aligned} \mathscr{D}^+ &= \{d = p_1 \cdots p_r : p_r < \cdots < p_1 < z,\ p_1 \cdots p_k p_k^{\beta} < D \text{ for all odd } k \leqslant r\}, \\ \mathscr{D}^- &= \{d = p_1 \cdots p_r : p_r < \cdots < p_1 < z,\ p_1 \cdots p_k p_k^{\beta} < D \text{ for all even } k \leqslant r\} \end{aligned} \tag{5.4.4}$$

with the convention that $1$ is contained in the sets $\mathscr{D}^{\pm}$, so that $\mu^{\pm}(1) = 1$.

**Lemma 5.4.3.** *Suppose that $z = D^{1/s}$ for some $s \geqslant 1$, and that $\beta \geqslant 1$. Then $\mu^+(d)$ (resp. $\mu^-(d)$) as defined above are upper (resp. lower) bound sieve coefficients for $S(\mathscr{A}, z)$ of level $D$.*

*Proof.* We begin by showing that $\mu^+$ and $\mu^-$ have level $D$. Suppose that $d = p_1 \cdots p_r$ and $\mu^+(d) \neq 0$. If $r$ is odd, then $p_1 \cdots p_r p_r^{\beta} < D$, from which it is

immediate that $p_1 \cdots p_r < D$. If $r$ is even, then we know that $p_1 \cdots p_{r-1} p_{r-1}^{\beta} < D$. However, since $\beta \geqslant 1$ and $p_{r-1} > p_r$ this also implies that $p_1 \cdots p_r < D$. We conclude that $\mu^+$ has level $D$. When $r \geqslant 2$, we have a similar argument for $\mu^-$. When $r = 1$, so $d$ is prime, we use that if $\mu^-(d) \neq 0$, then $d \mid P(z)$, so $d < z = D^{1/s}$. Since $s \geqslant 1$, this implies that $d < D$.

We now prove that $\mu^+(d)$ are upper bound sieve coefficients. (A similar argument can also be used to treat $\mu^-(d)$, and so we omit the details.) We have $\mu^+(1) = 1$ by definition, so it remains to show that $\sum_{d|n} \mu^+(d) \geqslant 0$ for all integers $n \mid P(z)$. We proceed by induction on the number of prime factors of $n$. Suppose that $\sum_{d|m} \mu^+(d) \geqslant 0$ and $\sum_{d|m} \mu^-(d) \leqslant 0$ for any $D \geqslant 1$ and any $m \mid P(z)$ with at most $r$ prime factors. Suppose we are given an integer $n \mid P(z)$ with $r+1$ prime factors $p_1 > \cdots > p_{r+1}$. We have

$$\begin{aligned} \sum_{d|n} \mu^+(d) &= \sum_{d|p_2 \cdots p_{r+1}} \mu^+(d) + \sum_{d|p_2 \cdots p_{r+1}} \mu^+(p_1 d) \\ &\geqslant \sum_{d|p_2 \cdots p_{r+1}} \mu^+(p_1 d), \end{aligned} \tag{5.4.5}$$

where the last line follows from the inductive hypothesis with $m = p_2 \cdots p_{r+1}$. Let $d = q_1 \cdots q_s$, for $q_1 > \cdots > q_s$. We observe that

$$\mu^+(p_1 d) = \begin{cases} -\mu(d), & \text{if } d \in \mathscr{D}, \\ 0, & \text{otherwise}, \end{cases} \tag{5.4.6}$$

where $\mathscr{D}$ is defined by the conditions

$$p_1 q_1 \cdots q_j q_j^{\beta} < D \text{ for all even } j \leqslant s, \text{ and } p_1^{\beta+1} < D.$$

If $p_1^{\beta+1} \geqslant D$, then we conclude that $\mu^+(p_1 d) = 0$ for all $d$, and so it trivially follows that (5.4.5) is at least $0$. Otherwise, we have $p_1^{\beta+1} < D$, and we recognise $\mathscr{D}$ as the set $\mathscr{D}^-$ from (5.4.4), but with the parameter $D$ replaced by $D/p_1$. The result now follows by applying the inductive hypothesis to (5.4.5) with $m = p_2 \cdots p_{r+1}$, and with the function $\mu^-$ as defined in (5.3.1), but with $D$ replaced by $D/p_1$. □

## 5.5 The Fundamental lemma of sieve theory

With the choice of sieve coefficients $\mu^+$ and $\mu^-$ from (5.4.3), we can actually obtain good estimates for $S(\mathscr{A}, z)$ even when $z$ is a small power of $D$. This is a substantial improvement on applying the Legendre sieve identity (5.2.2), where we can only take $z$ to be logarithmic in $D$.

We recall from (5.2.4) the notation

$$V(z) = \prod_{p|P(z)} (1 - g(p)).$$

Suppose that there is some $\kappa > 0$ and some $K > 0$ (depending on $\kappa$) such that $g(p)$ satisfies the bounds

$$V(w) \leqslant K\left(\frac{\log z}{\log w}\right)^{\kappa} V(z) \tag{5.5.1}$$

for all $2 \leqslant w \leqslant z$. The smallest value of $\kappa$ such that (5.5.1) holds is called the *sieve dimension*, and plays a key role in the analysis of the beta sieve. In practice, $E_p$ usually consists of the integers $n$ lying in some set of congruence classes modulo $p$. If there are $\kappa$ congruence classes defining each $E_p$, and if $P = \{\text{all primes}\}$, then typically we choose $g(p) = \frac{\kappa}{p}$. In this case, the sieve dimension is $\kappa$. For example, the sieve dimension in the Legendre–Eratosthenes sieve used in Section 5.1 to estimate $\pi(x)$ is $1$, and the sieve dimension in (5.2.5) for twin primes is $2$. Henceforth, $\kappa$ will always denote the sieve dimension.

**Lemma 5.5.1** (The Fundamental lemma of sieve theory)**.** *Let $z = D^{1/s}$. Suppose that $g$ satisfies (5.5.1) and that $s \geqslant 9\kappa + 1$. Then*

$$V^+(z) = \left(1 + e^{9\kappa - s}K^{10}\right)V(z)$$
$$V^-(z) = \left(1 - e^{9\kappa - s}K^{10}\right)V(z)$$

*and so*

$$S(\mathscr{A}, z) \leqslant XV(z)\left(1 + e^{9\kappa - s}K^{10}\right) + R^+(D, z)$$
$$S(\mathscr{A}, z) \geqslant XV(z)\left(1 - e^{9\kappa - s}K^{10}\right) + R^-(D, z),$$

*where $R^+(D, z)$ and $R^-(D, z)$ are as defined in (5.3.5).*

*Proof.* See [52, Lemma 6.8]. □

**Example 5.5.2.** Armed with the Fundamental lemma, we return to the problem of estimating $\pi(x)$ discussed in Section 5.1. Recalling Mertens' theorem (5.1.9), for the relevant sifting function $S(A, P, z)$ from (5.1.1), we see that $\kappa = 1$ and $K = 1$, so we may choose $s = 10$ in Lemma 5.5.1. Applying (5.3.6) and the bound $r_d = O(1)$, we have $R^+(D, z) \leqslant D$. We choose $D = x^{1-o(1)}$, so that $R^+(D, z)$ is negligible. Then for any $\epsilon > 0$, Lemma 5.5.1 yields

$$S(A, P, z) \leqslant xV(z)(1+e^{-1}+\epsilon) \leqslant \frac{(1 + e^{-1} + \epsilon)e^{-\gamma}x}{\log z} \leqslant 10e^{-\gamma}(1+e^{-1})\frac{x}{\log x}.$$

Therefore, in contrast to (5.1.10), we have now provided an upper bound sieve which can get within a constant factor of the true asymptotic $\pi(x) \sim \frac{x}{\log x}$.

Brun [24] observed that the Fundamental lemma provides a first step towards the twin prime conjecture. We end this section by proving a weaker form of the conjecture.

**Corollary 5.5.3.** *There are infinitely many integers $n$ such that $n$ and $n+2$ both have fewer than $20$ prime factors.*

*Proof.* We use the setup from (5.2.5). We choose $g(p) = 2/p$, so that for squarefree integers $d$, we have $g(d) = \frac{\tau(d)}{d}$, where $\tau(d)$ denotes the divisor function. We claim that (5.5.1) holds with $\kappa = 2$ and $K = 1$. To see this, we apply a variant of Mertens' theorem [71, Equation (2.15)], which states that

$$\sum_{p \leqslant x} \frac{1}{p} = \log\log x + c + O((\log x)^{-1}) \tag{5.5.2}$$

for some constant $c$. Below, we allow $c, C$ to denote explicit constants which may vary from line to line. We obtain

$$\log V(z) = \log\left(\prod_{p<z}\left(1-\frac{2}{p}\right)\right) = \sum_{p<z}\log\left(1-\frac{2}{p}\right) = \sum_{p<z}\left(-\frac{2}{p}+T(p)\right), \tag{5.5.3}$$

where $T(p) = \log(1-2/p) + 2/p$. Since $T(p) = O(p^{-2})$, the sum $\sum_p T(p)$ converges to some constant $c$, and moreover $\sum_{p>z} T(p) = O(z^{-1})$. Combining with (5.5.2), we obtain

$$\log V(z) = -2\log\log z + c + O\left(\frac{1}{\log z}\right).$$

Exponentiating, we conclude that

$$V(z) \sim \frac{c}{(\log z)^2}\left(\sum_{k=0}^{\infty}\frac{(C\log z)^{-k}}{k!}\right) \sim \frac{c}{(\log z)^2}\left(1+O\left(\frac{1}{\log z}\right)\right), \tag{5.5.4}$$

which establishes the claim.

We observe that

$$|\mathscr{A}_d| = \#\{1 \leqslant n \leqslant x : n \equiv 0 \text{ or } -2 \pmod p \text{ for all } p \mid d\},$$

so $|\mathscr{A}_d|$ counts integers $n \leqslant x$ in $\tau(d)$ congruence classes modulo $d$. Therefore, we have the estimate $|\mathscr{A}_d| = g(d) + O(\tau(d))$, so $r(d) = \tau(d) = O_\epsilon(d^\epsilon)$ by the trivial bound for the divisor function. We obtain the level of distribution result

$$|R^-(D,z)| \leqslant \sum_{\substack{d \leqslant D \\ d \text{ squarefree}}} |r_d| \ll D^{1+\epsilon},$$

and hence $R^-(D,z)$ is negligible provided that $D \ll x^{1-2\epsilon}$. In Lemma 5.5.1, we may choose $s = 9\kappa + 1 = 19$. Then $(1 - e^{9\kappa - s}K^{10}) > 0$. For $\epsilon$ sufficiently

small and $x$ sufficiently large, we have $z = D^{1/19} \geqslant x^{1/20}$. Applying the lower bound sieve from Lemma 5.5.1, we conclude that

$$S(\mathscr{A}, x^{1/20}) \geqslant S(\mathscr{A}, z) \gg xV(z) \gg \frac{x}{(\log x)^2}. \tag{5.5.5}$$

If $n \leqslant x-2$ and one of $n$ or $n+2$ has at least $20$ prime factors, then necessarily one of these factors must be $\leqslant x^{1/20}$, and so $S(\mathscr{A}, x^{1/20})$ counts integers $n \leqslant x-2$ such that both $n$ and $n+2$ have fewer than $20$ prime factors. This quantity is in particular unbounded as $x \to \infty$ by (5.5.5). □

## 5.6 The main theorem of the beta sieve

In this section, we discuss the main theorem of the beta sieve, first introduced by Rosser and Iwaniec, which is an improvement of the fundamental lemma (Lemma 5.5.1). A key refinement made in their result is a careful optimisation of the parameter $\beta$ used to define the sieve coefficients from (5.4.3). It turns out that when $0 < \kappa \leqslant \frac{1}{2}$, it is best to simply choose $\beta = 1$, whilst for $\kappa > \frac{1}{2}$, larger values of $\beta$ produce sharper results. The case $\kappa = 1$ has received particular attention, and is known as the *linear sieve*. For the linear sieve, the optimal choice is $\beta = 2$. More generally, the precise choice of the parameter $\beta$ made by Rosser and Iwaniec is given in [52, Section 11.3], and some numerical values are given in [52, Section 11.19]. For the remainder of this section, we assume that $\beta$ is as defined in [52, Section 11.19].

In place of (5.5.1), we now make a slightly stronger assumption on the regularity of $g$, namely that there is a constant $L > 0$ such that

$$V(w) \leqslant \left(\frac{\log z}{\log w}\right)^{\kappa} \left(1 + \frac{L}{\log w}\right) V(z) \tag{5.6.1}$$

for all $2 \leqslant w \leqslant z$.

The main theorem of the beta sieve is stated in terms of continuous real-valued functions $f(s), F(s)$ in the variable $s = \log D / \log z$, satisfying the system of delay differential equations

$$\begin{cases} (s^{\kappa} F(s))' = \kappa s^{\kappa-1} f(s-1), & \text{if } s > \beta + 1, \\ (s^{\kappa} f(s))' = \kappa s^{\kappa-1} F(s-1), & \text{if } s > \beta, \end{cases} \tag{5.6.2}$$

with initial conditions

$$\begin{cases} s^{\kappa} F(s) = A, & \text{if } \beta - 1 \leqslant s \leqslant \beta + 1, \\ s^{\kappa} f(s) = B, & \text{if } s = \beta, \end{cases} \tag{5.6.3}$$

for constants $A, B$ determined by $\kappa$ and $\beta$. For $0 < \kappa \leqslant \frac{1}{2}$, $A$ and $B$ are given in [52, Equations (11.61), (11.62)], whilst for $\kappa > \frac{1}{2}$ we have $B = 0$ and $A$ is given by [52, Equations (11.44), (11.57)].

**Theorem 5.6.1** (Main theorem of the beta sieve)**.** *Let $g(d)$ be a multiplicative function supported on squarefree integers $d$ such that (5.6.1) holds for some $\kappa > 0$. Let $z = D^{1/s}$ and let $R^{\pm}(D, z)$ be as defined in (5.3.5). Then for $s \geqslant \beta - 1$, we have*

$$S(\mathscr{A}, z) \leqslant XV(z)\left\{F(s) + O\left((\log D)^{-1/6}\right)\right\} + R^{+}(D, z), \tag{5.6.4}$$

*and for $s \geqslant \beta$, we have*

$$S(\mathscr{A}, z) \geqslant XV(z)\left\{f(s) + O\left((\log D)^{-1/6}\right)\right\} + R^{-}(D, z), \tag{5.6.5}$$

*for implied constants depending only on $\kappa$ and $L$.*

*Proof.* See [52, Theorem 11.13]. □

We see that $F(s)$ and $f(s)$ play the role of the functions $1 + e^{9\kappa - s}K^{10}$ and $1 - e^{9\kappa - s}K^{10}$ appearing in the Fundamental lemma (Lemma 5.5.1), which converge to $1$ exponentially as $s$ grows. One improvement of the beta sieve over Lemma 5.5.1 is that $F(s), f(s)$ converge to $1$ even more rapidly than this [52, Equation (11.134)]. Moreover, the assumptions $s \geqslant \beta - 1$ and $s \geqslant \beta$ are typically much weaker than the assumption $s \geqslant 9\kappa + 1$ in Lemma 5.5.1, which means that we can often obtain estimates when $z$ is a larger power of $D$ than allowed by the fundamental lemma. In fact, in Chapter 8, we apply upper and lower bound beta sieves with $z = D$, so that $s = 1$. The sieve dimensions will be $\kappa < 1/2$ for the lower bound sieve and $\kappa \in (0, 1)$ for the upper bound sieves. Consequently, in our application, we have $\beta \in [1, 2)$ and $F(s) = F(1) = A, f(s) = f(1) = B$ by the initial conditions given in (5.6.3).

Whilst the beta sieve will be sufficient for our purposes, some of the ideas in this chapter can be pushed even further. The beta sieve makes use of estimates for $|\mathscr{A}_d|$ by a multiplicative function $g$, which is known as *Type I* arithmetic information. More refined sieves have been developed which additionally exploit *Type II* arithmetic information involving the estimation of certain bilinear sums. This approach was successfully employed in the groundbreaking work of Friedlander and Iwaniec, which establishes that there are infinitely many primes of the form $x^2 + y^4$ [51], and Maynard, who proved that for any $a \in \{0, \dots, 9\}$, there are infinitely many primes whose decimal expansion does not feature the digit $a$ [87].

## 5.7 Sieving prime factors from binary forms

In this section, we discuss the main auxiliary sieve results we require in order to prove Theorems A and C. Let $\mathscr{P}$ be a set of primes. We assume that $\mathscr{P}$ is disjoint from a finite set of primes $S$. Suppose that $f(x, y)$ is a binary form

with nonzero discriminant, and $N \geqslant 1$ is a parameter, which we are free to take sufficiently large. Let $\mathscr{B} \subseteq [-1,1]^2$ be a measurable set of volume $\gg 1$, whose boundary is a continuous closed curve with piecewise continuous derivatives, and with perimeter $\ll 1$. We denote by $\mathscr{B}N$ the set $\{(Nx, Ny) : (x,y) \in \mathscr{B}\}$. In the applications in Chapter 8, we shall make the choice

$$\mathscr{B} = \left\{(x,y) \in (0,1]^2 : \left|\frac{x}{y} - r\right| < \xi\right\}, \tag{5.7.1}$$

for a fixed real number $r > 0$ and a small parameter $\xi > 0$.

Let $\Delta$ be an integer with only prime factors in $S$ and let $a_0, b_0 \in \mathbb{Z}/\Delta\mathbb{Z}$. We consider the quantity

$$S(\mathscr{P}, \mathscr{B}, N) = \#\left\{(a,b) \in \mathscr{B}N \cap \mathbb{Z}^2 : \begin{array}{c} a \equiv a_0, b \equiv b_0 \pmod{\Delta} \\ p \mid f(a,b) \implies p \notin \mathscr{P} \end{array}\right\}. \tag{5.7.2}$$

We explain how this fits into the context of the abstract sieve problem from (5.2.1). We choose $\mathscr{A} = (a_n)$ to be the number of representations of $n$ as $f(a,b) = n$ for $(a,b) \in \mathscr{B}N \cap \mathbb{Z}^2$ satisfying $a \equiv a_0, b \equiv b_0 \pmod{\Delta}$. For each prime $p \in \mathscr{P}$ we define the set $E_p = \{n \in \mathbb{Z} : p \mid n\}$. We note that due to the assumption $(a,b) \in \mathscr{B}N \cap \mathbb{Z}^2$, the sequence $\mathscr{A}$ has finite support; Namely, $a_n \neq 0$ implies that $n \ll N^{\deg f}$ for an implied constant depending only on $f$. Let $x$ denote the largest prime factor of $f(a,b)$ for $(a,b) \in \mathscr{B}N \cap \mathbb{Z}^2$. Then $x \ll N^{\max(\deg f_i)}$, where the maximum is over the irreducible factors $f_i$ of $f$. Therefore, in the notation of (5.2.1), the quantity from (5.7.2) is equal to $S(\mathscr{A}, \mathscr{P}, x)$.

We would like to find a lower bound for $S(\mathscr{A}, \mathscr{P}, x)$. In practice, this is not possible directly, so we first apply the Buchstab identity from (5.4.1) to obtain

$$S(\mathscr{A}, \mathscr{P}, x) = S(\mathscr{A}, \mathscr{P}, N^\gamma) - \sum_{N^\gamma < p \leqslant x} S(\mathscr{A}_p, \mathscr{P}, p),$$

where $\gamma < 1$ is a parameter, and we recall that $\mathscr{A}_p$ denotes the sequence $(a_n 1_{E_p}(n))$. It turns out to be useful to further subdivide $S(\mathscr{A}_p, \mathscr{P}, p)$ into quantities $S(\mathscr{A}_p^{(i)}, \mathscr{P}, p)$, which keep track of the particular irreducible factor $f_i$ of $f$ that the prime $p$ divides. To this end, we factorise $f$ as

$$f(x,y) = \prod_{i=0}^{m} f_i(x,y) \prod_{i=m+1}^{k} f_i(x,y), \tag{5.7.3}$$

where $f_i(x,y)$ are linear forms for $1 \leqslant i \leqslant m$, and forms of degree $\geqslant 2$ for $m+1 \leqslant i \leqslant k$. If $y \mid f(x,y)$, then we define $f_0(x,y) = y$, and otherwise we let $f_0(x,y) = 1$. The assumption that $f$ has nonzero discriminant implies that it is squarefree, so $y \nmid f_i(x,y)$ for all $i \geqslant 1$.

In Section 8.2, we apply the beta sieve to obtain a lower bound for the sifting function $S(\mathscr{A}, \mathscr{P}, N^\gamma)$, and an upper bound for each $S(\mathscr{A}_p^{(i)}, \mathscr{P}, p)$. In our main sieve results, we assume that the (natural) density of $\mathscr{P}$ and the average number of roots of $f_i$ modulo $p$ for $p \in \mathscr{P}$ exist for all $i \in \{1, \dots, k\}$. In fact, we need slightly more quantitative assumptions, which we now state more precisely.

For $i \in \{0, \dots, k\}$, we define

$$\nu_i(p) = \#\{[x : y] \in \mathbb{P}^1(\mathbb{F}_p) : f_i(x, y) \equiv 0 \pmod p\}, \tag{5.7.4}$$
$$\nu(p) = \#\{[x : y] \in \mathbb{P}^1(\mathbb{F}_p) : f(x, y) \equiv 0 \pmod p\}. \tag{5.7.5}$$

Let $\mathscr{P}_{\leqslant x} = \{p \in \mathscr{P} : p \leqslant x\}$. For all $i \in \{0, \dots, k\}$, we need to assume that $\mathscr{P}$ has the following properties, for some $\alpha, \theta_i > 0$ and any $A \geqslant 1$.

$$\sum_{p \in \mathscr{P}_{\leqslant x}} 1 = \alpha \pi(x) \left(1 + O_A\left((\log x)^{-A}\right)\right), \tag{5.7.6}$$
$$\sum_{p \in \mathscr{P}_{\leqslant x}} \nu_i(p) = \alpha \theta_i \pi(x) \left(1 + O_A\left((\log x)^{-A}\right)\right). \tag{5.7.7}$$

The reason we require explicit error terms in (5.7.6) and (5.7.7) is so that the sieve dimension $\kappa$ exists and satisfies (5.6.1). We note that $\theta_0 = 1$ if $f_0(x, y) = y$, and $\theta_0 = 0$ if $f_0(x, y) = 1$. Additionally, from (5.7.7) and the assumption that $f$ has nonzero discriminant, we have

$$\sum_{p \in \mathscr{P}_{\leqslant x}} \nu(p) = \alpha \theta \pi(x) \left(1 + O_A\left((\log x)^{-A}\right)\right), \tag{5.7.8}$$

where $\theta = \theta_0 + \cdots + \theta_k$.

We are now ready to state the main sieve results from Chapter 8.

**Theorem 5.7.1.** *Let $f(x, y)$ be a binary form consisting of distinct irreducible factors, all of degree at most $2$. Then there exists a finite set of primes $S_0$, depending on $f$, such that the following holds:*

*Let $S$ be a finite set of primes containing $S_0$. Let $\Delta$ be an integer with only prime factors in $S$, and let $a_0, b_0 \in \mathbb{Z}/\Delta\mathbb{Z}$. Let $\mathscr{P}$ be a set of primes disjoint from $S$ and satisfying (5.7.6) and (5.7.7) for some $\alpha, \theta_i > 0$. Assume that $\alpha\theta < 0.39006....$ Then $S(\mathscr{A}, \mathscr{P}, x) > 0$ for sufficiently large $N$.*

We also have a similar result when $f$ may contain irreducible factors of degree up to $3$, but with a less general sifting set $\mathscr{P}$.

**Theorem 5.7.2.** *Let $f(x, y)$ be a binary form consisting of distinct irreducible factors, all of degree at most $3$. Then there exists a finite set of primes $S_0$, depending on $f$, such that the following holds:*

*Let $S$ be a finite set of primes containing $S_0$. Let $\Delta$ be an integer with only prime factors in $S$, and let $a_0, b_0 \in \mathbb{Z}/\Delta\mathbb{Z}$. Let $\mathscr{P}$ be a set of primes satisfying $\mathscr{P} \subseteq \{p \notin S : p \equiv 1 \pmod q\}$ for some prime $q \geqslant (3.08825...) \deg f + 1$. Then $S(\mathscr{A}, \mathscr{P}, x) > 0$ for $N$ sufficiently large.*

## 5.8 The Chebotarev density theorem

In this section, we discuss the *Chebotarev density theorem*, which can be viewed as a vast generalisation of Dirichlet's theorem on primes in arithmetic progressions. In Chapter 8, we apply the sieve results from Theorems 5.7.1 and 5.7.2 with a choice of $\mathscr{P}$ related to the splitting of primes in the extension $K/\mathbb{Q}$ used to define the norm form in (1.1.1). Therefore, the densities of these splitting types will be important in order to compute the sieve dimensions of the sifting functions $S(\mathscr{A}_p^{(i)}, \mathscr{P}, p)$ introduced in Section 5.7. Our discussion of the Chebotarev density theorem is based on [73, Sections 3.1, 3.2].

Let $K$ be a number field with degree $n$ over $\mathbb{Q}$. Let $p$ be a prime, unramified in $K/\mathbb{Q}$. We can factorise the ideal $(p)$ as $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are distinct prime ideals in $\mathscr{O}_K$. The *splitting type* of $p$ in $K/\mathbb{Q}$ is the partition $(a_1, \dots, a_r)$ of $n$, where $a_i$ is the inertia degree of $\mathfrak{p}_i$, i.e., $N(\mathfrak{p}_i) = p^{a_i}$. Equivalently, the splitting type is the list of degrees of the irreducible factors of the minimum polynomial of $K/\mathbb{Q}$, when factorised modulo $p$.

Suppose first that $K/\mathbb{Q}$ is Galois, with Galois group $G$. Then $G$ acts transitively on $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. Fix $i \in \{1, \dots, r\}$. The *Decomposition* group $D_{\mathfrak{p}_i}$ is the stabilizer of $\mathfrak{p}_i$ under this action. Note that $D_{\mathfrak{p}_i}$ is cyclic, and there is an isomorphism

$$\psi_i : D_{\mathfrak{p}_i} \to \mathrm{Gal}((\mathscr{O}_K/\mathfrak{p}_i)/(\mathbb{Z}/(p))).$$

The group $\mathrm{Gal}((\mathscr{O}_K/\mathfrak{p}_i)/(\mathbb{Z}/(p)))$ is generated by the *Frobenius element* defined by $x \mapsto x^p$, which has order $a_i$. Let $\sigma_i$ denote the preimage of the Frobenius element under $\psi_i$. We define the *Artin symbol*

$$\left[\frac{K/\mathbb{Q}}{p}\right] = \{\sigma_1, \dots, \sigma_r\}.$$

The Artin symbol is a conjugacy class of $G$. Indeed, all the $\mathfrak{p}_i$'s lie in the same orbit of $G$ (there is only one orbit as $G$ acts transitively). Stabilisers of points in the same orbit of an action are conjugate, and so all of the $D_{\mathfrak{p}_i}$ are conjugate.

We now come to the statement of the Chebotarev density theorem. For a conjugacy class $C$ of $G$, we let $\pi_C(x)$ denote the number of primes $p \leqslant x$

whose Artin symbol is equal to $C$. We define the (natural) *density* of a set of primes $\mathscr{P}$ to be

$$\lim_{x\to\infty}\left(\frac{\#\{p\in\mathscr{P}:p\leqslant x\}}{\pi(x)}\right),$$

if such a limit exists.

**Lemma 5.8.1** (Chebotarev density theorem)**.** *Let $C$ be a conjugacy class of $G$. The density of primes $p$ for which the Artin symbol is equal to $C$ is $\#C/\#G$.*

In Chapter 8, we shall also need an effective version of the Chebotarev density theorem in order to establish the conditions (5.7.6) and (5.7.7) required to apply Theorem 5.7.1. The following lemma is a straightforward consequence of a more refined result due to Lagarias and Odlyzko [77, Theorem 1].

**Lemma 5.8.2** (Effective Chebotarev density theorem)**.** *For any $A\geqslant 1$, we have*

$$\pi_C(x)=\pi(x)\left(\frac{\#C}{\#G}+O_A((\log x)^{-A})\right),$$

*where the implied constant may depend on $K, C$ and $A$.*

We now consider the non-Galois case. As above, let $(p)=\mathfrak{p}_1\cdots\mathfrak{p}_r$ be the factorisation of $(p)$ in $\mathscr{O}_K$. Let $\widehat{K}$ denote the Galois closure of $K$, and let $G=Gal(\widehat{K}/\mathbb{Q})$. This time, there is no action of $G$ on $\{\mathfrak{p}_1,\dots,\mathfrak{p}_r\}$, because the $\mathfrak{p}_i$'s could split further in $\widehat{K}$, and elements of $G$ could permute prime factors which are above different $\mathfrak{p}_i$'s.

To get around this, we define $H=Gal(\widehat{K}/K)$, and instead consider the action of $G$ on the set $X$ of left cosets of $H$ in $G$. For an element $\sigma\in G$, the cyclic group $\langle\sigma\rangle$ generated by $\sigma$ acts by left multiplication on $X$. The sizes of the orbits of this action form a partition of $[G:H]=[K:\mathbb{Q}]=n$. Moreover, it can be checked that conjugate elements of $G$ give the same orbit sizes, so we can associate a single partition of $n$ with each Artin symbol $\left[\frac{\widehat{K}/\mathbb{Q}}{p}\right]$.

**Example 5.8.3.** Keeping the notation from above, we suppose that $G=S_n$ and $K=\mathbb{Q}(\alpha)$. We label the roots of $g$ as $(1,\dots,n)$, where $1$ corresponds to $\alpha$. Then $H$ consists of all automorphisms of $\widehat{K}$ fixing $K$, which corresponds to the permutations of $\{1,\dots,n\}$ fixing $1$. We have $X=\{H,(12)H,\dots,(1n)H\}$. For any $\sigma\in G$, the action of $\langle\sigma\rangle$ on $X$ is equivalent to the action of $\langle\sigma\rangle$ on $\{1,\dots,n\}$ via the obvious identification of $(1j)H$ with $j$.

The following fact relating the partition of $n$ given by the Artin symbol $\left[\frac{\widehat{K}/\mathbb{Q}}{p}\right]$ to the splitting type of $p$ can be found in [73, Ch. 3, Proposition 2.8].

**Lemma 5.8.4.** *Let $\sigma \in \left[\frac{\widehat{K}/\mathbb{Q}}{p}\right]$. Then $p$ has splitting type $(a_1, \dots, a_r)$ in $K/\mathbb{Q}$ if and only if the action of $\langle\sigma\rangle$ on $X$ has orbit sizes $(a_1, \dots, a_r)$.*

Let $K = \mathbb{Q}(\alpha)$, and let $f$ be the minimum polynomial of $\alpha$. We can also view $\langle\sigma\rangle$ as acting on the set of $n$ roots of $f$ in $\widehat{K}$. By definition of $H$, we have that $\sigma\alpha = \sigma'\alpha$ if and only if $\sigma H = \sigma' H$. It follows that the orbit sizes of $\langle\sigma\rangle$ acting on $X$ are the same as the orbit sizes of $\langle\sigma\rangle$ acting on the roots of $f$, which in turn are the cycle lengths of $\sigma$ viewed as a permutation on the $n$ roots of $f$ in $\widehat{K}$. The set of $\sigma \in G$ with cycle lengths $(a_1, \dots, a_r)$ is a union $\bigcup_{i=1}^{s} C_i$ of conjugacy classes $C_i$. We may now apply Lemma 5.8.2 to each of these conjugacy classes separately. Putting everything together, we have the following result on densities of splitting types in non-Galois extensions.

**Lemma 5.8.5.** *Let $K$ be a number field of degree $n$ over $\mathbb{Q}$, and let $\widehat{K}$ denote its Galois closure. Let $G = Gal(\widehat{K}/\mathbb{Q})$, viewed as a permutation group on the $n$ roots of the minimum polynomial of $K$ in $\widehat{K}$. For a partition $\mathbf{a} = (a_1, \dots, a_r)$ of $n$, let $\mathscr{P}(\mathbf{a})$ denote the set of primes with splitting type $\mathbf{a}$ in $K/\mathbb{Q}$, and let $T(\mathbf{a})$ denote the proportion of elements of $G$ with cycle shape $\mathbf{a}$. Then for any $A \geqslant 1$,*

$$\#\{p \in \mathscr{P}(\mathbf{a}) : p \leqslant x\} = \pi(x)\left(T(\mathbf{a}) + O_A((\log x)^{-A})\right),$$

*where the implied constant depends only on $K, \mathbf{a}$ and $A$.*

The quantity $T(\mathbf{a})$ is certainly not a property of $G$ as an abstract group, but depends on the way we represent $G$ as a permutation group. Care must be taken to ensure $G$ is viewed as acting on the roots of the minimum polynomial of $K$, as the following example demonstrates.

**Example 5.8.6.** Suppose that $K$ is a biquadratic extension $\mathbb{Q}(\sqrt{a}, \sqrt{b})$. Then $K$ is the splitting field of $f(t) = (t^2 - a)(t^2 - b)$, and the Galois group $G = \mathrm{G}al(K/\mathbb{Q})$ acts naturally on the roots $\{\sqrt{a}, -\sqrt{a}, \sqrt{b}, -\sqrt{b}\}$ of $f$ over $\overline{\mathbb{Q}}$. To ease notation, we identify this set with $\{1, 2, 3, 4\}$. Viewed as a permutation group on this set, $G \cong G_1 := \{\mathrm{id}, (12), (34), (12)(34)\}$.

On the other hand, it is easy to check that $K = \mathbb{Q}(\sqrt{a} + \sqrt{b})$, and that $\sqrt{a} + \sqrt{b}$ has minimum polynomial $g(t) = (t^2 - a - b)^2 - 4ab$, which has the four roots $\pm\sqrt{a} \pm \sqrt{b}$. Identifying this set with $\{1, 2, 3, 4\}$, we have $G \cong G_2 := \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.

Whilst $G_1, G_2$ are both isomorphic to the Klein four group $C_2 \times C_2$, clearly the cycle shapes in $G_1$ and $G_2$ occur with different frequencies. For example, $G_1$ features two elements $(12)$ and $(34)$ of cycle shape $(2, 1, 1)$, whilst $G_2$ features none. When applying Lemma 5.8.5, we must use $G_2$. (In general, if $K/\mathbb{Q}$ is Galois of degree $n$, all splitting types take the form $(a, \dots, a)$ for some

$a \mid n$, which demonstrates that our representation of $G$ as a permutation group should not feature cycle shapes $(2,1,1)$.) We conclude that the splitting types $(1,1,1,1)$ and $(2,2)$ appear with density $1/4$ and $3/4$ respectively in $K/\mathbb{Q}$.

**Example 5.8.7.** When $[K:\mathbb{Q}] = n$ and $Gal(\widehat{K}/\mathbb{Q}) = S_n$, any partition $\mathbf{a}$ of $n$ is realised as the splitting type in $K/\mathbb{Q}$ for a positive proportion of primes $p$, and by Lemma 5.8.5, this proportion is $T(\mathbf{a})$. We write $\mathbf{a} = (b_1)^{m_1} \cdots (b_k)^{m_k}$ for pairwise distinct $b_1, \ldots, b_k$ to mean that $\mathbf{a}$ has exactly $m_i$ cycles of length $b_i$ for every $i$. By the well-known formula for the number of permutations with cycle shape $\mathbf{a}$, we have

$$T(\mathbf{a}) = \frac{1}{b_1^{m_1} \cdots b_k^{m_k} m_1! \cdots m_k!}. \tag{5.8.1}$$

**Example 5.8.8.** We end this section with one more example, which we shall return to in Chapter 8. Let $q$ be a prime and let $K = \mathbb{Q}(2^{1/q})$. Then $K/\mathbb{Q}$ has degree $q$, and the minimum polynomial of $2^{1/q}$ is $x^q - 2$. The extension $K/\mathbb{Q}$ is not Galois, and so we now compute $G = Gal(\widehat{K}/\mathbb{Q})$. The roots of $x^q - 2$ are $\{\beta, \beta\omega, \ldots, \beta\omega^{q-1}\}$, where $\omega$ is a primitive $q$th root of unity and $\beta$ is the real root of $x^q - 2$. We identify these roots with $\{0, \ldots, q-1\}$ in the obvious way. An element $\sigma \in G$ is determined by the image of $0$ and $1$, since $\beta, \beta\omega$ multiplicatively generate all the other roots. Therefore, $\sigma$ takes the form $\sigma_{a,b} : x \mapsto ax + b$ for some $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$. Conversely, the maps $\sigma_{1,b}$ correspond to the $q$ different embeddings $K \hookrightarrow \widehat{K}$, and the maps $\sigma_{a,0}$ for $a \in \mathbb{F}_q^\times$ are elements of $Gal(\widehat{K}/K) \leqslant G$. Combining these, we see that $\sigma_{a,b} \in G$ for any $a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q$. We conclude that $G \cong \mathrm{AGL}(1,q)$, the group of affine linear transformations on $\mathbb{F}_q$.

When $a = 1$ and $b = 0$, $\sigma_{a,b}$ is the identity. When $a = 1$ and $b \neq 0$, $\sigma_{a,b}$ is a $q$-cycle. In the remaining case $a \neq 1$, the equation $ax + b = x$ has a unique solution $x \in \mathbb{F}_q$, and so $\sigma_{a,b}$ has one fixed point, which we denote by $r$. The subgroup $G_r$ of $G$ consisting of those $\sigma_{a,b}$ which fix $r$ is a cyclic group of order $q-1$ acting on $\{0, \ldots, q-1\} \backslash \{r\}$. (This can be proven directly, or alternatively by applying the fundamental theorem of Galois theory, which tells us that $G_r = Gal(\widehat{K}/\mathbb{Q}(\beta\omega^r))$.) Let $\varphi$ denote the Euler totient function. We recall that a cyclic group of order $k$ has $\varphi(d)$ elements of order $d$ for every $d \mid k$. Therefore, the number of elements of $G_r$ with cycle shape $(d, \ldots, d) = (d)^{(q-1)/d}$ is $\varphi(d)$ for every $d \mid (q-1)$. Applying Lemma 5.8.5, we deduce the following densities of splitting types in $K/\mathbb{Q}$.

| Splitting type | Density |
|---|---|
| $(1,\dots,1)$ | $1/q(q-1)$ |
| $(q)$ | $1/q$ |
| $(1,d,\dots,d)$ for $d \mid (q-1), d>1$ | $\varphi(d)/q$ |

Table 5.2: Distribution of splitting types in $\mathbb{Q}(2^{1/q})/\mathbb{Q}$

We remark that the number $2$ can be replaced by any positive integer $r$ such that $x^q - r$ is irreducible in the above example, and the Galois group and density of splitting types remain unchanged. A necessary and sufficient condition for irreducibility of $x^q - r$ is given in [74, Theorem 8.16].

## 5.9 A level of distribution result

Crucial to the success of the beta sieve in proving Theorems 5.7.1 and 5.7.2 is a good level of distribution result, which provides an approximation of the quantities

$$\#\{(a,b) \in \mathscr{B}N \cap \mathbb{Z}^2 : p \mid f_i(a,b), d \mid f(a,b)\}$$

by multiplicative functions, at least on average over $p$ and $d$. (Here, and throughout this section, we adopt the notation from Section 5.7.) In this section, we provide such an estimate, following similar arguments to [40, Lemma 3.3], which were developed by Daniel in order to study the divisor function on binary forms. We slightly generalise the setup as follows:

Let $g_1, g_2$ be binary forms with nonzero discriminants. Throughout this section, we fix $S, \Delta, a_0$ and $b_0$, and denote the congruence condition $a \equiv a_0, b \equiv b_0 \pmod{\Delta}$ by $C(a,b)$. We also assume that $S$ contains all primes dividing the discriminants of $g_1$ and $g_2$. All implied constants are allowed to depend only on the degrees of $g_1$ and $g_2$ and on $\epsilon$.

Let $\mathscr{R}$ be a compact region of $\mathbb{R}^2$ whose boundary is a continuous closed curve with piecewise continuous derivatives. In this section, in all maximums involving $\mathscr{R}$, it is assumed that $\mathscr{R}$ satisfies these properties. For $d_1, d_2 \in \mathbb{N}$, we define

$$R(d_1,d_2) = \#\{(a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : C(a,b), d_1 \mid g_1(a,b), d_2 \mid g_2(a,b)\}, \quad (5.9.1)$$

$$\varrho(d_1,d_2) = \#\{(a,b) \pmod{d_1 d_2} : d_1 \mid g_1(a,b), d_2 \mid g_2(a,b)\}. \quad (5.9.2)$$

We denote by $\mathrm{Vol}(\mathscr{R})$ and $P(\mathscr{R})$ the volume and perimeter of $\mathscr{R}$ respectively. In what follows, we let $d = d_1 d_2$, and we assume that $\gcd(d_1,d_2) = \gcd(d,\Delta) = 1$. The main aim of this section is to prove the following proposition.

**Proposition 5.9.1.** *For any $D_1, D_2 > 0$ and any $\epsilon > 0$, we have*

$$\sum_{\substack{d_1 \leqslant D_1, d_2 \leqslant D_2 \\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}} \max_{P(\mathscr{R}) \leqslant N} \left| R(d_1,d_2) - \frac{\varrho(d_1,d_2)\operatorname{Vol}(\mathscr{R})}{d^2\Delta^2} \right| \ll (D_1D_2)^{\epsilon}(D_1D_2 + N(D_1D_2)^{1/2} + ND_2).$$

We obtain the following level of distribution result.

**Corollary 5.9.2.** *Let $\mathscr{B} \subseteq [-1,1]^2$ be as in Section 5.7, and let $\mathscr{R} = \mathscr{B}N$. Then for any $\epsilon > 0$, there exists $\delta > 0$ such that for any $D_1, D_2 > 0$ with $D_2 \ll N^{1-\epsilon}$ and $D_1D_2 \ll N^{2-\epsilon}$ , we have*

$$\sum_{\substack{d_1 \leqslant D_1, d_2 \leqslant D_2 \\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}} \left| R(d_1,d_2) - \frac{N^2\varrho(d_1,d_2)\operatorname{Vol}(\mathscr{B})}{d^2\Delta^2} \right| \ll N^{2-\delta}. \tag{5.9.3}$$

Proposition 5.9.1 and Corollary 5.9.2 are generalisations of Irving's results from [69, Section 3], which can be recovered by taking $g_1(x,y) = f(x,y)$ to be the cubic form Irving considered, and $g_2(x,y) = yf(x,y)$. We remark that Daniel's argument from [40, Lemma 3.3] on which our method of proof is based is more delicate, keeping track of powers of $\log N$ in place of factors of $N^{\epsilon}$, and Corollary 5.9.2 could be similarly refined. However, this does not appear to yield any advantage for our applications in Chapter 8.

We now commence with the proof of Proposition 5.9.1. We introduce the quantities $R^*(d_1,d_2)$ and $\varrho^*(d_1,d_2)$, which are defined similarly to $R(d_1,d_2)$ and $\varrho(d_1,d_2)$ but with the added condition $\gcd(a,b,d) = 1$. We write $(a_1,b_1) \sim (a_2,b_2)$ if there exists an integer $\lambda$ such that $(a_1,b_1) \equiv \lambda(a_2,b_2) \pmod{d}$. This forms an equivalence relation on points $(a,b) \in \mathbb{Z}^2$ with $\gcd(a,b,d) = 1$. Moreover, the properties $g_1(a,b) \equiv 0 \pmod{d_1}$ and $g_2(a,b) \equiv 0 \pmod{d_2}$ are preserved under this equivalence. We may therefore define

$$\mathscr{U}(d_1,d_2) = \left\{ a,b \pmod{d} : \begin{array}{l} \gcd(a,b,d) = 1 \\ d_1 \mid g_1(a,b), d_2 \mid g_2(a,b) \end{array} \right\} \Big/ \sim .$$

For $\mathscr{C} \in \mathscr{U}(d_1,d_2)$, we define

$$\Lambda(\mathscr{C}) = \{y \in \mathbb{Z}^2 : y \equiv \lambda(a,b) \pmod{d} \text{ for some } (a,b) \in \mathscr{C}, \lambda \in \mathbb{Z}\}.$$

It is easy to check that $\Lambda(\mathscr{C})$ is a lattice in $\mathbb{Z}^2$, and its set of primitive points is $\mathscr{C}$. For $e \in \mathbb{Z}$, we define

$$\Lambda(\mathscr{C}, e) = \{(a,b) \in \Lambda(\mathscr{C}) : e \mid \gcd(a,b)\}.$$

By Möbius inversion, we have

$$R^*(d_1,d_2)=\sum_{\mathscr{C}\in\mathscr{U}(d_1,d_2)}\sum_{e|d}\mu(e)\#\{(a,b)\in\mathscr{R}\cap\Lambda(\mathscr{C},e):C(a,b)\}.$$

Since $\gcd(d,\Delta)=1$, the set $\{(a,b)\in\Lambda(\mathscr{C},e):C(a,b)\}$ is a coset of the lattice $\Lambda(\mathscr{C},e\Delta)$, which has determinant $de\Delta^2$. Therefore,

$$R^*(d_1,d_2)=\sum_{\mathscr{C}\in\mathscr{U}(d_1,d_2)}\sum_{e|d}\mu(e)\left(\frac{\mathrm{Vol}(\mathscr{R})}{de\Delta^2}+O\left(1+\frac{P(\mathscr{R})}{R_1(\mathscr{C})}\right)\right), \tag{5.9.4}$$

where $R_1(\mathscr{C})$ denotes the length of the shortest nonzero vector in $\Lambda(\mathscr{C})$. Each equivalence class $\mathscr{C}\in\mathscr{U}(d_1,d_2)$ consists of $\varphi(d)$ elements, and so

$$\sum_{\mathscr{C}\in\mathscr{U}(d_1,d_2)}\sum_{e|d}\frac{\mu(e)}{e}=\sum_{\mathscr{C}\in\mathscr{U}(d_1,d_2)}\frac{\varphi(d)}{d}=\frac{\varrho^*(d_1,d_2)}{d}.$$

Moreover, we have $\#\mathscr{U}(d_1,d_2)\ll d^\epsilon$, as we now explain. We observe that $\#\mathscr{U}(d_1,d_2)=\varrho^*(d_1,d_2)/\varphi(d)$, and $\varrho^*$ is multiplicative by the Chinese remainder theorem. For primes $p\notin S$, we may apply Hensel's lemma to show that $\varrho^*(p^e,1),\varrho^*(1,p^e)=O(p^e)$ for any integer $e\geqslant 1$. Therefore, by the trivial bound for the divisor function, we conclude that

$$\#\mathscr{U}(d_1,d_2)=\frac{\varrho^*(d_1,d_2)}{\varphi(d)}\ll\frac{d^{1+\epsilon}}{\varphi(d)}\ll d^\epsilon. \tag{5.9.5}$$

Applying (5.9.4), and (5.9.5), we obtain

$$\begin{aligned}&\sum_{\substack{d_1\leqslant D_1,d_2\leqslant D_2\\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}}\max_{P(\mathscr{R})\leqslant N}\left|R^*(d_1,d_2)-\frac{\varrho^*(d_1,d_2)\,\mathrm{Vol}(\mathscr{R})}{d^2\Delta^2}\right|\\ &\ll_\epsilon (D_1D_2)^\epsilon\left(D_1D_2+N\sum_{\substack{d_1\leqslant D_1,d_2\leqslant D_2\\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}}\sum_{\mathscr{C}\in\mathscr{U}(d_1,d_2)}R_1(\mathscr{C})^{-1}\right).\end{aligned} \tag{5.9.6}$$

Let $v_1(\mathscr{C})$ denote a shortest nonzero vector of $\Lambda(\mathscr{C})$, and let $\|\cdot\|$ be the usual Euclidean norm. Then $\|v_1(\mathscr{C})\|^2\ll|\det\Lambda(\mathscr{C})|=d\leqslant D_1D_2$. Therefore,

$$\sum_{\substack{d_1\leqslant D_1,d_2\leqslant D_2\\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}}\sum_{\mathscr{C}\in\mathscr{U}(d_1,d_2)}R_1(\mathscr{C})^{-1}\ll\sum_{0<a^2+b^2\ll D_1D_2}\frac{M(a,b)}{\sqrt{a^2+b^2}}, \tag{5.9.7}$$

where

$$M(a,b)=\#\left\{\begin{array}{l}d_1\leqslant D_1,d_2\leqslant D_2,\mathscr{C}\in\mathscr{U}(d_1,d_2):\\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1,v_1(\mathscr{C})=(a,b)\end{array}\right\}.$$

For any $d_1, d_2$ enumerated by $M(a,b)$, we have $d_1 \mid g_1(a,b)$ and $d_2 \mid g_2(a,b)$, so

$$M(a,b) \leqslant \#\{d_1 \leqslant D_1, d_2 \leqslant D_2 : d_1 \mid g_1(a,b), d_2 \mid g_2(a,b)\}.$$

Since $g_1$ contains no linear factors, we know that $g_1(a,b) \neq 0$ whenever $(a,b) \neq (0,0)$. Suppose in addition that $g_2(a,b) \neq 0$. Then by the trivial bound for the divisor function we have $M(a,b) \ll (D_1D_2)^\epsilon$. We deduce that

$$\begin{aligned}\sum_{\substack{0<a^2+b^2\ll D_1D_2\\ g_2(a,b)\neq 0}} \frac{M(a,b)}{\sqrt{a^2+b^2}} &\ll (D_1D_2)^\epsilon \sum_{0<a^2+b^2\ll D_1D_2} \frac{1}{\sqrt{a^2+b^2}}\\ &\ll (D_1D_2)^{1/2+\epsilon}.\end{aligned}$$

Now suppose that $g_2(a,b) = 0$. Then as above, we have $O(D_1^\epsilon)$ choices for $d_1$, but now $D_2$ choices for $d_2$, so that $M(a,b) \ll D_1^\epsilon D_2$. We obtain

$$\sum_{\substack{0<a^2+b^2\ll D_1D_2\\ g_2(a,b)=0}} \frac{M(a,b)}{\sqrt{a^2+b^2}} \ll D_1^\epsilon D_2 \sum_{\substack{0<a^2+b^2\ll D_1D_2\\ g_2(a,b)=0}} \frac{1}{\sqrt{a^2+b^2}}.$$

For a fixed $b \neq 0$, $g_2(a,b)$ is a nonzero polynomial in $a$, and so has $O(1)$ roots. Therefore

$$\begin{aligned}\sum_{\substack{0<a^2+b^2\ll D_1D_2\\ g_2(a,b)=0}} \frac{1}{\sqrt{a^2+b^2}} &= \sum_{\substack{0<a^2+b^2\ll D_1D_2\\ b\neq 0\\ g_2(a,b)=0}} \frac{1}{\sqrt{a^2+b^2}} + \sum_{\substack{0<a^2\ll D_1D_2\\ g_2(a,0)=0}} \frac{1}{a}\\ &\ll \sum_{b\ll\sqrt{D_1D_2}} \frac{1}{b} + \sum_{a\ll\sqrt{D_1D_2}} \frac{1}{a}\\ &\ll (D_1D_2)^\epsilon.\end{aligned}$$

To summarize, we have established the following generalisation of [69, Lemma 3.2].

**Lemma 5.9.3.** *For any $D_1, D_2 > 0$ and any $\epsilon > 0$, we have*

$$\begin{aligned}&\sum_{\substack{d_1\leqslant D_1, d_2\leqslant D_2\\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}} \max_{P(\mathscr{R})\leqslant N} \left| R^*(d_1,d_2) - \frac{\varrho^*(d_1,d_2)\operatorname{Vol}(\mathscr{R})}{d^2\Delta^2}\right|\\ &\ll (D_1D_2)^\epsilon(D_1D_2 + N(D_1D_2)^{1/2} + ND_2).\end{aligned}$$

Now we remove the restriction $\gcd(a,b,d) = 1$. Below we write $R(d_1,d_2) = R(\mathscr{R}, d_1, d_2; C(a,b))$ in order to make the dependence on $\mathscr{R}$ and $C(a,b)$ clear. Let $k_1 = \deg g_1$ and $k_2 = \deg g_2$. We work with multiplicative functions $\psi_k$ for

$k = k_1$ and $k = k_2$, which map prime powers $p^r$ to $p^{\lceil r/k \rceil}$. We follow the same argument as Irving, but with $\psi_{k_1}, \psi_{k_2}$ in place of $\psi_3, \psi_4$. The motivation for this definition of $\psi_k$ comes from the fact that for any integers $d, e, k \geqslant 1$ with $e \mid \psi_k(d)$, and for any prime $p$, we have

$$p \mid \frac{\psi_k(d)}{e} \iff p \mid \frac{d}{\gcd(d, e^k)}. \tag{5.9.8}$$

Since $\gcd(d_1, d_2) = 1$, we have

$$R(\mathscr{R}, d_1, d_2; C(a,b)) = \sum_{\substack{e_1 \mid \psi_{k_1}(d_1) \\ e_2 \mid \psi_{k_2}(d_2)}} N(d_1, d_2, e_1, e_2), \tag{5.9.9}$$

where

$$N(d_1, d_2, e_1, e_2) = \#\left\{(a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : \begin{matrix} C(a,b), d_1 \mid g_1(a,b), d_2 \mid g_2(a,b), \\ \gcd(a, b, \psi_{k_1}(d_1)\psi_{k_2}(d_2)) = e_1 e_2 \end{matrix}\right\}. \tag{5.9.10}$$

We make a change of variables $a' = a/e_1e_2, b' = b/e_1e_2$ in (5.9.10). Let $\overline{e_1e_2}$ denote the multiplicative inverse of $e_1e_2$ modulo $\Delta$, which exists due to the assumption $\gcd(d_1d_2, \Delta) = 1$. The congruence condition $C(a,b)$ is equivalent to the congruence condition $a' \equiv \overline{e_1e_2}a_0 \pmod{\Delta}$ and $b' \equiv \overline{e_1e_2} \pmod{\Delta}$, which we denote by $C'(a', b')$. We have

$$\begin{aligned} d_1 \mid g_1(a,b) &\iff d_1 \mid (e_1e_2)^{k_1} g_1(a', b') \\ &\iff d_1 \mid e_1^{k_1} g_1(a', b') \\ &\iff \frac{d_1}{\gcd(d_1, e_1^{k_1})} \mid g_1(a', b'), \end{aligned}$$

and similarly for $d_2 \mid g_2(a,b)$. For convenience, we define

$$f_1 = \frac{d_1}{\gcd(d_1, e_1^{k_1})}, \quad f_2 = \frac{d_2}{\gcd(d_2, e_2^{k_2})}.$$

changing notation from $a', b'$ back to $a, b$, we deduce that $N(d_1, d_2, e_1, e_2)$ can be rewritten as

$$\begin{aligned} &\#\left\{(a,b) \in \mathscr{R}/(e_1e_2) \cap \mathbb{Z}^2 : \begin{matrix} C'(a,b), f_1 \mid g_1(a,b), f_2 \mid g_2(a,b), \\ \gcd(a, b, \psi_{k_1}(d_1)\psi_{k_2}(d_2)) = 1 \end{matrix}\right\} \\ &= \#\left\{(a,b) \in \mathscr{R}/(e_1e_2) \cap \mathbb{Z}^2 : \begin{matrix} C'(a,b), f_1 \mid g_1(a,b), f_2 \mid g_2(a,b), \\ \gcd(a, b, f_1f_2) = 1 \end{matrix}\right\}. \\ &= R^*\left(\mathscr{R}/(e_1e_2), f_1, f_2; C'(a,b)\right). \end{aligned} \tag{5.9.11}$$

The above arguments, but with the congruence conditions removed, and with the specific choice $\mathscr{R} = [0, d_1 d_2]^2$ also demonstrate that $\varrho(d_1, d_2)$ is equal to

$$\sum_{\substack{e_1 | \psi_{k_1}(d_1) \\ e_2 | \psi_{k_2}(d_2)}} \# \left\{ (a,b) \in \mathscr{R}/(e_1 e_2) \cap \mathbb{Z}^2 : \begin{array}{l} f_1 \mid g_1(a,b), f_2 \mid g_2(a,b), \\ \gcd(a, b, \psi_{k_1}(d_1)\psi_{k_2}(d_2)) = 1 \end{array} \right\}$$

$$= \sum_{\substack{e_1 | \psi_{k_1}(d_1) \\ e_2 | \psi_{k_2}(d_2)}} \left( \frac{d_1 d_2}{e_1 e_2 f_1 f_2} \right)^2 \varrho^*(f_1, f_2). \tag{5.9.12}$$

We denote the quantity

$$R^*(\mathscr{R}/(e_1 e_2), f_1, f_2; C'(a,b)) - \frac{\mathrm{Vol}(\mathscr{R}/(e_1 e_2)) \varrho^*(f_1, f_2)}{(f_1 f_2 \Delta)^2}$$

by $E(e_1, e_2, f_1, f_2)$. Combining (5.9.9), (5.9.11) and (5.9.12), we have

$$\sum_{\substack{d_1 \leqslant D_1, d_2 \leqslant D_2 \\ (d_1, d_2) = (d_1 d_2, \Delta) = 1}} \max_{P(\mathscr{R}) \leqslant N} \left| R(\mathscr{R}, d_1, d_2) - \frac{\varrho(d_1, d_2) \mathrm{Vol}(\mathscr{R})}{(d_1 d_2 \Delta)^2} \right|$$

$$= \sum_{\substack{d_1 \leqslant D_1, d_2 \leqslant D_2 \\ (d_1, d_2) = (d_1 d_2, \Delta) = 1}} \max_{P(\mathscr{R}) \leqslant N} \sum_{\substack{e_1 | \psi_{k_1}(d_1) \\ e_2 | \psi_{k_2}(d_2)}} |E(e_1, e_2, f_1, f_2)| \tag{5.9.13}$$

$$\leqslant \sum_{e_1 \leqslant D_1, e_2 \leqslant D_2} \sum_{\substack{f_1 \leqslant D_1/e_1, f_2 \leqslant D_2/e_2 \\ (f_1, f_2) = (f_1 f_2, \Delta) = 1}} \delta(e_1, f_1) \delta(e_2, f_2) \max_{P(\mathscr{R}) \leqslant N} |E(e_1, e_2, f_1, f_2)|, \tag{5.9.14}$$

where for integers $e, f, k, D \geqslant 1$, we have defined

$$\delta(e, f) = \# \left\{ d \leqslant D : e \mid \psi_k(d), f = \frac{d}{\gcd(d, e^k)} \right\}.$$

We claim that $\delta(e, f) \ll e^\epsilon$. To see this, suppose that $p$ is a prime and let $r = \nu_p(d), s = \nu_p(e)$ and $t = \nu_p(f)$. There is a unique choice of $r$ for a given $k, s$ and $t$ provided that $t > 0$, namely, $r = ks + t$. If $t = 0$, then we deduce from $f = d/\gcd(d, e^k)$ that $r \leqslant ks$. Taking a product over primes, we conclude that each $d$ enumerated by $\delta(e, f)$ is a divisor of $e^k$ multiplied by a quantity that is uniquely determined by $e$ and $f$. The claim follows, since the number of divisors of $e^k$ is $O(e^\epsilon)$. In our situation, where $e_1 \leqslant D_1$ and $e_2 \leqslant D_2$, we obtain $\delta(e_1, f_1)\delta(e_2, f_2) \ll (D_1 D_2)^\epsilon$. Therefore, applying Lemma 5.9.3 for each

choice of $e_1, e_2$ in (5.9.14), we conclude that

$$\begin{aligned}
&\sum_{\substack{d_1 \leqslant D_1, d_2 \leqslant D_2 \\ (d_1,d_2)=(d_1 d_2, \Delta)=1}} \max_{P(\mathscr{R}) \leqslant N} \left| R(\mathscr{R}, d_1, d_2) - \frac{\varrho(d_1,d_2)\operatorname{Vol}(\mathscr{R})}{(d_1 d_2 \Delta)^2} \right| \\
&\ll (D_1 D_2)^{\epsilon} \sum_{\substack{e_1 \leqslant D_1 \\ e_2 \leqslant D_2}} \left( \frac{D_1 D_2}{e_1 e_2} + N \left( \frac{D_1 D_2}{e_1 e_2} \right)^{1/2} + \frac{N D_2}{e_2} \right) \\
&\ll (D_1 D_2)^{\epsilon} \left( D_1 D_2 + N (D_1 D_2)^{1/2} + N D_2 \right),
\end{aligned}$$

which completes the proof of Proposition 5.9.1.

**Remark 5.9.4.** If $g_2(a,b) \neq 0$ for all $(a,b) \neq (0,0)$, then we do not need to consider the case $g_2(a,b) = 0$ in the analysis of the sum in (5.9.7), and so in our final level of distribution result, we do not require the assumption $D_2 \ll N^{1-\epsilon}$.

When $g_1(a,b)$ does contain linear factors, we can still obtain a basic level of distribution result from the above argument using the trivial estimate $R_1(\mathscr{C})^{-1} \leqslant 1$ in (5.9.6). This establishes the following lemma.

**Lemma 5.9.5.** *Let $g_1, g_2$ be arbitrary binary forms with nonzero discriminant. Then for any $\epsilon > 0$, there exists $\delta > 0$ such that for any $D_1, D_2 > 0$ with $D_1 D_2 \ll N^{1-\epsilon}$ , we have*

$$\sum_{\substack{d_1 \leqslant D_1, d_2 \leqslant D_2 \\ \gcd(d_1,d_2)=\gcd(d,\Delta)=1}} \max_{P(\mathscr{R}) \leqslant N} \left| R(d_1,d_2) - \frac{\varrho(d_1,d_2)\operatorname{Vol}(\mathscr{R})}{d^2 \Delta^2} \right| \ll N^{2-\delta}.$$

CHAPTER 6

# Sums of four squareful numbers

## 6.1 Introduction

This chapter is devoted to the quantitative study of the Campana points $(\mathbb{P}^2, \mathscr{D})(\mathbb{Z})$, where $D = \sum_{i=1}^4 \frac{1}{2} D_i$ with hyperplane divisors

$$D_1 = \{z_1 = 0\}, D_2 = \{z_2 = 0\}, D_3 = \{z_3 = 0\}, D_4 = \{z_1 + z_2 + z_3\} = 0,$$

and $\mathscr{D}$ is the obvious integral model of $D$ over $\mathbb{Z}$. We shall count points on this orbifold with respect to the height $H : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{R}_{\geqslant 0}$ given by

$$H(z) = \max\{|z_1|, |z_2|, |z_3|, |z_1 + z_2 + z_3|\}$$

for $(z_1, z_2, z_3) \in \mathbb{Z}^3_{\text{prim}}$ representing $z$. As discussed in the Introduction, this problem provides the best approximation to a major open question of Poonen [98] concerning Campana points on the orbifold $(\mathbb{P}^1, \frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[\infty])$.

We recall that a nonzero integer $n$ is *squareful* if for any prime $p \mid n$, we also have $p^2 \mid n$. We have

$$\#\{P \in (\mathbb{P}^2, \mathscr{D})(\mathbb{Z}) : H(P) \leqslant B\} = \frac{1}{2} \#\mathscr{N}_4(B), \tag{6.1.1}$$

where

$$\#\mathscr{N}_4(B) = \#\left\{\mathbf{z} \in (\mathbb{Z}_{\neq 0})^4_{\text{prim}} : |z_i| \leqslant B, z_i \text{ squareful for all } i, \sum_{i=1}^4 z_i = 0\right\} \tag{6.1.2}$$

is as defined in (1.2.2). To explain the factor $1/2$ in (6.1.1), we let $z_1, z_2, z_3$ be coordinates on $\mathbb{P}^2$, and define an additional variable $z_4 := z_1 + z_2 + z_3$. The Campana condition requires that $z_1, z_2, z_3$ and $z_1 + z_2 + z_3 = z_4$ are all squareful

for a representative $(z_1, z_2, z_3) \in \mathbb{Z}^3_{\text{prim}}$. We note that $(z_1, z_2, z_3) \in \mathbb{Z}^3_{\text{prim}}$ if and only if $(z_1, \dots, z_4) \in \mathbb{Z}^4_{\text{prim}}$. Therefore, there is a 2-1 map

$$\begin{aligned} \varphi : \mathscr{N}_4(B) &\to \{z \in (\mathbb{P}^2, \mathscr{D})(\mathbb{Z}) : H(z) \leqslant B\} \\ (z_1, \dots, z_4) &\mapsto [z_1 : z_2 : z_3]. \end{aligned} \tag{6.1.3}$$

We recall from (1.2.3) the notation

$$\mathscr{T} = \{(z_1, \dots, z_4) \in \mathbb{Z}^4_{\text{prim}} : z_1 \cdots z_4 = \square\}, \tag{6.1.4}$$

where $n = \square$ means that $n = m^2$ for some $m \in \mathbb{Z}$. We define

$$N(B) = \#(\mathscr{N}_4(B) \backslash \mathscr{T}). \tag{6.1.5}$$

The main aim of this chapter is to prove the Theorem D, which we recall here for convenience.

**Theorem 6.1.1.** *We have*

$$N(B) = cB + O(B^{734/735+\epsilon}), \tag{6.1.6}$$

*where the implied constant depends only on $\epsilon$, and $c$ is a positive constant given explicitly in (6.5.9) and Lemma 6.6.1.*

We shall demonstrate in Section 6.2 that Theorem 6.1.1 is compatible in the power of $B$ and $\log B$ with the PSTV-A conjecture (Conjecture 3.0.8). We gave a sketch proof of Theorem 6.1.1 in Section 4.5, which involved applying Lemma 3.3.1 to obtain a decomposition

$$N(B) = \frac{1}{16} \sum_{\substack{\mathbf{y} \in (\mathbb{Z}_{\neq 0})^4 \\ y_1, \dots, y_4 \text{ squarefree} \\ y_1 \cdots y_4 \neq \square}} N_{\mathbf{y}}(B), \tag{6.1.7}$$

where

$$N_{\mathbf{y}}(B) = \# \left\{ \mathbf{x} \in (\mathbb{Z}_{\neq 0})^4 : \sum_{i=1}^4 y_i^3 x_i^2 = 0, \begin{array}{l} \gcd(x_1 y_1, \dots, x_4 y_4) = 1 \\ \max_{1 \leqslant i \leqslant 4} |y_i^3 x_i^2| \leqslant B \end{array} \right\}.$$

In Section 6.3, we deal with the large coefficients $\mathbf{y}$ via an elementary argument. The technical heart of this chapter lies in Section 6.4, where we prove Theorem 4.5.1 by applying the delta method to count points on diagonal quadrics in $\mathbb{P}^3$ with a good explicit dependence on the coefficients. We recall from (4.5.4) that

$$N_{\mathbf{a}}(B) = \# \left\{ \mathbf{x} \in (\mathbb{Z}_{\neq 0})^4 : F_{\mathbf{a}}(\mathbf{x}) = 0, \max_{1 \leqslant i \leqslant 4} |a_i x_i^2| \leqslant B \right\}, \tag{6.1.8}$$

where we have introduced the notation

$$F_{\mathbf{a}}(\mathbf{x}) := \sum_{i=1}^{4} a_i x_i^2$$

for a vector $\mathbf{a} = (a_1, \dots, a_4) \in (\mathbb{Z}_{\neq 0})^4$. In Section 6.5, we complete the proof of Theorem 6.1.1 by applying Theorem 4.5.1 together with an inclusion-exclusion argument in order to reinsert the condition $\gcd(x_1 y_1, \dots, x_4 y_4) = 1$. Finally, in Section 6.6, we discuss the leading constant $c$ obtained in Theorem 6.1.1.

Several authors have previously studied rational points of bounded height on quadratic forms with an aim to provide estimates in which the dependence on the coefficients is made explicit. Browning [10, Theorem 2] applies the machinery from [61] to find such an estimate for the counting problem corresponding to $N_{\mathbf{a}}(B)$, but in $n \geqslant 5$ variables. Subsequently, Browning and Heath-Brown [17, Theorem 4.1] carried this out in $4$ variables. This latter result is nearly sufficient for our purposes, but Theorem 4.5.1 represents a refinement in which we drop the assumptions made in [17, Theorem 4.1] that $A$ is nearly squarefree and all the coefficients $a_1, \dots, a_4$ are roughly the same size. Finally, we mention that using other techniques from the geometry of numbers, Comtat provides in [39, Theorem 1.2] a completely uniform estimate for the number of zeros $(x_1, \dots, x_n) \in \mathbb{Z}^n_{\text{prim}}$ of a non-singular quadratic form $Q$ in $n \geqslant 3$ variables which lie in an arbitrary box $|x_i| \leqslant B_i$ for $i \in \{1, \dots, n\}$. However, the resulting bound $N_{\mathbf{a}}(B) \leqslant B/|A|^{1/4}$ does not have a good enough dependence on $A$ to be useful for our purposes.

### Notation

We write $e(\cdot)$ for the function $e^{2\pi i(\cdot)}$ and $e_q(\cdot)$ for the function $e^{2\pi i(\cdot)/q}$. We use boldface letters to denote vectors with four components, for example $\mathbf{z} = (z_1, \dots, z_4)$. For a vector $\mathbf{v}$, we define $|\mathbf{v}| = \max_{1 \leqslant i \leqslant 4} |v_i|$. We write "$M$ dyadic" under a summation to indicate that the sum is over integers of the form $M = 2^k$ for $k \in \mathbb{N}$.

**Acknowledgements.** The author is grateful to Tim Browning for suggesting this project and for helpful feedback and guidance during the development of this work.

## 6.2 Compatibility with the PSTV-A conjecture

We now discuss the compatibility of Theorem 6.1.1 with the PSTV-A conjecture (Conjecture 3.0.8). We begin by computing the constants $a$ and $b$ from Conjecture 3.0.8. We let $[L]$ denote the hyperplane class corresponding to

the line bundle $\mathscr{L}$, and $[K_{\mathbb{P}^2}]$ the canonical divisor class. We recall that $\operatorname{Pic}\mathbb{P}^2 \cong \mathbb{Z}$, with the isomorphism given by the degree. We have $\deg([L]) = 1$, $\deg([K_{\mathbb{P}^2}]) = -3$ and $\deg([D]) = 4 \cdot \frac{1}{2} = 2$. Therefore,

$$\begin{aligned} a &= \inf\{t \in \mathbb{R} : t[L] + [K_{\mathbb{P}^2}] + [D] \in \Lambda_{\text{eff}}\} \\ &= \inf\{t \in \mathbb{R} : t - 3 + 2 \geqslant 0\} \\ &= 1. \end{aligned}$$

The minimal supported face of $\Lambda_{\text{eff}}$ which contains $a[L] + [K_{\mathbb{P}^2}] + [D] = [0]$ is $\{0\}$, which has codimension $1$ in $\Lambda_{\text{eff}}$, so $b = 1$. Conjecture 3.0.8 therefore predicts that there is a thin set of Campana points $\mathscr{Z} \subseteq (\mathbb{P}^2, \mathscr{D})(\mathbb{Z})$, such that

$$\#\{P \in (\mathbb{P}^2, \mathscr{D})(\mathbb{Z}) \backslash \mathscr{Z} : H(P) \leqslant B\} \sim c_{\text{PSTV-A}} B$$

for some constant $c_{\text{PSTV-A}} > 0$. Theorem 6.1.1 is therefore consistent in the power of $B$ and $\log B$ with the PSTV-A conjecture, after removing the thin set $\mathscr{Z} = \varphi(\mathscr{T}) \cap (\mathbb{P}^2, \mathscr{D})(\mathbb{Z})$, where $\varphi$ and $\mathscr{T}$ are defined in (6.1.3) and (6.1.4). This choice of $\mathscr{Z}$ does indeed define a thin set. This is a special case of [96, Lemma 3.10], but we include a more direct argument here for completeness.

**Lemma 6.2.1.** *Let $\varphi$ and $\mathscr{T}$ be defined as in (6.1.3) and (6.1.4) respectively. Then $\varphi(\mathscr{T}) \cap (\mathbb{P}^2, \mathscr{D})(\mathbb{Z})$ is a thin set of Campana points in $(\mathbb{P}^2, \mathscr{D})(\mathbb{Z})$.*

*Proof.* It suffices to show that $\varphi(\mathscr{T})$ is a thin set in $\mathbb{P}^2(\mathbb{Q})$. By abuse of notation, we view $\mathscr{T}$ as a subset of $\mathbb{P}^3(\mathbb{Q})$ via the map $(z_1, \dots, z_4) \mapsto [z_1 : \cdots : z_4]$. We begin by showing that $\mathscr{T}$ is a thin subset of $\mathbb{P}^3(\mathbb{Q})$. Consider the weighted projective space $\mathbb{P}_{\mathbb{Q}}(2, 1, 1, 1, 1)$ with variables $t, z_1, \dots, z_4$. (We refer the reader to [68] for the basic definitions pertaining to weighted projective spaces.) We have an embedding

$$\begin{aligned} \nu : \mathbb{P}(2, 1, 1, 1, 1) &\hookrightarrow \mathbb{P}^{10} \\ [t : z_1 : \cdots : z_4] &\mapsto [t : z_1^2 : z_1 z_2 : \cdots : z_4^2], \end{aligned}$$

which on the $z_i$-variables is the Veronese embedding of degree 2. The polynomial $f(t, z_1, \dots, z_4) := t^2 - z_1 z_2 z_3 z_4$ is weighted homogeneous of degree $4$, and defines a subvariety $V$ of $\mathbb{P}(2, 1, 1, 1, 1)$. Let $Y \subseteq \mathbb{P}^{10}$ denote the image of $\nu$ and write $t, y_{11}, \dots, y_{44}$ for variables on $\mathbb{P}^{10}$. Then $\nu(V)$ is a hypersurface of $Y$ defined by the equation $t^2 = y_{12} y_{34}$. From this we see that $V$ is integral, projective and of dimension 3.

Consider the morphism $\pi : V \to \mathbb{P}^3$ given by $[t : z_1 : \cdots z_4] \to [z_1 : \cdots : z_4]$. This is étale of degree $2$ on the open subset $V'$ of $V$ defined by $z_1 \cdots z_4 \neq 0$. The set $W \subseteq \mathbb{P}^3(\mathbb{Q})$ defined by the equation $z_1 \cdots z_4 = 0$ is a type I thin set, and $\mathscr{T} = \pi(V'(\mathbb{Q})) \cup W$, so we deduce that $\mathscr{T}$ is thin in $\mathbb{P}^3(\mathbb{Q})$.

We can now show that $\varphi(\mathscr{T})$ is thin in $\mathbb{P}^2(\mathbb{Q})$. To do this, we intersect $\mathbb{P}^3, V'$ and $W$ with the hyperplane $H$ defined by the equation $z_1 + z_2 + z_3 = z_4$. The map $\pi$ is ramified along the set $W$, which is a union of hyperplanes $H_i$ given by $\{z_i = 0\}$. Since the intersection of $H$ with the $H_i$ is smooth and transversal, it follows from [104, Section 9.4] that $\pi([V'(\mathbb{Q}) \cap H(\mathbb{Q})] \cup [W \cap H(\mathbb{Q})])$ is thin in $H(\mathbb{Q})$. The image of this set under the obvious isomorphism $H \cong \mathbb{P}^2$ sending $[z_1 : \cdots : z_4]$ to $[z_1 : z_2 : z_3]$ is precisely $\varphi(\mathscr{T})$, so we conclude that $\varphi(\mathscr{T})$ is a thin set in $\mathbb{P}^2(\mathbb{Q})$. □

The leading constant $c$ from Theorem 6.1.1 is discussed in Section 6.5. However, in the light of Chapter 7, we do not expect the leading constant to agree with the prediction from the PSTV-A conjecture without the removal of further thin sets.

## 6.3 Dealing with the large coefficients

Given a nonzero squareful number $z_i$, we let $x_i, y_i$ denote the unique integers such that $x_i \in \mathbb{N}$, $y_i \in \mathbb{Z}$ is squarefree, and $z_i = y_i^3 x_i^2$, as obtained from Lemma 3.3.1. We shall also use the notation $Y = y_1 \cdots y_4$. For $B, D \geqslant 1$, we define

$$M(B, D) = \# \left\{ \mathbf{z} \in (\mathbb{Z}_{\neq 0})^4_{\mathrm{prim}} : \begin{array}{l} \sum_{i=1}^4 z_i = 0, z_i \text{ squareful for all } i, \\ |\mathbf{z}| \leqslant B, |Y| \geqslant D \end{array} \right\}.$$

The aim of this section is to prove the following upper bound.

**Proposition 6.3.1.** *We have* $M(B, D) = O(B^{1+\epsilon} D^{-1/12})$.

The key result in the proof of Proposition 6.3.1 is the following upper bound for the quantity

$$N(\boldsymbol{X}, \boldsymbol{Y}) = \# \left\{ \mathbf{x}, \mathbf{y} \in (\mathbb{Z}_{\neq 0})^4 : \begin{array}{l} y_1, \ldots, y_4 \text{ squarefree}, \sum_{i=1}^4 x_i^2 y_i^3 = 0, \\ |x_i| \leqslant X_i, |y_i| \leqslant Y_i \text{ for all } i \end{array} \right\}.$$

**Proposition 6.3.2.** *We have*

$$N(\boldsymbol{X}, \boldsymbol{Y}) = O((X_1 \cdots X_4)^{1/2+\epsilon} (Y_1 \cdots Y_4)^{2/3+\epsilon}).$$

We explain how to deduce Proposition 6.3.1 from Proposition 6.3.2. We define

$$M_1(B; \boldsymbol{R}) = \# \left\{ \mathbf{z} \in (\mathbb{Z}_{\neq 0})^4 : \begin{array}{l} \sum_{i=1}^4 z_i = 0, z_i \text{ squareful for all } i, \\ |z_i| \leqslant B, R_i \leqslant |y_i| < 2R_i \text{ for all } i \end{array} \right\}.$$

Then

$$M(B,D) \ll \sum_{\substack{R_1,\dots,R_4 \text{ dyadic} \\ R_1\cdots R_4 \gg D}} M_1(B;\boldsymbol{R}). \tag{6.3.1}$$

We observe that the conditions $|\mathbf{z}| \leqslant B$ and $R_i \leqslant |y_i|$ imply that $|x_i|^2 \leqslant B/R_i^3$. Consequently,

$$M_1(B;\boldsymbol{R}) \leqslant N\left(\left(\sqrt{\frac{B}{R_1^3}},\dots,\sqrt{\frac{B}{R_4^3}}\right),(2R_1,\dots,2R_4)\right).$$

Applying Proposition 6.3.2, we obtain

$$M_1(B;\boldsymbol{R}) \ll B^{1+\epsilon}(R_1\cdots R_4)^{-1/12}.$$

We conclude from (6.3.1) that

$$M(B,D) \ll B^{1+\epsilon} \sum_{\substack{R_1,\dots,R_4 \text{ dyadic} \\ R_1\cdots R_4 \gg D}} (R_1\cdots R_4)^{-1/12} \ll B^{1+\epsilon}D^{-1/12},$$

as claimed in Proposition 6.3.1.

*Proof of Proposition 6.3.2.* For $k \in \{1,\dots,4\}$, we define

$$S_k(\alpha) = \sum_{\substack{x_k\in\mathbb{Z}_{\neq 0} \\ |x_k|\leqslant X_k}} \sum_{\substack{y_k\in\mathbb{Z}_{\neq 0} \\ |y_k|\leqslant Y_k \\ y_k \text{ squarefree}}} e(\alpha x_k^2 y_k^3).$$

Then

$$N(\boldsymbol{X},\boldsymbol{Y}) = \int_0^1 \prod_{k=1}^4 S_k(\alpha)\mathrm{d}\alpha.$$

By Hölder's inequality, we have

$$N(\boldsymbol{X},\boldsymbol{Y}) \leqslant \left(\prod_{k=1}^4 \int_0^1 |S_k(\alpha)|^4\mathrm{d}\alpha\right)^{1/4}. \tag{6.3.2}$$

We fix $k \in \{1,\dots,4\}$, and to ease notation we write $X_k = X, Y_k = Y$. Then

$$\int_0^1 |S_k(\alpha)|^4\mathrm{d}\alpha = N(X,Y), \tag{6.3.3}$$

where

$$N(X,Y) = \#\left\{\mathbf{x},\mathbf{y}\in(\mathbb{Z}_{\neq 0})^4 : \begin{array}{c} y_1,\dots,y_4 \text{ squarefree}, \\ x_1^2y_1^3 + x_2^2y_2^3 = -(x_3^2y_3^3 + x_4^2y_4^3) \\ |\mathbf{x}| \leqslant X, |\mathbf{y}| \leqslant Y \end{array}\right\}.$$

In view of (6.3.2), the task now is to show that

$$N(X,Y) = O(X^{2+\epsilon}Y^{8/3+\epsilon}). \tag{6.3.4}$$

Throughout the remainder of the argument, we make repeated use of the trivial estimate for the divisor function, namely that the number of divisors of a positive integer $d$ is $O(d^{\epsilon})$ [56, Section 18.1].

We begin by considering the trivial cases $x_i = \pm x_j$ for some $i \neq j$. Without loss of generality, suppose $i = 1, j = 2$. We obtain

$$x_1^2(y_1^3 + y_2^3) = -(x_3^2y_3^3 + x_4^2y_4^3). \tag{6.3.5}$$

If both sides of (6.3.5) are zero, then $y_1 = -y_2$, since we are assuming $x_1 \neq 0$. Hence there are $O(XY)$ choices for $x_1, y_1, y_2$. On the right hand side, since $y_3, y_4$ are squarefree, it follows that $x_3 = \pm x_4$ and $y_3 = -y_4$, hence there are $O(XY)$ choices for $x_3, x_4, y_3, y_4$. This gives a total of $O(X^2Y^2)$ solutions. If both sides of (6.3.5) are nonzero, then there are $O(X^2Y^2)$ choices for $x_3, x_4, y_3, y_4$. Let $n = -(x_3^2y_3^3 + x_4^2y_4^3)$ and $t = y_1 + y_2$. Then we can rewrite (6.3.5) as $x_1^2t(y_1^2 - y_1y_2 - y_2^2) = n$. There are $O(n^{\epsilon}) = O(X^{\epsilon}Y^{\epsilon})$ choices for $x_1, t$ by the trivial estimate for the divisor function, and if $n, x_1, t$ are fixed, then there are $O(1)$ integers $y_1, y_2$ satisfying $x_1^2t(y_1^2 - y_1y_2 - y_2^2) = n$ and $y_1 + y_2 = t$. Overall, in the case $x_i = \pm x_j$, we conclude that there are $O(X^{2+\epsilon}Y^{2+\epsilon})$ solutions, which is satisfactory for establishing (6.3.4). From now on we assume $x_i \neq \pm x_j$ for all $i \neq j$.

Returning to the integral representation of $N(X,Y)$ from (6.3.3), we can apply the Cauchy–Schwarz inequality in two different ways to $|S_k(\alpha)|^2$. We have

$$\begin{aligned} |S_k(\alpha)|^2 &\leqslant 2X \sum_{|x|\leqslant X} \Bigg| \sum_{\substack{|y|\leqslant Y \\ y \text{ squarefree}}} e(\alpha x^2y^3) \Bigg|^2 \\ &= 2X \sum_{|x|\leqslant X} \sum_{\substack{|y_1|,|y_2|\leqslant Y \\ y_1,y_2 \text{ squarefree}}} e(\alpha x^2(y_1^3 - y_2^3)), \end{aligned}$$

and similarly,

$$|S_k(\alpha)|^2 \leqslant 2Y \sum_{\substack{|y|\leqslant Y \\ y \text{ squarefree}}} \sum_{|x_1|,|x_2|\leqslant X} e(\alpha y^3(x_1^2 - x_2^2)).$$

Applying these inequalities once each to $|S_k(\alpha)|^4$, we obtain

$$N(X,Y) \leqslant 4XYL(X,Y), \tag{6.3.6}$$

where

$$L(X,Y) = \#\left\{\begin{array}{l}(x,x_1,x_2,y,y_1,y_2)\in(\mathbb{Z}_{\neq 0})^6: \\ |x|,|x_1|,|x_2|\leqslant X \\ |y|,|y_1|,|y_2|\leqslant Y \text{ and } y,y_1,y_2 \text{ squarefree} \\ x^2(y_1^3-y_2^3)=y^3(x_1^2-x_2^2)\end{array}\right\}.$$

It will be convenient to work with the quantity $L(X,Y,U)$ defined to be $L(X,Y)$ but with the additional assumption $U/2<|x|\leqslant U$, which we denote by $|x|\sim U$. we shall then perform a sum over dyadic intervals for $U\leqslant 2X$ at the end of the argument. We also need to extract from $L(X,Y,U)$ the greatest common divisor $k=\gcd(x,y)$. Note that since $y$ is squarefree, so is $k$. Hence

$$L(X,Y,U)=\sum_{k\leqslant \min(U,Y)}\mu^2(k)L_k(X,Y,U),$$

where

$$L_k(X,Y,U) = \#\left\{\begin{array}{l}(x,x_1,x_2,y,y_1,y_2)\in(\mathbb{Z}_{\neq 0})^6: \\ |x|\sim U/k,|x_1|,|x_2|\leqslant X, \\ |y|\leqslant Y/k,|y_1|,|y_2|\leqslant Y, \text{ and } y,y_1,y_2 \text{ squarefree}, \\ \gcd(x,y)=1, \\ x^2(y_1^3-y_2^3)=ky^3(x_1^2-x_2^2).\end{array}\right\}.$$

We now obtain two different estimates for $L_k(X,Y,U)$, depending on the size of $k$. Our first estimate is suitable for large values of $k$.

We have $ky^3(x_1^2-x_2^2)\neq 0$, since $y\neq 0$, and the cases $x_1=\pm x_2$ have already been dealt with above. Consequently, for any fixed $x,y_1,y_2,k$, there are $O((XY)^\epsilon)$ choices for $y,x_1,x_2$ such that $x^2(y_1^3-y_2^3)=ky^3(x_1^2-x_2^2)$, by the trivial estimate for the divisor function. Therefore

$$L_k(X,Y,U)\ll (XY)^\epsilon A(k), \tag{6.3.7}$$

where

$$A(k)=\#\{|x|\sim U/k,|y_1|,|y_2|\leqslant Y : k|x^2(y_1^3-y_2^3)\}.$$

Now $k|x^2(y_1^3-y_2^3)$ implies that there exist integers $d,r$ with $dr=k$, such that $d|x^2$ and $r|(y_1^3-y_2^3)$. Observe that since $k$ is squarefree, $d|x^2$ if and only if $d|x$. Defining

$$N(r)=\#\{y_1,y_2\leqslant Y : r|(y_1^3-y_2^3)\},$$

we therefore have

$$A(k) \leqslant \sum_{\substack{d,r\\ dr=k}} \sum_{\substack{|x|\sim U/k\\ d|x}} N(r) \ll U \sum_{\substack{d,r\\ dr=k}} \frac{N(r)}{dk}. \tag{6.3.8}$$

Note that $r \leqslant k \leqslant Y$, so $N(r) \ll Y^2\varrho(r)/r^2$, where we have defined

$$\varrho(r) = \#\{\eta_1, \eta_2 \pmod r : \eta_1^3 \equiv \eta_2^3\}.$$

It is easy to see that $\varrho(r) \ll r^{1+\epsilon}$ for any sqaurefree integer $r$. Indeed, for a prime $p$ and a fixed $\eta_1 \pmod p$, there are at most $3$ choices for $\eta_2 \pmod p$ such that $\eta_1^3 \equiv \eta_2^3 \pmod p$, and so $\varrho(p) \leqslant 3p$. Since $r$ is squarefree and $\varrho$ is multiplicative, it follows from the Chinese Remainder theorem that

$$\varrho(r) = \prod_{p|r} \varrho(p) \leqslant \prod_{p|r} 3p \ll r^{1+\epsilon}.$$

Applying this bound on $\varrho(r)$, we conclude that $N(r) \ll Y^2/r^{1-\epsilon} \ll Y^{2+\epsilon}/r$, and hence from (6.3.7) and (6.3.8) we obtain

$$L_k(X,Y,U) \ll \frac{(XY)^\epsilon U}{k} \sum_{\substack{d,r\\ dr=k}} \frac{Y^{2+\epsilon}}{dr} \ll \frac{X^\epsilon Y^{2+\epsilon} U}{k^2}. \tag{6.3.9}$$

We now find a different estimate for when $k$ is small. If $(x,y) = 1$ and $x^2(y_1^3 - y_2^3) = ky^3(x_1^2 - x_2^2)$, then $x^2 | k(x_1^2 - x_2^2)$, so we may define the integer $u = k(x_1^2 - x_2^2)/x^2$. Note $u \neq 0$ by the assumption $x_1 \neq \pm x_2$. We have $|u| \ll kX^2/(U/k)^2 = k^3X^2/U^2$. Therefore

$$L_k(X,Y,U) \ll \sum_{\substack{|u| \ll \frac{k^3X^2}{U^2}\\ u\neq 0}} \sum_{\substack{|x|\sim U/k\\ |x_1|,|x_2|\leqslant X\\ k(x_1^2-x_2^2)=ux^2}} \sum_{\substack{|y|\leqslant Y/k\\ y\neq 0\\ |y_1|,|y_2|\leqslant Y\\ uy^3=y_1^3-y_2^3}} 1. \tag{6.3.10}$$

For a fixed $n = uy^3 \neq 0$, there are $O(Y^\epsilon)$ solutions $y_1, y_2$ to $y_1^3 - y_2^3 = n$, using the trivial estimate for the divisor function, and so the inner sum of (6.3.10) is $O(Y^{1+\epsilon}/k)$. Similarly, for a given $|x| \sim U/k$, there are $O(X^\epsilon)$ choices for $x_1, x_2$ in the middle sum. Hence

$$L_k(X,Y,U) \ll (XY)^\epsilon \sum_{\substack{|u| \ll \frac{k^3X^2}{U^2}\\ u\neq 0}} \frac{UY}{k^2} \ll \frac{kX^{2+\epsilon}Y^{1+\epsilon}}{U}.$$

Combining this with the estimate in (6.3.9), we obtain

$$\begin{aligned} L_k(X,Y,U) &\ll X^{\epsilon}Y^{1+\epsilon}\min\left(\frac{UY}{k^2},\frac{kX^2}{U}\right) \\ &\leqslant X^{\epsilon}Y^{1+\epsilon}\left(\frac{UY}{k^2}\right)^{2/3}\left(\frac{kX^2}{U}\right)^{1/3} \\ &= \frac{X^{2/3+\epsilon}Y^{5/3+\epsilon}U^{1/3}}{k}. \end{aligned}$$

Finally, we take a sum over $k \leqslant Y$ and dyadic intervals $U \leqslant 2X$ to obtain

$$\begin{aligned} L(X,Y) &\ll X^{2/3+\epsilon}Y^{5/3+\epsilon}\sum_{\substack{U \text{ dyadic}\\ U\leqslant 2X}}\sum_{k\leqslant Y}\frac{U^{1/3}}{k} \\ &\ll X^{1+\epsilon}Y^{5/3+\epsilon}. \end{aligned}$$

Recalling (6.3.6), we have established (6.3.4), which from (6.3.2) gives the required bound for $N(\boldsymbol{X},\boldsymbol{Y})$. □

## 6.4 Application of the circle method

In this section, we use the circle method from [61] to count zeros of diagonal quadratic forms in four variables, the main goal being the proof of Theorem 4.5.1. Before proceeding with the proof, we collect together some of the notation which we shall use throughout this section. Much of the notation depends on a vector $\mathbf{a} = (a_1,\dots,a_4) \in (\mathbb{Z}_{\neq 0})^4$, which remains fixed throughout this section.

- $F_{\mathbf{a}}(\mathbf{x})$ denotes the quadratic form $\sum_{i=1}^4 a_i x_i^2$.
- $\boldsymbol{P} = (P_1,\dots,P_4)$, where $P_i = \sqrt{\frac{B}{|a_i|}}$ for $i \in \{1,\dots,4\}$.
- $N_{\mathbf{a}}(B) = \#\{\mathbf{x} \in (\mathbb{Z}_{\neq 0})^4 : F_{\mathbf{a}}(\mathbf{x}) = 0, |x_i| \leqslant P_i\}$, as defined in (6.1.8).
- $A = a_1 \cdots a_4$.
- $\Delta = \Delta(\mathbf{a}) = \prod_{i=1}^4 \gcd\left(a_i, \prod_{j\neq i} a_j\right)$.
- $\boldsymbol{\epsilon} = (\epsilon_1,\dots,\epsilon_4) \in \{\pm 1\}^4$, where $\epsilon_i = a_i/|a_i|$ is the sign of $a_i$.
- $G(\mathbf{x})$ is the quadratic form $\sum_{i=1}^4 \epsilon_i x_i^2 = F_{\boldsymbol{\epsilon}}(\mathbf{x})$.
- $\eta \in (0,1/4)$ is a small real parameter depending only on $\mathbf{a}$ and $B$.
- $w : \mathbb{R}^4 \to \mathbb{R}_{\geqslant 0}$ is an infinitely differentiable smooth weight function, which has compact support and satisfies $w(\mathbf{x}) = 0$ for all $|\mathbf{x}| \leqslant \eta$.

- $w_1, w_2$ are particular choices of such a smooth weight function, constructed explicitly in Lemma 6.4.3.
- $Q = B^{1/2}$, and for a positive integer $q$, we write $r = q/Q$.
- $\mathbf{c}$ denotes a vector in $\mathbb{Z}^4$.
- $\mathbf{v} = (v_1, \dots, v_4)$ is given by $v_i = q^{-1}P_i c_i$.
- $C_i = \eta^{-1}B^{\epsilon}|a_i|^{1/2}$ for $i \in \{1, \dots, 4\}$.

**Definition 6.4.1.** The *singular integral* $\sigma_\infty(\boldsymbol{\epsilon})|A|^{-1/2}$ and the *singular series* $\mathfrak{G}_{\mathbf{a}}$ associated to $F_{\mathbf{a}}$ are given respectively by the equations

$$\sigma_\infty(\boldsymbol{\epsilon}) = \int_{-\infty}^{\infty} \int_{[-1,1]^4} e(-\theta G(\mathbf{x}))\, \mathrm{d}\mathbf{x}\, \mathrm{d}\theta, \tag{6.4.1}$$

$$\mathfrak{G}_{\mathbf{a}} = \sum_{q=1}^{\infty} q^{-4} \sum_{\substack{k \bmod q \\ \gcd(k,q)=1}} \sum_{\mathbf{b} \bmod q} e_q(kF_{\mathbf{a}}(\mathbf{b})). \tag{6.4.2}$$

For convenience we record again here the statement of Theorem 4.5.1.

**Theorem 6.4.2.** *Let $\mathbf{a} \in (\mathbb{Z}_{\neq 0})^4$ be such that $A \neq \square$ and $|A| \leqslant B^{4/7}$. Then*

$$N_{\mathbf{a}}(B) = \frac{\mathfrak{G}_{\mathbf{a}}\sigma_\infty(\boldsymbol{\epsilon})B}{|A|^{1/2}} + O\left(\frac{B^{41/42+\epsilon}\Delta^{1/3}}{|A|^{11/24}}\right). \tag{6.4.3}$$

The circle method from [61] makes use of smooth weight functions $w : \mathbb{R}^4 \to \mathbb{R}_{\geqslant 0}$, which we shall take to approximate the characteristic function on $[-1, 1]^4$. We introduce a smoothly weighted version of $N_{\mathbf{a}}(B)$ given by

$$N_{w,\mathbf{a}}(B) = \sum_{\substack{\mathbf{x} \in (\mathbb{Z}_{\neq 0})^4 \\ F_{\mathbf{a}}(\mathbf{x}) = 0}} w(P_1^{-1}x_1, \dots, P_4^{-1}x_4). \tag{6.4.4}$$

We also introduce a weighted version of $\sigma_\infty(\boldsymbol{\epsilon})$ defined by

$$\sigma_\infty(w) = \int_{-\infty}^{\infty} \int_{\mathbb{R}^4} w(\mathbf{x}) e(-\theta G(\mathbf{x}))\, \mathrm{d}\mathbf{x}\, \mathrm{d}\theta. \tag{6.4.5}$$

Whilst the arguments in this section could be applied to quite a general class of weight functions $w$, in order to get the power savings in Theorem 6.1.1, we shall need to keep track of the dependence of our estimates on $w$. Therefore, we now construct two explicit weight functions $w_1, w_2 : \mathbb{R}^4 \to \mathbb{R}_{\geqslant 0}$ that we shall use in the remainder of the analysis. Let $\eta \in (0, 1/4)$ be a parameter, which is allowed to depend on $\mathbf{a}$ and $B$. We would like $w_1, w_2$ to satisfy the following properties:

1. For $i \in \{1,2\}$, $w_i$ is infinitely differentiable, and for any integer $N \geqslant 0$, any integers $j_1, \dots, j_4 \geqslant 0$ satisfying $j_1 + \cdots + j_4 \leqslant N$, and any $\mathbf{x} \in \mathbb{R}^4$, we have
$$\frac{\partial^{j_1+\cdots+j_4}}{\partial x_1^{j_1} \cdots \partial x_4^{j_4}} w_i(\mathbf{x}) \ll_N \eta^{-N}. \tag{6.4.6}$$
2. $w_1, w_2$ vanish in a neighbourhood of the origin, and approximate the characteristic function on $[-1,1]^4$. More precisely, $w_1$ is supported on $[-1,1]^4 \backslash [-\eta,\eta]^4$ and takes the value 1 on $[-1+\eta, 1-\eta]^4 \backslash [-2\eta, 2\eta]^4$, whilst $w_2$ is supported on $[-1-\eta, 1+\eta]^4 \backslash [-\eta,\eta]^4$ and takes the value 1 on $[-1,1]^4 \backslash [-2\eta, 2\eta]^4$.

**Lemma 6.4.3.** *Let $\eta \in (0, 1/4)$. Then there exist functions $w_1, w_2 : \mathbb{R}^4 \to \mathbb{R}_{\geqslant 0}$ satisfying properties (1) and (2) above.*

*Proof.* Let $\|\cdot\|$ denote the Euclidean norm. We build $w_1, w_2$ from a higher-dimensional analogue of the standard bump function defined in (4.4.2). Let $\psi : \mathbb{R}^4 \to \mathbb{R}_{\geqslant 0}$ be given by
$$\psi(\mathbf{x}) = \begin{cases} c \exp\left(\frac{1}{\|\mathbf{x}\|^2 - 1}\right), & \text{if } \|\mathbf{x}\| < 1, \\ 0, & \text{otherwise,} \end{cases} \tag{6.4.7}$$
where $c$ is chosen such that $\int_{\mathbb{R}^4} \psi(\mathbf{x})\, \mathrm{d}\mathbf{x} = 1$. Note that all $N$th partial derivatives of $\psi$ are $\ll_N 1$. For $\delta > 0$, we define $\psi_\delta(\mathbf{x}) = \delta^{-4}\psi(\mathbf{x}/\delta)$. Then $\psi_\delta$ also integrates to 1, and its $N$th partial derivatives are $\ll_N \delta^{-N}$.

For a compact subset $R \subseteq \mathbb{R}^4$, consider the convolution
$$(1_R * \psi_\delta)(\mathbf{x}) = \int_R \psi_\delta(\mathbf{x} - \mathbf{t})\, \mathrm{d}\mathbf{t}. \tag{6.4.8}$$
Let $B_\delta(\mathbf{x})$ denote the Euclidean ball of radius $\delta$ around $\mathbf{x}$. We observe that, as a function of $\mathbf{t}$, we have $\operatorname{supp} \psi_\delta(\mathbf{x} - \mathbf{t}) = B_\delta(\mathbf{x})$. Consequently,
$$(1_R * \psi_\delta)(\mathbf{x}) = \begin{cases} 1, & \text{if } B_\delta(\mathbf{x}) \subseteq R, \\ 0, & \text{if } B_\delta(\mathbf{x}) \cap R = \emptyset, \\ v \in [0,1], & \text{otherwise.} \end{cases} \tag{6.4.9}$$
Moreover, all $N$th partial derivatives of $1_R * \psi_\delta$ are $\ll_N \delta^{-N} \operatorname{meas}(R)$, where $\operatorname{meas}(R)$ denotes the Lebesgue measure of $R$.

To conclude the proof, we define $w_1$ (resp. $w_2$) as in (6.4.8), with $\delta = \eta/2$ and $R = R_1$ (resp. $R = R_2$), where
$$R_1 = \left[-1 + \frac{\eta}{2}, 1 - \frac{\eta}{2}\right]^4 \setminus \left[\frac{-3\eta}{2}, \frac{3\eta}{2}\right]^4,$$
$$R_2 = \left[-1 - \frac{\eta}{2}, 1 + \frac{\eta}{2}\right]^4 \setminus \left[\frac{-3\eta}{2}, \frac{3\eta}{2}\right]^4.$$

It is now straightforward to deduce that $w_1, w_2$ satisfy the required properties (1) and (2). $\square$

We now state a smoothly weighted version of Theorem 6.4.2.

**Theorem 6.4.4.** *Suppose $\eta \in (0, 1/4)$ and $\mathbf{a} \in (\mathbb{Z}_{\neq 0})^4$. Let $w$ be one of the weights $w_1$ or $w_2$ from Lemma 6.4.3. Suppose that $A \neq \square$. Then*

$$N_{w,\mathbf{a}}(B) = \frac{\mathfrak{G}_{\mathbf{a}}\sigma_\infty(w)B}{|A|^{1/2}} + O\left(\frac{\eta^{-6}B^{5/6+\epsilon}\Delta^{1/3}}{|A|^{5/24}}\right) + O(\eta^{-7}B^{1/2+\epsilon}). \quad (6.4.10)$$

We explain how Theorem 6.4.2 can be deduced from Theorem 6.4.4 by applying the methods from [16, Section 5.3] and [18, Section 2.4], together with the upper bound $\mathfrak{G}_{\mathbf{a}} \ll |A|^{\epsilon}\Delta^{1/4}$ for the singular series, which we prove in Lemma 6.4.16 at the end of this section.

Let $1_{[-1,1]^4}$ denote the characteristic function on $[-1, 1]^4$, and for an integer $j \geqslant 0$, define $w_2^{(j)}(\mathbf{x}) = w_2((2\eta)^{-j}\mathbf{x})$. Then for any nonzero $\mathbf{x} \in \mathbb{R}^4$, we have

$$w_1(\mathbf{x}) \leqslant 1_{[-1,1]^4}(\mathbf{x}) \leqslant \sum_{j=0}^{\infty} w_2^{(j)}(\mathbf{x}).$$

The above series converges because a given $\mathbf{x} \neq \mathbf{0}$ is contained in the support of only finitely many of the $w_2^{(j)}$. Consequently,

$$N_{w_1,\mathbf{a}}(B) \leqslant N_{\mathbf{a}}(B) \leqslant \sum_{j=0}^{\infty} N_{w_2^{(j)},\mathbf{a}}(B) = \sum_{j=0}^{\infty} N_{w_2,\mathbf{a}}((2\eta)^{2j}B).$$

The assumption $|A| \leqslant B^{4/7}$ in the statement of Theorem 6.4.2 implies that the error term $\eta^{-7}B^{1/2+\epsilon}$ is dominated by the other error term in (6.4.10), provided that $\eta \gg B^{-3/14+\epsilon}$. For any $\eta \in (0, 1/4)$ satisfying this condition, it follows from Theorem 6.4.4 that

$$\sum_{j=0}^{\infty} N_{w_2,\mathbf{a}}((2\eta)^{2j}B) = \frac{(1 + O(\eta^2))\mathfrak{G}_{\mathbf{a}}\sigma_\infty(w_2)B}{|A|^{1/2}} + O\left(\frac{\eta^{-6}B^{5/6+\epsilon}\Delta^{1/3}}{|A|^{5/24}}\right).$$

As explained in [18, Lemma 2.9], for $i \in \{1, 2\}$, we have

$$|\sigma_\infty(w_i) - \sigma_\infty(\boldsymbol{\epsilon})| \ll \eta\sigma_\infty(\boldsymbol{\epsilon}) \ll \eta,$$

from which we deduce that

$$N_{\mathbf{a}}(B) = \frac{(1 + O(\eta))\mathfrak{G}_{\mathbf{a}}\sigma_\infty(\boldsymbol{\epsilon})B}{|A|^{1/2}} + O\left(\frac{\eta^{-6}B^{5/6+\epsilon}\Delta^{1/3}}{|A|^{5/24}}\right).$$

We choose

$$\eta = \frac{1}{5}B^{-1/42}|A|^{1/24}.$$

Clearly $\eta \gg B^{-3/14+\epsilon}$. Moreover, using the assumption $|A| \leqslant B^{4/7}$, we have that $\eta \in (0, 1/4)$, as was required in order to apply Theorem 6.4.4. Theorem 6.4.2 now follows from the estimate $\mathfrak{G}_{\mathbf{a}} \ll |A|^{\epsilon}\Delta^{1/4}$ found in Lemma 6.4.16.

We commence with the proof of Theorem 6.4.4. It will be convenient to make the assumptions

$$\eta^{-1}, |\mathbf{a}| \ll B^R \tag{6.4.11}$$

for some fixed $R \geqslant 0$, so that quantities bounded by an arbitrarily small power of $\eta^{-1}$ or $|A|$ are also $\ll B^{\epsilon}$ for any $\epsilon > 0$. If these assumptions do not hold, then the statement of Theorem 6.4.4 is trivial, because we would have $w(P_1^{-1}x_1, \dots, P_4^{-1}x_4) = 0$ for all $\mathbf{x} \in (\mathbb{Z}_{\neq 0})^4$, and thus $N_{w,\mathbf{a}}(B) = 0$. Applying the delta method as stated in Theorem 4.4.1, we have

$$N_{w,\mathbf{a}}(B) = \frac{C_Q}{Q^2} \sum_{\mathbf{c}\in\mathbb{Z}^4} \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{a}}(\mathbf{c}) I_{q,\mathbf{a}}(\mathbf{c}), \tag{6.4.12}$$

where $C_Q = 1 + O_N(Q^{-N})$ for any integer $N \geqslant 1$, and $Q = B^{1/2}$. We recall also the definitions of the exponentials sums and integrals

$$\begin{aligned} S_{q,\mathbf{a}}(\mathbf{c}) &= \sum_{\substack{k \bmod q \\ \gcd(k,q)=1}} \sum_{\mathbf{b} \bmod q} e_q(kF_{\mathbf{a}}(\mathbf{b}) + \mathbf{b}\cdot\mathbf{c}), \\ I_{q,\mathbf{a}}(\mathbf{c}) &= \int_{\mathbb{R}^4} w(P_1^{-1}x_1, \dots, P_4^{-1}x_4) h\left(\frac{q}{Q}, \frac{F_{\mathbf{a}}(\mathbf{x})}{Q^2}\right) e_q(-\mathbf{c}\cdot\mathbf{x})\,\mathrm{d}\mathbf{x}, \end{aligned} \tag{6.4.13}$$

and the construction of the smooth function $h : (0,\infty) \times \mathbb{R} \to \mathbb{R}$ from (4.4.4). As observed in [61, Section 3], it is straightforward to check that $h(x,y) \ll x^{-1}$ and $h(x,y) = 0$ whenever $x > \max(1, 2|y|)$.

We note that by changing variables $P_i^{-1}x_i$ into $x_i$, we can rewrite $I_{q,\mathbf{a}}(\mathbf{c})$ as

$$\begin{aligned} I_{q,\mathbf{a}}(\mathbf{c}) &= P_1\cdots P_4 \int_{\mathbb{R}^4} w(\mathbf{x}) h\left(\frac{q}{Q}, \frac{F_{\mathbf{a}}(P_1x_1, \dots, P_4x_4)}{Q^2}\right) e(-\mathbf{v}\cdot\mathbf{x})\mathrm{d}\mathbf{x} \\ &= P_1\cdots P_4 \int_{\mathbb{R}^4} w(\mathbf{x}) h(r, G(\mathbf{x})) e(-\mathbf{v}\cdot\mathbf{x})\mathrm{d}\mathbf{x}. \end{aligned} \tag{6.4.14}$$

## 6.4.1 The main term

The main term for $N_{w,\mathbf{a}}(B)$ comes from the case $\mathbf{c} = \mathbf{0}$ in (6.4.12). We define

$$M(B) = \frac{1}{Q^2} \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{a}}(\mathbf{0}) I_{q,\mathbf{a}}(\mathbf{0}). \tag{6.4.15}$$

We have

$$\mathfrak{G}_{\mathbf{a}} = \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{a}}(\mathbf{0}). \tag{6.4.16}$$

The convergence of this series follows from Lemma 6.4.16. Moreover, from (6.4.14), we have

$$I_{q,\mathbf{a}}(\mathbf{0}) = P_1 \cdots P_4 \int_{\mathbb{R}^4} w(\mathbf{x}) h\left(r, G(\mathbf{x})\right) \mathrm{d}\mathbf{x}.$$

We let $w_0$ denote a smooth weight function supported on $[-17, 17]$ and taking the value 1 in $[-16, 16]$. Since $\mathrm{supp}(w) \subseteq [-1-\eta, 1+\eta] \subset [-2, 2]$, we have $w_0(G(\mathbf{x})) = 1$ whenever $\mathbf{x} \in \mathrm{supp}(w)$. We obtain

$$I_{q,\mathbf{a}}(\mathbf{0}) = P_1 \cdots P_4 \int_{\mathbb{R}^4} w(\mathbf{x}) w_0(G(\mathbf{x})) h(r, G(\mathbf{x})) \mathrm{d}\mathbf{x}.$$

The arguments at the beginning of [17, Section 4.3] can be applied to obtain

$$I_{q,\mathbf{a}}(\mathbf{0}) = P_1 \cdots P_4 \left( \lim_{\delta \to 0} \int_{-\infty}^{\infty} \left( \frac{\sin(\pi\delta\theta)}{\pi\delta\theta} \right)^2 J(w;\theta) L(\theta) \, \mathrm{d}\theta \right), \tag{6.4.17}$$

where

$$J(w;\theta) = \int_{\mathbb{R}^4} w(\mathbf{x}) e(-\theta G(\mathbf{x})) \, \mathrm{d}\mathbf{x}, \tag{6.4.18}$$

$$L(\theta) = \int_{-\infty}^{\infty} w_0(t) h(r,t) e(\theta t) \, \mathrm{d}t. \tag{6.4.19}$$

We would like to compare the bracketed expression in (6.4.17) with $\sigma_\infty(w)$ from (6.4.5), which by definition equals $\int_{-\infty}^{\infty} J(w;\theta) \mathrm{d}\theta$. We apply [17, Lemma 4.11] to estimate $L(\theta)$. In addition to the integer $N \geqslant 1$, the implied constants in [17, Lemma 4.11] depend only on $\mathrm{supp}(w_0)$. However, we note that we have chosen $w_0$ independently of $w$, and hence independently of $\eta$. Therefore for any $q \leqslant Q$ and any $N \geqslant 1$, we have

$$L(\theta) = 1 + O_N(\{1 + |\theta|^N\} r^N). \tag{6.4.20}$$

Our next task is to bound $J(w;\theta)$. In order to achieve this, we need to work with more general smooth weight functions $\widetilde{w} : \mathbb{R}^4 \to \mathbb{R}_{\geqslant 0}$ which belong to a class $S$ defined by the following properties.

**Definition 6.4.5.** We say $\widetilde{w} \in S$ if

1. $\widetilde{w}$ is smooth,
2. $\widetilde{w}$ is supported on $[-2, 2]^4$,
3. $\widetilde{w}(\mathbf{x}) = 0$ for $|\mathbf{x}| \leqslant \eta$,
4. $|\widetilde{w}(\mathbf{x})| \ll 1$ for all $\mathbf{x} \in \mathbb{R}^4$,

5. The derivatives of $\widetilde{w}(\mathbf{x})$ are bounded as in (6.4.6).

Since in Theorem 6.4.4, $w$ is equal to $w_1$ or $w_2$, we note in particular that $w \in S$.

**Lemma 6.4.6.** *For any $\widetilde{w} \in S$ and any $M \in \mathbb{Z}_{\geqslant 0}$, we have $J(\widetilde{w};\theta) \ll_M |\eta^2\theta|^{-M}$.*

*Proof.* The case $M = 0$ is trivial since the integrand in the definition of $J(\widetilde{w};\theta)$ is bounded and has compact support. For $M \geqslant 1$, we follow a similar argument to [61, Lemma 10], by applying integration by parts and induction on $M$. We have

$$J(\widetilde{w};\theta) = \int_{\mathbb{R}^4} \widetilde{w}(\mathbf{x}) e(-\theta G(\mathbf{x}))\mathrm{d}\mathbf{x} \ll \max_{1\leqslant j\leqslant 4} \left| \int_{\substack{\mathbf{x}\in\mathbb{R}^4,\\ |x_j|=\max_i |x_i|}} \widetilde{w}(\mathbf{x}) e(-\theta G(\mathbf{x}))\mathrm{d}\mathbf{x} \right|.$$

Without loss of generality, we may assume that $j = 1$. We note that

$$e(-\theta G(\mathbf{x})) = \frac{1}{-4\pi i\epsilon_1\theta x_1} \frac{\partial}{\partial x_1} e(-\theta G(\mathbf{x})).$$

We perform integration by parts with respect to $x_1$ to obtain

$$J(\widetilde{w};\theta) \ll \left| \int_{\substack{\mathbf{x}\in\operatorname{supp}\widetilde{w}\\ |x_1|=\max_i |x_i|}} \frac{\partial}{\partial x_1} \left( \frac{\widetilde{w}(\mathbf{x})}{4\pi i\theta x_1} \right) e(-\theta G(\mathbf{x}))\mathrm{d}\mathbf{x} \right|.$$

Since $|x_1| = \max_i |x_i|$, we have $|x_1|^{-1} = |\mathbf{x}|^{-1} \leqslant \eta^{-1}$ for any $\mathbf{x} \in \operatorname{supp}\widetilde{w}$. Therefore by the assumptions on the size of $\widetilde{w}$ and its derivatives, we see that

$$\frac{\partial}{\partial x_1} \left( \frac{\widetilde{w}(\mathbf{x})}{4\pi i\theta x_1} \right) = \widetilde{w}^{(1)} (4\pi i\theta\eta^2)^{-1}$$

for some $\widetilde{w}^{(1)} \in S$. Hence

$$J(\widetilde{w};\theta) \ll |\eta^2\theta|^{-1} |J(\widetilde{w}^{(1)};\theta)|.$$

Proceeding by induction, we obtain $J(\widetilde{w}(\mathbf{x});\theta) \ll_M |\eta^2\theta|^{-M} |J(\widetilde{w}^{(M)};\theta)|$ for some $\widetilde{w}^{(M)} \in S$, from which we deduce the required result by applying the trivial bound $J(\widetilde{w}^{(M)};\theta) \ll 1$. □

Lemma 6.4.6 together with the trivial bound $J(w;\theta) \ll 1$ imply that for any integer $M \geqslant 1$, we have

$$J(w;\theta) \ll_M (1 + |\eta^2\theta|)^{-M} \leqslant \eta^{-2M} (1 + |\theta|)^{-M}.$$

Combining this with (6.4.17), (6.4.20) and the fact that

$$\lim_{\delta\to 0}\int_{-\infty}^{\infty}\left(\frac{\sin(\pi\delta\theta)}{\pi\delta\theta}\right)^2 J(\theta;w)\,\mathrm{d}\theta=\int_{-\infty}^{\infty}J(\theta;w)\,\mathrm{d}\theta=\sigma_\infty(w),$$

we obtain

$$|(P_1\cdots P_4)^{-1}I_{q,\mathbf{a}}(\mathbf{0})-\sigma_\infty(w)|\ll_{M,N}\int_{-\infty}^{\infty}\frac{r^N\{1+|\theta|\}^N}{\eta^{2M}\{1+|\theta|\}^M}\,\mathrm{d}\theta.$$

In order to ensure that the integral converges, we make the choice $M=N+2$, and we conclude that

$$I_{q,\mathbf{a}}(\mathbf{0})=P_1\cdots P_4\{\sigma_\infty(w)+O_N(\eta^{-2N-4}r^N)\},\tag{6.4.21}$$

for any integer $N\geqslant 1$.

Let $R=B^{1/2-\epsilon}\eta^2$. We note that if $q\leqslant R$, then the error term in (6.4.21) can be made smaller than any negative power of $B$ by appropriate choice of $N$ (depending on $\epsilon$), due to the assumption in (6.4.11).

We now split the main term up. We have

$$M(B)=\frac{P_1\cdots P_4\sigma_\infty(w)}{B}\sum_{q\leqslant R}q^{-4}S_{q,\mathbf{a}}(\mathbf{0})+O(T(R)+1),\tag{6.4.22}$$

where

$$T(R)=\frac{1}{Q^2}\sum_{q>R}q^{-4}S_{q,\mathbf{a}}(\mathbf{0})I_{q,\mathbf{a}}(\mathbf{0}).\tag{6.4.23}$$

we shall estimate $T(R)$ using partial summation. The following lemma is similar to [17, Lemma 4.3], and gives bounds for $I_{q,\mathbf{a}}(\mathbf{c})$ and its derivative. Only the case $\mathbf{c}=\mathbf{0}$ is needed in the study of the main term, but the case $\mathbf{c}\neq\mathbf{0}$ will be useful later.

**Lemma 6.4.7.** *Let $\mathbf{c}\in\mathbb{Z}^4$ and $k\in\{0,1\}$. Then*

1. *If $k=0$ or $\mathbf{c}=\mathbf{0}$ then $q^k\frac{\partial^k I_{q,\mathbf{a}}(\mathbf{c})}{\partial q^k}\ll P_1\cdots P_4$,*
2. *If $k=1$ and $\mathbf{c}\neq\mathbf{0}$ then $q^k\frac{\partial^k I_{q,\mathbf{a}}(\mathbf{c})}{\partial q^k}\ll\eta^{-1}P_1\cdots P_4$.*

*Proof.* Suppose that $\mathbf{c}=\mathbf{0}$. Recalling (6.4.14) and the notation $r=q/Q$, it is clear that

$$q^k\frac{\partial^k I_{q,\mathbf{a}}(\mathbf{0})}{\partial q^k}=r^kP_1\cdots P_4\int_{\mathbb{R}^4}w(\mathbf{x})\frac{\partial^k h(r,G(\mathbf{x}))}{\partial r^k}\mathrm{d}\mathbf{x}.\tag{6.4.24}$$

From [61, Lemma 5] with $m = k, n = 0$ and $N = 2$, we have

$$\frac{\partial^k h(r, G(\mathbf{x}))}{\partial r^k} \ll r^{-1-k}\left(r^2 + \min\left\{1, \frac{r^2}{|G(\mathbf{x})|^2}\right\}\right), \tag{6.4.25}$$

and so

$$(P_1 \cdots P_4)^{-1} q^k \frac{\partial^k I_{q,\mathbf{a}}(\mathbf{0})}{\partial q^k} \ll r + r^{-1}\int_{\substack{\mathbf{x}\in\operatorname{supp} w\\ |G(\mathbf{x})|\leqslant r}} 1\mathrm{d}\mathbf{x} + r\int_{\substack{\mathbf{x}\in\operatorname{supp} w\\ |G(\mathbf{x})|> r}} \frac{1}{|G(\mathbf{x})|^2}\mathrm{d}\mathbf{x}. \tag{6.4.26}$$

We need to show that the right hand side of (6.4.26) is $O(1)$. We can assume that the first term $r$ is $O(1)$, since $h(r, G(\mathbf{x})) = 0$ when $r > \max(1, 2|G(\mathbf{x})|)$, and $G(\mathbf{x}) \ll 1$ for $x \in \operatorname{supp} w$, and so $I_{q,\mathbf{a}}(\mathbf{0}) = 0$ unless $r \ll 1$. In order to estimate the integrals in (6.4.26), we consider for $z > 0$ the Lebesgue measure $m(z)$ of the set

$$S(z) = \{\mathbf{x} \in \operatorname{supp} w : |G(\mathbf{x})| \leqslant z\}.$$

We can find distinct indices $i, j$ such that $\epsilon_i = \epsilon_j$. Without loss of generality we may assume $i = 1, j = 2$, and in addition that $\epsilon_1 = \epsilon_2 = 1$. For a fixed choice of $x_3, x_4$, we define $c = \epsilon_3 x_3^2 + \epsilon_4 x_4^2$, so that if $\mathbf{x} \in S(z)$ then $x_1^2 + x_2^2 \in [-c - z, -c + z]$. The measure of the set of pairs $x_1, x_2$ satisfying this condition is $O(z)$. For $\mathbf{x} \in \operatorname{supp} w$, we have $|x_3|, |x_4| \ll 1$, and hence $m(z) = O(z)$. From this we see that the first integral in (6.4.26) is $O(r)$, and by breaking into dyadic intervals, the second integral is $O(r^{-1})$. Therefore the right hand side of (6.4.26) is $O(1)$, as required.

When $\mathbf{c} \neq \mathbf{0}$, we first note that for $k = 0$, we can reduce to the case above by applying the trivial estimate to the extra exponential factor $e(-\mathbf{v}\cdot\mathbf{x})$ appearing in the integral defining $I_{q,\mathbf{a}}(\mathbf{c})$. It remains only to deal with the case $\mathbf{c} \neq \mathbf{0}, k = 1$. We recall the vector $\mathbf{v} \in \mathbb{R}^4$ is given by $v_i = q^{-1}P_i c_i$. Similarly to (6.4.24), we obtain

$$\begin{aligned}
&(P_1 \cdots P_4)^{-1} q \frac{\partial I_{q,\mathbf{a}}(\mathbf{c})}{\partial q}\\
&\ll r\int_{\mathbb{R}^4} w(\mathbf{x}) \frac{\partial\{h(r, G(\mathbf{x}))e(-\mathbf{v}\cdot\mathbf{x})\}}{\partial r}\mathrm{d}\mathbf{x}\\
&= r\int_{\mathbb{R}^4} w(\mathbf{x})\left(\frac{\partial h(r, G(\mathbf{x}))}{\partial r}e(-\mathbf{v}\cdot\mathbf{x}) - h(r, G(\mathbf{x}))(2\pi i r\mathbf{v}\cdot\mathbf{x})e(-\mathbf{v}\cdot\mathbf{x})\right)\mathrm{d}\mathbf{x}.
\end{aligned} \tag{6.4.27}$$

The first term can again be dealt with using the trivial estimate for $e(-\mathbf{v}\cdot\mathbf{x})$ and the argument for the case $\mathbf{c} = \mathbf{0}$ given above. In order to estimate the second term, as in [61, Lemma 14], we apply the divergence theorem

$$\int_{\mathbb{R}^4} \nabla\cdot(w(\mathbf{x})h(r, G(\mathbf{x}))e(-\mathbf{v}\cdot\mathbf{x})\mathbf{x})\mathrm{d}\mathbf{x} = 0$$

in order to remove the additional factor of $2\pi i\mathbf{v}\cdot\mathbf{x}$. This yields

$$\begin{aligned}\int_{\mathbb{R}^4} w(\mathbf{x})h(r,G(\mathbf{x}))e(-\mathbf{v}\cdot\mathbf{x})(2\pi ir\mathbf{v}\cdot\mathbf{x})\mathrm{d}\mathbf{x}&\\ = \int_{\mathbb{R}^4} \widetilde{w}(\mathbf{x})h(r,G(\mathbf{x}))e(-\mathbf{v}\cdot\mathbf{x})\mathrm{d}\mathbf{x}&\\ + \int_{\mathbb{R}^4} 4w(\mathbf{x})h(r,G(\mathbf{x}))e(-\mathbf{v}\cdot\mathbf{x})\mathrm{d}\mathbf{x}&\\ + \int_{\mathbb{R}^4} 2w(\mathbf{x})G(\mathbf{x})e(-\mathbf{v}\cdot\mathbf{x})\frac{\partial h(r,G(\mathbf{x}))}{\partial G(\mathbf{x})}\mathrm{d}\mathbf{x},&\end{aligned} \tag{6.4.28}$$

where $\widetilde{w}(\mathbf{x}) = (\mathbf{x}\cdot\nabla)w(\mathbf{x})$. The second integral on the right hand side of (6.4.28) can now be treated in the same way as the easier cases $k=0$ or $\mathbf{c}=\mathbf{0}$ using the trivial estimate for $e(-\mathbf{v}\cdot\mathbf{x})$. The third integral can be estimated by noting that $G(\mathbf{x}) \ll 1$ for $\mathbf{x}\in\mathrm{supp}(w)$, and applying [61, Lemma 5] with $n=1, m=0, N=2$. From this, we see that $\frac{\partial h(r,G(\mathbf{x}))}{\partial G(\mathbf{x})}$ also satisfies the bound in (6.4.25), and so we may proceed as in the case $\mathbf{c}=\mathbf{0}$. For the first integral, we note that $\widetilde{w}(\mathbf{x})$ is uniformly bounded by $\eta^{-1}$. Hence the above arguments can be applied to the first integral as well, but with an extra factor of $\eta^{-1}$. □

We define

$$\Sigma(x;\mathbf{c}) = \sum_{q\leqslant x} q^{-3}S_{q,\mathbf{a}}(\mathbf{c}). \tag{6.4.29}$$

Moreover, we let $F^*_{\mathbf{a}}$ denote the $\mathrm{dual\ form}$ of $F_{\mathbf{a}}$, i.e., the quadratic form given by the equation

$$F^*_{\mathbf{a}}(\mathbf{c}) = a_2a_3a_4c_1^2 + a_1a_3a_4c_2^2 + a_1a_2a_4c_3^2 + a_1a_2a_3c_4^2.$$

We also define

$$\Delta_{\mathbf{c}}(\mathbf{a}) = \prod_{i=1}^{4}\gcd\left(\gcd(a_i,c_i), \prod_{j\neq i}\gcd(a_j,c_j)\right). \tag{6.4.30}$$

In particular we have $\Delta_{\mathbf{c}}(\mathbf{a}) = \Delta$ when $\mathbf{c}=\mathbf{0}$.

The following lemma is a slight modification of [17, Lemma 4.9].

**Lemma 6.4.8.** *Suppose $A\neq\square$. Let $\mathbf{c}\in\mathbb{Z}^4$ be such that $F^*_{\mathbf{a}}(\mathbf{c})=0$. Then*

$$\Sigma(x;\mathbf{c}) \ll A^{3/16+\epsilon}\Delta_{\mathbf{c}}(\mathbf{a})^{3/8}x^{1/2+\epsilon}.$$

*Proof.* We use the fact that $S_{q,\mathbf{a}}(\mathbf{c})$ is multiplicative in $q$, as proved by Heath-Brown in the discussion following [61, Lemma 28]. This allows us to write

$$\Sigma(x;\mathbf{c}) = \sum_{\substack{q_2\leqslant x\\ q_2\mid(2A)^\infty}} q_2^{-3}S_{q_2,\mathbf{a}}(\mathbf{c}) \sum_{\substack{q_1\leqslant x/q_2\\ \gcd(q_1,2A)=1}} q_1^{-3}S_{q_1,\mathbf{a}}(\mathbf{c}), \tag{6.4.31}$$

where the notation $q_2|(2A)^\infty$ means that every prime dividing $q_2$ also divides $2A$. We recall that $c_{q_1}(0) = \varphi(q_1)$, where $\varphi$ denotes the Euler totient function. Therefore, by [17, Lemma 4.6], we have

$$\sum_{\substack{q_1 \leqslant x/q_2 \\ \gcd(q_1, 2A)=1}} q_1^{-3} S_{q_1,\mathbf{a}}(\mathbf{c}) = \sum_{\substack{q_1 \leqslant x/q_2 \\ \gcd(q_1, 2A)=1}} \left(\frac{A}{q_1}\right) \frac{\varphi(q_1)}{q_1}.$$

Applying the Burgess bound [71, Theorem 12.6] as in the proof of [17, Lemma 4.9], we obtain

$$\sum_{\substack{q_1 \leqslant x/q_2 \\ \gcd(q_1, 2A)=1}} q_1^{-3} S_{q_1,\mathbf{a}}(\mathbf{c}) \ll \frac{|A|^{3/16+\epsilon} x^{1/2}}{q_2^{1/2}}.$$

Returning to (6.4.31), we have

$$\Sigma(x; \mathbf{c}) \ll |A|^{3/16+\epsilon} x^{1/2} \sum_{\substack{q_2 \leqslant x \\ q_2|(2A)^\infty}} \frac{|S_{q_2,\mathbf{a}}(\mathbf{c})|}{q_2^{7/2}}. \tag{6.4.32}$$

Now [17, Lemma 4.5] states that $S_{q,\mathbf{a}}(\mathbf{c}) \ll q^3 \prod_{i=1}^4 \gcd(q, a_i, c_i)^{1/2}$. Moreover, there are $O(x^\epsilon A^\epsilon)$ choices for $q_2 \leqslant x$ with $q_2|(2A)^\infty$, as explained in the paragraph after (3.3.8). Therefore

$$\sum_{\substack{q_2 \leqslant x \\ q_2|(2A)^\infty}} \frac{|S_{q_2,\mathbf{a}}(\mathbf{c})|}{q_2^{7/2}} \ll x^\epsilon A^\epsilon \sup_{q|(2A)^\infty} \left( \frac{\prod_{i=1}^4 \gcd(q, a_i, c_i)^{1/2}}{q^{1/2}} \right). \tag{6.4.33}$$

Let $p$ be a prime. We define

$$L_p = \nu_p \left( \frac{\prod_{i=1}^4 \gcd(q, a_i, c_i)}{q} \right), \quad k_p = \nu_p(q).$$

For an index $i = 1, \dots, 4$, we let $m_{i,p}$ denote the $i$th smallest element of $\nu_p(\gcd(a_1, c_1)), \dots, \nu_p(\gcd(a_4, c_4))$. Then

$$L_p = \sum_{i=1}^4 \left( \min(k_p, m_{i,p}) - k_p \right).$$

It can be checked that the maximum possible value of $L_p$ is attained by choosing $k_p = m_{3,p}$, and so $L_p \leqslant m_{1,p} + m_{2,p} + m_{3,p}$. We have $L_p \leqslant 0$ unless $p|\Delta_{\mathbf{c}}(\mathbf{a})$. Hence the supremum in (6.4.33) is bounded by

$$\prod_{p|\Delta_{\mathbf{c}}(\mathbf{a})} p^{(m_{1,p}+m_{2,p}+m_{3,p})/2}.$$

For any prime $p$, we have

$$\begin{aligned}\nu_p(\Delta_{\mathbf{c}}(\mathbf{a})) &= m_{1,p} + m_{2,p} + m_{3,p} + \min(m_{1,p} + m_{2,p} + m_{3,p}, m_{4,p}) \\ &\geqslant \frac{4}{3}(m_{1,p} + m_{2,p} + m_{3,p}),\end{aligned}$$

and hence the supremum in (6.4.33) is bounded by $\Delta_{\mathbf{c}}(\mathbf{a})^{3/8}$. Recalling (6.4.32) we obtain the desired estimate for $\Sigma(x;\mathbf{c})$. □

**Proposition 6.4.9.** *Suppose $A \neq \square$, and let $M(B)$ be as defined in (6.4.15). Then*

$$M(B) = \frac{\mathfrak{G}_{\mathbf{a}}\sigma_\infty(w)B}{|A|^{1/2}} + O\left(\frac{\eta^{-2}B^{3/4+\epsilon}\Delta^{3/8}}{|A|^{5/16}}\right).$$

*Proof.* We recall the estimate for $M(B)$ from (6.4.22) and the definition of $T(R)$ from (6.4.23). We may restrict the sum to the range $R < q \ll Q$, since $h(r, G(\mathbf{x})) = 0$ unless $q \ll Q$. Using Lemma 6.4.8 with $x \ll Q$ and $\mathbf{c} = \mathbf{0}$, together with Lemma 6.4.7, and partial summation, we obtain

$$\begin{aligned}T(R) &= \frac{-I_{R,\mathbf{a}}(\mathbf{0})}{Q^2R}\Sigma(R;\mathbf{0}) - \frac{1}{Q^2}\int_R^Q \Sigma(x;\mathbf{0})\frac{\partial}{\partial x}\left(\frac{I_{x,\mathbf{a}}(\mathbf{0})}{x}\right)\mathrm{d}x \\ &\ll \frac{P_1\cdots P_4}{BR}\sup_{R\leqslant t\ll Q}|\Sigma(t;\mathbf{0})| \\ &\ll \frac{P_1\cdots P_4}{BR}|A|^{3/16+\epsilon}\Delta^{3/8}B^{1/4+\epsilon} \\ &\ll \frac{\eta^{-2}B^{3/4+\epsilon}\Delta^{3/8}}{|A|^{5/16}},\end{aligned}$$

which is the error term claimed in the proposition. (We note that in the last line, we may absorb the factor $|A|^\epsilon$ into the factor $B^\epsilon$ due to the assumption (6.4.11).) Finally, the same error term is also obtained when we extend the sum $\sum_{q\leqslant R} q^{-4}S_{q,\mathbf{a}}(\mathbf{0})$ in (6.4.22) to the singular series $\mathfrak{G}_{\mathbf{a}} = \sum_{q=1}^\infty q^{-4}S_{q,\mathbf{a}}(\mathbf{0})$, as can be seen by applying Lemma 6.4.8 and partial summation in a very similar manner to above. □

## 6.4.2 The error term

We now study the error term coming from the case $\mathbf{c} \neq \mathbf{0}$. We begin with a lemma which is similar to [17, Lemma 4.2 (i)].

**Lemma 6.4.10.** *For any nonzero $\mathbf{c} \in \mathbb{Z}^4$ and any integer $N \geqslant 0$, we have*

$$I_{q,\mathbf{a}}(\mathbf{c}) \ll_N \frac{P_1\cdots P_4}{r}\left(1 + \frac{r}{\eta}\right)^N \min_{1\leqslant i\leqslant 4}\left(\frac{|a_i|^{1/2}}{|c_i|}\right)^N.$$

*Proof.* We apply integration by parts $N$ times to the integral in (6.4.14), where we differentiate $f(\mathbf{x}) := w(\mathbf{x})h(r, G(\mathbf{x}))$ and integrate $g(\mathbf{x}) := e(\mathbf{v} \cdot \mathbf{x})$. Each integral of $g(\mathbf{x})$ with respect to $x_i$ introduces a factor of $(2\pi i q^{-1} P_i c_i)^{-1}$ .

We recall from (6.4.6) that for any $i \in \{1, \dots, 4\}$ and any $N \geqslant 1$,

$$\left| \frac{\partial^N}{\partial x_i^N} w(\mathbf{x}) \right| \ll_N \eta^{-N}.$$

Using the product rule, we have

$$\left| \frac{\partial^N}{\partial x_i^N} f(\mathbf{x}) \right| \ll_N \max_{0 \leqslant j \leqslant N} \left| \eta^{j-N} \frac{\partial^j}{\partial x_i^j} h(r, G(\mathbf{x})) \right|.$$

Clearly

$$\left| \frac{\partial^j}{\partial x_i^j} G(\mathbf{x}) \right| \ll 1$$

for all $\mathbf{x} \in \operatorname{supp} w$. By [17, Equation (4.10)], we have

$$\frac{\partial^j h(r, y)}{\partial y^j} \ll_j r^{-1-j}. \tag{6.4.34}$$

Hence by the chain rule, we have

$$\left| \frac{\partial^N}{\partial x_i^N} f(\mathbf{x}) \right| \ll_N \max_{0 \leqslant j \leqslant N} r^{-1-j} \eta^{j-N} = r^{-1} \min(r, \eta)^{-N} \leqslant r^{-1} \left( \frac{1}{r} + \frac{1}{\eta} \right)^N. \tag{6.4.35}$$

After performing integration by parts $N$ times, we apply (6.4.35) to all derivatives of $f(\mathbf{x})$ that appear, and the trivial estimate $|e(-\mathbf{v} \cdot \mathbf{x})| \leqslant 1$, to obtain for any $i \in \{1, \dots, 4\}$,

$$I_{q,\mathbf{a}}(\mathbf{c}) \ll_N \frac{P_1 \cdots P_4}{r(q^{-1}|P_i c_i|)^N} \left( \frac{1}{r} + \frac{1}{\eta} \right)^N.$$

Recalling that $P_i = (B/|a_i|)^{1/2}, Q = B^{1/2}, r = q/Q$, and choosing the index $i$ such that $|P_i c_i|$, is maximised, the last expression rearranges to give the desired estimate. □

**Remark 6.4.11.** Lemma 6.4.10 allows us to assume $|c_i| \ll \eta^{-1}|a_i|^{1/2} B^{\epsilon} = C_i$ for all $i \in \{1, \dots, 4\}$, since outside this range the estimate in Lemma 6.4.10 can be made smaller than any power of $B$ by an appropriate choice of $N$.

The following lemma is a variant of the first derivative test and is based on [61, Lemma 10].

**Lemma 6.4.12.** *Let $f(\mathbf{x}) = \theta G(\mathbf{x}) - \mathbf{v}\cdot\mathbf{x}$, where $\mathbf{v} \in \mathbb{R}^4$ and $\theta \in \mathbb{R}$ are such that $|\mathbf{v}| \geqslant 5|\theta|$. Then for any integer $N \geqslant 0$ and any $w$ in the class of smooth weight functions $S$ from Definition 6.4.5, we have*

$$\int_{\mathbb{R}^4} w(\mathbf{x})e(f(\mathbf{x}))\mathrm{d}\mathbf{x} \ll_N (\eta|\mathbf{v}|)^{-N}.$$

*Proof.* The case $N = 0$ is trivial. We define $f_j(\mathbf{x}) = \partial f(\mathbf{x})/\partial x_j = 2\epsilon_j\theta x_j - v_i$. By the assumption $|\mathbf{v}| \geqslant 5|\theta|$, there is some index $j \in \{1,\dots,4\}$ such that $|f_j(\mathbf{x})| \gg |\mathbf{v}|$ for any $\mathbf{x} \in [-2,2]^4$. Without loss of generality, we may assume $j = 1$.

We write

$$w(\mathbf{x})e(f(\mathbf{x})) = \frac{w(\mathbf{x})}{2\pi i f_1(\mathbf{x})}\frac{\partial}{\partial x_1}e(f(\mathbf{x}))$$

and integrate by parts with respect to $x_1$ to obtain

$$\int_{\mathbb{R}^4} w(\mathbf{x})e(f(\mathbf{x}))\mathrm{d}\mathbf{x} = -(2\pi i\eta|\mathbf{v}|)^{-1}\int_{\mathbb{R}^4} e(f(\mathbf{x}))\widetilde{w}(\mathbf{x})\mathrm{d}\mathbf{x},$$

where

$$\widetilde{w}(\mathbf{x}) = \frac{\partial}{\partial x_1}\left(\frac{\eta|\mathbf{v}|w(\mathbf{x})}{f_1(\mathbf{x})}\right) = \frac{\partial}{\partial x_1}(\eta w(\mathbf{x}))\frac{|\mathbf{v}|}{f_1(\mathbf{x})} + \eta w(\mathbf{x})\frac{\partial}{\partial x_1}\left(\frac{|\mathbf{v}|}{f_1(\mathbf{x})}\right).$$

It remains to show that $\widetilde{w}$ belongs to the class of smooth weight functions $S$ from Definition 6.4.5, since the result then follows by induction on $N$. But this is immediate from the observations that for any $\mathbf{x} \in [-2,2]^4$,

$$\frac{|\mathbf{v}|}{f_1(\mathbf{x})} \ll 1, \quad \frac{\partial}{\partial x_1}\left(\frac{|\mathbf{v}|}{f_1(\mathbf{x})}\right) \ll 1, \quad \text{and} \quad \frac{\partial}{\partial x_1}(\eta w) \in S. \qquad \square$$

We require one further estimate for $I_{q,\mathbf{a}}(\mathbf{c})$, which involves the second derivative test.

**Lemma 6.4.13.** *Let $\mathbf{c} \neq \mathbf{0}$. Then*

$$I_{q,\mathbf{a}}(\mathbf{c}) \ll \frac{\eta^{-4}B^{3/2+\epsilon}q}{|A|^{1/2}}\min_{1\leqslant i\leqslant 4}\left(\frac{|a_i|^{1/2}}{|c_i|}\right).$$

*Proof.* We would like to apply Fourier inversion to $w(\mathbf{x})h(r,G(\mathbf{x}))e(-\mathbf{v}\cdot\mathbf{x})$, the integrand appearing in the definition of $I_{q,\mathbf{a}}(\mathbf{c})$. The function $\mathbf{x} \mapsto h(r,G(\mathbf{x}))$ does not have compact support. We define the smooth weight $w_0 : \mathbb{R} \to \mathbb{R}_{\geqslant 0}$

by $w_0(x) = \psi(x/17)$, where $\psi(x)$ is the standard bump function in one variable, as defined in (4.4.2). Then we define the smooth weight $w_3 : R^4 \to \mathbb{R}_{\geqslant 0}$ by

$$w_3(\mathbf{x}) = \begin{cases} \frac{w(\mathbf{x})}{w_0(G(\mathbf{x}))}, & \text{if } w_0(G(\mathbf{x})) \neq 0, \\ 0, & \text{otherwise.} \end{cases}$$

Note that $w$ is supported on $[-2,2]^4$, and in this region $G(\mathbf{x})$ takes values in $[-16,16]$. Therefore $w_0(G(\mathbf{x})) \gg 1$ for all $\mathbf{x} \in \mathrm{supp}(w)$. We deduce that $\mathrm{supp}(w_3) = \mathrm{supp}(w)$ and $w(\mathbf{x}) = w_3(\mathbf{x})w_0(G(\mathbf{x}))$ for all $\mathbf{x} \in \mathbb{R}^4$. Moreover, since all the derivatives of $w_0(G(\mathbf{x}))$ are $O(1)$ for any $\mathbf{x} \in \mathrm{supp}(w)$, we have $w_3 \in S$. Applying Fourier inversion, we obtain

$$I_{q,\mathbf{a}}(\mathbf{c}) = P_1 \cdots P_4 \int_{-\infty}^{\infty} p(\theta) \int_{\mathbb{R}^4} w_3(\mathbf{x}) e(\theta G(\mathbf{x}) - \mathbf{v} \cdot \mathbf{x}) \, \mathrm{d}\mathbf{x} \, \mathrm{d}\theta, \tag{6.4.36}$$

where

$$p(\theta) = \int_{-\infty}^{\infty} w_0(k) h(r,k) e(-\theta k) \, \mathrm{d}k.$$

We have the estimate $p(\theta) \ll 1$. Indeed, taking $m = n = 0$ and $N = 2$ in [61, lemma 5] we see that

$$h(r,k) \ll r^{-1}(r^2 + \min(1, (r/|k|)^2),$$

and so

$$p(\theta) \ll r^{-1} \left( \int_{|k|<r} 1 \mathrm{d}k + \int_{r \leqslant |k| \leqslant 17} \left( \frac{r}{|k|} \right)^2 \mathrm{d}k \right) \ll r^{-1}(r + r^2 \cdot r^{-1}) \ll 1.$$

To deal with the inner integral in (6.4.36), which we denote by $I(\theta; \mathbf{v})$, we divide into the cases $5|\theta| \leqslant |\mathbf{v}|$ and $5|\theta| \geqslant |\mathbf{v}|$. In the former case, we apply Lemma 6.4.12 with $N = 2$ to obtain $I(\theta; \mathbf{v}) \ll (\eta|\mathbf{v}|)^{-2}$. The contribution to $I_{q,\mathbf{a}}(\mathbf{c})$ is

$$(\eta|\mathbf{v}|)^{-2} P_1 \cdots P_4 \int_{5|\theta| \leqslant |\mathbf{v}|} 1 \mathrm{d}\theta \ll \eta^{-2} |\mathbf{v}|^{-1} P_1 \cdots P_4.$$

In the case $5|\theta| \geqslant |\mathbf{v}|$, we use the arguments from [64, Lemma 3.2] to obtain

$$I(\theta; \mathbf{v}) \ll \left\{ \int_{\mathbb{R}^4} |\widehat{w_3}(\mathbf{y})| \mathrm{d}\mathbf{y} \right\} \sup_{\mathbf{y} \in \mathbb{R}^4} \left| \prod_{i=1}^{4} \int_{[-2,2]} e(\theta \epsilon_i x_i^2 + x_i(y_i - v_i)) \mathrm{d}x_i \right|, \tag{6.4.37}$$

where $\widehat{w_3}$ denotes the Fourier transform of $w_3$. The first factor on the right hand side of (6.4.37) is the $L^1$-norm of $\widehat{w_3}$, which we denote by $\|\widehat{w_3}\|_{L^1}$. The

$v_i$'s can be absorbed into the supremum over $\mathbf{y}$ via a change of variables, and so it remains to study

$$\int_{[-2,2]} e(\epsilon_i \theta x_i^2 - y_i x_i) \mathrm{d}x_i.$$

We can write the integrand as $e(\epsilon_i \theta \Phi(x_i))$, where $\Phi(x_i) = x_i^2 + x_i y_i \theta^{-1}$. Then $|\Phi''(x_i)| \geqslant 1$ throughout the interval $[-2, 2]$, and so we can apply the second derivative test as found in [113, Ch. 8, Proposition 2.3] to bound this integral by $|\theta|^{-1/2}$. Therefore

$$I(\mathbf{v}; \theta) \ll \|\widehat{w_3}\|_{L_1} |\theta|^{-2}.$$

Returning to (6.4.36), the contribution to $I_{q,\mathbf{a}}(\mathbf{c})$ from the range $5|\theta| \geqslant |\mathbf{v}|$ is bounded by

$$\|\widehat{w_3}\|_{L_1} P_1 \cdots P_4 \int_{|\theta| \gg |\mathbf{v}|} |\theta|^{-2} \mathrm{d}\theta \ll \|\widehat{w_3}\|_{L_1} P_1 \cdots P_4 |\mathbf{v}|^{-1}.$$

Since

$$\frac{P_1 \cdots P_4}{|\mathbf{v}|} = \frac{B^{3/2} q}{|A|^{1/2}} \min_{1 \leqslant i \leqslant 4} \left( \frac{|a_i|^{1/2}}{|c_i|} \right),$$

it remains only to show that $\|\widehat{w}_3\|_{L^1} \ll \eta^{-4}$. We have

$$\|\widehat{w}_3\|_{L^1} = \int_{|\mathbf{x}| \leqslant \eta^{-1}} |\widehat{w_3}(\mathbf{y})| \, \mathrm{d}\mathbf{y} + \int_{|\mathbf{x}| \geqslant \eta^{-1}} |\widehat{w_3}(\mathbf{y})| \, \mathrm{d}\mathbf{y}.$$

The first integral is trivially $O(\eta^{-4})$. For the second integral, we have

$$\int_{|\mathbf{x}| \geqslant \eta^{-1}} |\widehat{w_3}(\mathbf{y})| \, \mathrm{d}\mathbf{y} \ll \int_{\substack{|\mathbf{x}| \geqslant \eta^{-1} \\ |y_1| = \max_i |y_i|}} |\widehat{w_3}(\mathbf{y})| \, \mathrm{d}\mathbf{y}.$$

We can now apply integration by parts five times with respect to $x_1$ to obtain

$$\begin{aligned}
\int_{|\mathbf{y}| \geqslant \eta^{-1}} |\widehat{w_3}(\mathbf{y})| \, \mathrm{d}\mathbf{y} &\ll \int_{\substack{|\mathbf{y}| \geqslant \eta^{-1} \\ |y_1| = \max_i |y_i|}} \left| \int_{\mathbb{R}^4} \frac{\partial^5 w_3(\mathbf{x})}{\partial x_1^5} \frac{e(-\mathbf{x} \cdot \mathbf{y})}{(-2\pi i y_1)^5} \mathrm{d}\mathbf{x} \right| \mathrm{d}\mathbf{y} \\
&\ll \eta^{-5} \int_{\substack{|y_1| \geqslant \eta^{-1} \\ |y_2|, |y_3|, |y_4| \leqslant |y_1|}} y_1^{-5} \mathrm{d}\mathbf{y} \\
&\ll \eta^{-5} \int_{y_1 \geqslant \eta^{-1}} y_1^{-2} \, \mathrm{d}y_1 \\
&\ll \eta^{-4}.
\end{aligned}$$

□

We recall the notation $C_i = \eta^{-1} B^{\epsilon} |a_i|^{1/2}$ from Remark 6.4.11. We are now ready to estimate the quantity

$$E_{\mathbf{a}}(B) = \frac{1}{Q^2} \sum_{\substack{\mathbf{c} \in \mathbb{Z}^4 \setminus \{\mathbf{0}\} \\ |c_i| \ll C_i}} \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{a}}(\mathbf{c}) I_{q,\mathbf{a}}(\mathbf{c}). \tag{6.4.38}$$

Note that $I_{q,\mathbf{a}}(\mathbf{c})$ vanishes for $q \gg Q$ by the properties of the function $h$, and so we may restrict the $q$-sum to a sum over $q \ll Q$. We recall the notation $\Sigma(x;\mathbf{c}) = \sum_{q\leqslant x} q^{-3}S_{q,\mathbf{a}}(\mathbf{c})$. We would like to use Lemma 6.4.13 together with the bound for $\Sigma(x;\mathbf{c})$ from [17, Lemma 4.7] to estimate the inner sum of (6.4.38). Unfortunately, [17, Lemma 4.7] requires the dual form $F^*_{\mathbf{a}}(\mathbf{c})$ not to vanish. This was always true in [17, Section 4] due to the assumptions made in the setup, but we must treat this case separately. To this end, we let $E_{\mathbf{a}}(B) = E_{\mathbf{a},1}(B) + E_{\mathbf{a},2}(B)$, where in $E_{\mathbf{a},1}(B)$ we add the restriction $F^*_{\mathbf{a}}(\mathbf{c}) \neq 0$ to the sum over $\mathbf{c}$ in (6.4.38) and in $E_{\mathbf{a},2}(B)$ we sum over the remaining values of $\mathbf{c}$ where $F^*_{\mathbf{a}}(\mathbf{c}) = 0$.

### 6.4.3 Analysis of $E_{\mathbf{a},1}(B)$

Using Lemma 6.4.13, we have

$$E_{\mathbf{a},1}(B) \ll \frac{\eta^{-4}B^{1/2+\epsilon}}{|A|^{1/2}} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})\neq 0}} \min_{1\leqslant i\leqslant 4}\left(\frac{|a_i|^{1/2}}{|c_i|}\right) \sum_{q\ll Q} q^{-3}|S_{q,\mathbf{a}}(\mathbf{c})|.$$

For a fixed choice of $\mathbf{c}$, let $j(\mathbf{c}) \in \{1,\dots,4\}$ denote the index where $|a_i|^{1/2}|c_i|^{-1}$ is minimized. Note in particular that $c_{j(\mathbf{c})} \neq 0$. We have

$$E_{\mathbf{a},1}(B) \ll \frac{\eta^{-4}B^{1/2+\epsilon}}{|A|^{1/2}} \sum_{j=1}^{4} |a_j|^{1/2} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})\neq 0\\ j(\mathbf{c})=j}} \frac{1}{|c_j|} \sum_{q\ll Q} q^{-3}|S_{q,\mathbf{a}}(\mathbf{c})|.$$

An application of [17, Lemma 4.7] with $x = Q$ yields

$$\sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ j(\mathbf{c})=j}} \frac{1}{|c_j|} \sum_{q\ll Q} q^{-3}S_{q,\mathbf{a}}(\mathbf{c}) \ll B^{\epsilon} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i}} \frac{1}{|c_j|} \prod_{i=1}^{4} \gcd(a_i,c_i)^{1/2}.$$

For $i \neq j$, we have

$$\sum_{0\leqslant|c_i|\ll C_i} \gcd(a_i,c_i)^{1/2} \ll C_i B^{\epsilon},$$

and for $i = j$, we have

$$\sum_{0<|c_j|\ll C_j} \frac{\gcd(a_j,c_j)^{1/2}}{|c_j|} \ll B^{\epsilon}.$$

Hence

$$E_{\mathbf{a},1}(B) \ll \frac{\eta^{-4}B^{1/2+\epsilon}}{|A|^{1/2}} \sum_{j=1}^{4} |a_j|^{1/2} \prod_{i\neq j} C_i \ll \eta^{-7}B^{1/2+\epsilon}.$$

### 6.4.4 Analysis of $E_{\mathbf{a},2}(B)$

We write $E_{\mathbf{a},2}(B) = E^{(1)}_{\mathbf{a},2}(B) + E^{(2)}_{\mathbf{a},2}(B)$, where

$$E^{(1)}_{\mathbf{a},2}(B) = \frac{1}{B} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})=0}} \sum_{q\leqslant M} q^{-4} S_{q,\mathbf{a}}(\mathbf{c}) I_{q,\mathbf{a}}(\mathbf{c}),$$
$$E^{(2)}_{\mathbf{a},2}(B) = \frac{1}{B} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})=0}} \sum_{M\leqslant q\ll Q} q^{-4} S_{q,\mathbf{a}}(\mathbf{c}) I_{q,\mathbf{a}}(\mathbf{c}),$$

For a real parameter $M$ to be determined later. We recall the notation $j(\mathbf{c})$ from Section 6.4.3. To bound $E^{(1)}_{\mathbf{a},2}(B)$, we apply Lemma 6.4.13 to obtain

$$E_{2,a}(P) \ll \frac{\eta^{-4}B^{1/2+\epsilon}}{|A|^{1/2}} \sum_{j=1}^{4} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ j(\mathbf{c})=j}} \frac{|a_j|^{1/2}}{|c_j|} \sum_{q\leqslant M} q^{-3} |S_{q,\mathbf{a}}(\mathbf{c})|.$$

By [17, Lemma 4.5], we have $|S_{q,\mathbf{a}}(\mathbf{c})| \ll q^3 \prod_{i=1}^4 \gcd(a_i, c_i)^{1/2}$, and hence summing trivially over $q$ and proceeding as in Section 6.4.3, we obtain

$$E^{(1)}_{\mathbf{a},2}(B) \ll \eta^{-7} B^{1/2+\epsilon} M.$$

To bound $E^{(2)}_{\mathbf{a},2}(B)$ we require some cancellation from the sum over $q$. To achieve this, we use summation by parts, as in the treatment of the main term in Proposition 6.4.9, and then apply Lemma 6.4.8 to obtain a better estimate for the exponential sums. We also perform the $q$-sum over $R \leqslant q \leqslant 2R$ and later take a dyadic sum over $M \leqslant R \ll Q$. Summation by parts yields

$$\sum_{R\leqslant q\leqslant 2R} q^{-4} S_{q,\mathbf{a}}(\mathbf{c}) I_{q,\mathbf{a}}(\mathbf{c}) \ll -\Sigma(R;\mathbf{c}) \frac{I_{R,\mathbf{a}}(\mathbf{c})}{R} - \int_R^{2R} \Sigma(x;\mathbf{c}) \frac{\partial}{\partial x}\left(\frac{I_{x,\mathbf{a}}(\mathbf{c})}{x}\right) \mathrm{d}x. \tag{6.4.39}$$

Therefore, from Lemma 6.4.7, we obtain

$$\frac{1}{B} \sum_{R\leqslant q\leqslant 2R} q^{-4} S_{q,\mathbf{a}}(\mathbf{c}) I_{q,\mathbf{a}}(\mathbf{c}) \ll \frac{\eta^{-1} P_1 \cdots P_4}{BR} \sup_{R\leqslant x\leqslant 2R} |\Sigma(x;\mathbf{c})|. \tag{6.4.40}$$

We recall the definition of $\Delta_{\mathbf{c}}(\mathbf{a})$ from (6.4.30). Using the estimate for $|\Sigma(x;\mathbf{c})|$

from Lemma 6.4.8, we have

$$E^{(2)}_{\mathbf{a},2}(B) \ll \frac{\eta^{-1}P_1\cdots P_4|A|^{3/16}}{B} \sum_{\substack{R \text{ dyadic}\\ M/2\leqslant R\ll Q}} R^{-1/2+\epsilon} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})=0}} \Delta_{\mathbf{c}}(\mathbf{a})^{3/8}$$

$$\ll \frac{\eta^{-1}B^{1+\epsilon}}{M^{1/2}|A|^{5/16}} \sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})=0}} \Delta_{\mathbf{c}}(\mathbf{a})^{3/8}. \tag{6.4.41}$$

It is possible to obtain the asymptotic formula from Theorem 6.1.1 (albeit with a smaller power saving) by bounding the sum in (6.4.41) trivially by $C_1\cdots C_4\Delta^{3/8}$. However, in order to obtain the error terms claimed in Theorem 6.4.2, we now make use of the constraint $F^*_{\mathbf{a}}(\mathbf{c}) = 0$ in the $\mathbf{c}$-sum to obtain a more refined estimate. In the following two lemmas, we adopt the notation that $\mathbf{vw} = (v_1w_1, \dots, v_4w_4)$ for vectors $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^4$.

**Lemma 6.4.14.** *For any $\boldsymbol{d}, \boldsymbol{e} \in (\mathbb{Z}_{\neq 0})^4$, we have*

$$\Delta(\boldsymbol{de}) \leqslant (d_1\cdots d_4)^2\Delta(\boldsymbol{e}).$$

*Proof.* Fix a prime $p$, and define $\delta_i = \nu_p(d_i), \varepsilon_i = \nu_p(e_i)$ for $i \in \{1, \dots, 4\}$. Without loss of generality, we may assume that $\varepsilon_1 \leqslant \cdots \leqslant \varepsilon_4$. Then

$$\begin{aligned}\nu_p(\Delta(\boldsymbol{de})) &= \sum_{i=1}^4 \min\left(\delta_i+\varepsilon_i, \sum_{j\neq i}(\delta_j+\varepsilon_j)\right)\\ &\leqslant \sum_{i=1}^3(\delta_i+\varepsilon_i) + \min\left(\delta_4+\varepsilon_4, \sum_{i=1}^3(\delta_i+\varepsilon_i)\right),\end{aligned}$$

and

$$\nu_p(\Delta(\boldsymbol{e})) = \sum_{i=1}^3\varepsilon_i + \min\left(\varepsilon_4, \sum_{i=1}^3\varepsilon_i\right).$$

Therefore

$$\begin{aligned}\nu_p(\Delta(\boldsymbol{de})) - \nu_p(\Delta(\boldsymbol{e})) &\leqslant \begin{cases}\sum_{i=1}^3 2\delta_i, & \text{if } \varepsilon_1+\varepsilon_2+\varepsilon_3 \leqslant \varepsilon_4,\\ \sum_{i=1}^4\delta_i, & \text{otherwise.}\end{cases}\\ &\leqslant \nu_p((d_1\cdots d_4)^2).\end{aligned}$$

Taking a product over all primes $p$ completes the proof of the lemma. □

**Lemma 6.4.15.** *We have*

$$\sum_{\substack{\mathbf{c}\in\mathbb{Z}^4\setminus\{\mathbf{0}\}\\ |c_i|\ll C_i\\ F^*_{\mathbf{a}}(\mathbf{c})=0}} \Delta_{\mathbf{c}}(\mathbf{a})^{3/8} \ll \eta^{-3}B^{\epsilon}\Delta^{1/2}.$$

*Proof.* For a nonzero integer $m$, we define $\mathrm{sqf}(m)$ to be the smallest positive integer $r$ such that $|m|/r$ is a square. For $i \in \{1, \dots, 4\}$, we decompose $a_i$ into a product $a_i = e_i n_i k_i^2$, where

$$e_i = \gcd\left(a_i, \prod_{j \neq i} a_j\right), \quad n_i = \mathrm{sqf}(a_i/e_i), \quad k_i^2 = a_i/(e_i n_i).$$

By definition, we have $\prod_{i=1}^4 e_i = \Delta$. For any $i \in \{1, \dots, 4\}$, it is clear that

$$F_{\mathbf{a}}^*(\mathbf{c}) = 0 \implies a_i | c_i^2 \prod_{j \neq i} a_j \implies n_i k_i^2 | c_i^2 \implies n_i k_i | c_i. \tag{6.4.42}$$

We divide up the sum over $\mathbf{c}$ according to how many of the coordinates $c_1, \dots, c_4$ are equal to zero. At most two of the coordinates can be zero, due to the assumptions $\mathbf{c} \neq 0$ and $F_{\mathbf{a}}^*(\mathbf{c}) = 0$. Up to reordering the indices, we obtain

$$\sum_{\substack{\mathbf{c} \in \mathbb{Z}^4 \setminus \{\mathbf{0}\} \\ |c_i| \ll C_i \\ F_{\mathbf{a}}^*(\mathbf{c}) = 0}} \Delta_{\mathbf{c}}(\mathbf{a})^{3/8} \ll T_0 + T_1 + T_2, \tag{6.4.43}$$

where

$$\begin{aligned} T_0 &= \sum_{\substack{\mathbf{c} \in (\mathbb{Z}_{\neq 0})^4 \\ |c_i| \ll C_i \\ F_{\mathbf{a}}^*(\mathbf{c}) = 0}} \Delta_{\mathbf{c}}(\mathbf{a})^{3/8}, \\ T_1 &= \sum_{\substack{\mathbf{c} \in (\mathbb{Z}_{\neq 0})^3 \\ |c_i| \ll C_i \\ F_{\mathbf{a}}^*((\mathbf{c},0)) = 0}} \Delta_{(\mathbf{c},0)}(\mathbf{a})^{3/8}, \\ T_2 &= \sum_{\substack{\mathbf{c} \in (\mathbb{Z}_{\neq 0})^2 \\ |c_i| \ll C_i \\ F_{\mathbf{a}}^*((\mathbf{c},0,0)) = 0}} \Delta_{(\mathbf{c},0,0)}(\mathbf{a})^{3/8}. \end{aligned}$$

We begin by studying $T_0$. Given that $F_{\mathbf{a}}^*(\mathbf{c}) = 0$, we only need to take the sum over $c_1, c_2$ and $c_3$, because this implicitly determines (up to sign) the value of

$c_4$. Together with (6.4.42), this implies that

$$\begin{aligned} T_0 &\leqslant \sum_{\substack{c_1,c_2,c_3\in\mathbb{Z}_{\neq 0}\\ |c_i|\ll C_i\\ n_ik_i|c_i}} \Delta_{\mathbf{c}}(\mathbf{a})^{3/8} \qquad (6.4.44)\\ &\leqslant \sum_{\substack{c_1,c_2,c_3\in\mathbb{Z}_{\neq 0}\\ |c_i|\ll C_i/(n_ik_i)}} \prod_{i=1}^{4} \gcd\left(n_ik_i\gcd(a_i,c_i), \prod_{j\neq i} n_jk_j\gcd(a_j,c_j)\right)^{3/8}\\ &\leqslant \sum_{\substack{\boldsymbol{d}\in(\mathbb{Z}_{\neq 0})^4\\ d_i\ll C_i/(n_ik_i),\\ d_i|a_i}} \sum_{\substack{c_1,c_2,c_3\in\mathbb{Z}_{\neq 0}\\ |c_i|\ll C_i/(n_ik_i)\\ d_i|c_i}} \Delta(\boldsymbol{dnk})^{3/8}\\ &\ll \left(\prod_{i=1}^{3}\frac{C_i}{n_ik_i}\right) \sum_{\substack{\boldsymbol{d}\in(\mathbb{Z}_{\neq 0})^4\\ d_i\ll C_i/(n_ik_i)\\ d_i|a_i}} \Delta(\boldsymbol{nk})^{3/8}\prod_{i=1}^{4} d_i^{-1/4}, \qquad (6.4.45) \end{aligned}$$

where in the last line we have applied Lemma 6.4.14. However, $\Delta(\boldsymbol{nk}) = 1$ by the definition of $e_1,\dots,e_4$. There are $O(A^\epsilon)$ choices for $\boldsymbol{d}$ in the sum in (6.4.45), and each summand is bounded by $1$. Therefore

$$T_0 \ll \left(\prod_{i=1}^{3}\frac{C_i}{n_ik_i}\right) A^\epsilon. \qquad (6.4.46)$$

Returning to (6.4.46) and recalling that $C_i = \eta^{-1}B^\epsilon|a_i|^{1/2} = \eta^{-1}B^\epsilon(e_in_i)^{1/2}k_i$, we conclude that

$$T_0 \ll \eta^{-3}B^\epsilon\left(\prod_{i=1}^{3}\frac{|a_i|^{1/2}}{n_ik_i}\right) \leqslant \eta^{-3}B^\epsilon\Delta^{1/2}.$$

The approach for estimating $T_1$ and $T_2$ is very similar, so we focus on the main differences. It is sufficient to only use the divisibility conditions from (6.4.42) in these cases. For $T_1$, all the sums in the above argument will be over vectors indexed by $\{1,2,3\}$, because we have fixed $c_4 = 0$. We have

$$\begin{aligned} T_1 &\ll \left(\prod_{i=1}^{3}\frac{C_i}{n_ik_i}\right) A^\epsilon\Delta(n_1k_1,n_2k_2,n_3k_3,a_4)^{3/8}\\ &= \left(\prod_{i=1}^{3}\frac{C_i}{n_ik_i}\right) A^\epsilon\\ &\ll \eta^{-3}B^\epsilon\Delta^{1/2}. \end{aligned}$$

For $T_2$, we only take sums over vectors indexed by $\{1,2\}$, since we have fixed $c_3 = c_4 = 0$. We have

$$\begin{aligned} T_2 &\ll \left(\prod_{i=1}^{2} \frac{C_i}{n_i k_i}\right) A^{\epsilon} \Delta(n_1 k_1, n_2 k_2, a_3, a_4)^{3/8} \\ &= \left(\prod_{i=1}^{2} \frac{C_i}{n_i k_i}\right) A^{\epsilon} (a_3, a_4)^{3/4} \\ &\leqslant \eta^{-2} B^{\epsilon} (e_1 e_2)^{1/2} (e_3 e_4)^{3/8} \\ &\ll \eta^{-2} B^{\epsilon} \Delta^{1/2}. \end{aligned}$$

Thus each of $T_0, T_1, T_2$ is bounded by $\eta^{-3} B^{\epsilon} \Delta^{1/2}$, as required. □

Recalling (6.4.41), we therefore have

$$E^{(2)}_{2,\mathbf{a}}(B) \ll \frac{\eta^{-4} B^{1+\epsilon} \Delta^{1/2}}{M^{1/2} |A|^{5/16}}.$$

To combine with the error term $E^{(1)}_{2,\mathbf{a}}(B)$, we make the choice

$$M = \eta B^{1/3} \Delta^{1/3} |A|^{-5/24}.$$

This yields the estimate

$$E_{\mathbf{a}}(B) \ll \frac{\eta^{-6} B^{5/6+\epsilon} \Delta^{1/3}}{|A|^{5/24}} + \eta^{-7} B^{1/2+\epsilon}. \tag{6.4.47}$$

This estimate is larger than the error term from Proposition 6.4.9. Indeed, it features a larger power of $B$ and $\eta^{-1}$, and $\Delta^{1/3} |A|^{-5/24} \geqslant \Delta^{3/8} |A|^{-5/16}$ by applying the trivial bound $\Delta \leqslant |A|$. Combining with Proposition 6.4.9 this completes the proof of Theorem 6.4.4.

The final ingredient in the proof of Theorem 6.4.2 is an estimate for the singular series $\mathfrak{G}_{\mathbf{a}}$.

**Lemma 6.4.16.** *Let $\mathbf{a} \in (\mathbb{Z}_{\neq 0})^4$ and assume that $A \neq \square$. Then*

$$|\mathfrak{G}_{\mathbf{a}}| \ll |A|^{\epsilon} \Delta^{1/4}.$$

*Proof.* Beginning with the definition of the singular series, we have

$$\mathfrak{G}_{\mathbf{a}} = \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{a}}(\mathbf{0}) = \sum_{q \leqslant T} q^{-4} S_{q,\mathbf{a}}(\mathbf{0}) + \sum_{q > T} q^{-4} S_{q,\mathbf{a}}(\mathbf{0})$$

for any $T \geqslant 1$. For the sum over $q > T$, we apply partial summation and Lemma 6.4.8. We have

$$\sum_{q>T} q^{-4} S_{q,\mathbf{a}}(\mathbf{0}) = \frac{-\Sigma(T;\mathbf{0})}{T} - \int_T^\infty \Sigma(x;\mathbf{0}) \frac{\partial}{\partial x}(x^{-1})\,\mathrm{d}x \ll T^{-1/2+\epsilon}|A|^{3/16+\epsilon}\Delta^{3/8}.$$

By choosing $T = |A|^2$, we can ensure that the contribution from this region is negligible.

For the remaining sum over $q \leqslant T$, we follow a similar argument to the proof of Lemma 6.4.8. Using the multiplicativity of $S_{q,\mathbf{a}}(\mathbf{0})$ in $q$ and [17, Lemma 4.6], we have

$$\begin{aligned}\sum_{q\leqslant T} q^{-4} S_{q,\mathbf{a}}(\mathbf{0}) &\ll \left(\sum_{\substack{q_1\leqslant T\\ \gcd(q_1,2A)=1}} \left(\frac{A}{q_1}\right)\frac{\varphi(q_1)}{q_1^2}\right)\left(\sum_{\substack{q_2\leqslant T/q_1\\ q_2\mid(2A)^\infty}} q_2^{-4} S_{q_2,\mathbf{a}}(\mathbf{0})\right)\\ &\ll T^\epsilon |A|^\epsilon \max_{q\mid(2A)^\infty}\left(\frac{\prod_{i=1}^4 \gcd(q,a_i)^{1/2}}{q}\right),\end{aligned}$$

where in the second line we have estimated the sum over $q_1$ trivially, and the sum over $q_2$ by applying [17, Lemma 4.5]. We let $m_{i,p}$ denote the $i$th smallest element of $\nu_p(a_1),\dots,\nu_p(a_4)$. We define

$$L_p = \nu_p\left(\frac{\prod_{i=1}^4 \gcd(q,a_i)}{q^2}\right), \quad k_p = \nu_p(q).$$

Then

$$L_p = \sum_{i=1}^4 \min(k_p, m_{i,p}) - 2k_p.$$

The maximum possible value of $L_p$ is attained by choosing $k_p = m_{2,p}$, and so $L_p \leqslant m_{1,p} + m_{2,p}$. We have

$$\nu_p(\Delta) = m_{1,p}+m_{2,p}+m_{3,p}+\min(m_{1,p}+m_{2,p}+m_{3,p}, m_{4,p}) \geqslant 2(m_{1,p}+m_{2,p}),$$

and so $L_p \leqslant \nu_p(\Delta)/2$. Taking a product over $p|2A$ completes the proof of the lemma. □

## 6.5 Proof of Theorem 6.1.1

We recall that the quantity $N_{\mathbf{a}}(B)$ studied in Section 6.4 did not involve any primitivity conditions. In order to insert the condition $\gcd(z_1,\dots,z_4) = 1$, we apply an inclusion-exclusion argument which is a special case of [23, Section 3].

We begin by fixing some notation which we shall use throughout this section. Let $z_1, \dots, z_4$ denote nonzero squareful numbers, and $x_1, \dots, x_4 \in \mathbb{N}$, $y_1, \dots, y_4 \in \mathbb{Z}_{\neq 0}$ the unique integers such that $z_i = x_i^2 y_i^3$ and $y_i$ is squarefree for all $i$. Let $A = a_1 \cdots a_4, R = r_1 \cdots r_4, S = s_1 \cdots s_4$ and $Y = y_1 \cdots y_4$. For vectors $\mathbf{v}, \mathbf{w} \in \mathbb{N}^4$, we write $\mathbf{v}|\mathbf{w}$ to mean $v_i|w_i$ for all $i = 1, \dots, 4$. For an integer $m$, we write $\mathbf{v}|m$ for $v_i|m$ for all $i = 1, \dots, 4$, and $\gcd(m, \mathbf{v})$ for $(\gcd(m, v_1), \dots, \gcd(m, v_4))$. We also define $\mathbf{v}^{[m]}$ to be the vector in $\mathbb{N}^4$ with $i$th coordinate $v_i^{[m]} = \prod_{p|m} p^{\nu_p(v_i)}$, where $\nu_p$ denotes the $p$-adic valuation.

We recall from Proposition 6.3.1 that

$$N(B) = N(D, B) + O(B^{1+\epsilon} D^{-1/12}), \tag{6.5.1}$$

where $N(B)$ is defined in (6.1.5) and $N(D, B)$ is defined in the same way but with the additional constraint $|Y| \leqslant D$. For $\mathbf{r}, \mathbf{s} \in \mathbb{N}^4$ and $s_0 \in \mathbb{N}$, we define

$$\mathscr{N}(B; \mathbf{r}, \mathbf{s}, s_0) = \left\{ \mathbf{z} \in (\mathbb{Z}_{\neq 0})^4 : \begin{array}{l} |\mathbf{z}| \leqslant B, z_1 + \cdots + z_4 = 0, \\ z_i = x_i^2 y_i^3 \text{ squareful for all } i, \\ |Y| \leqslant D, Y \neq \square, \mathbf{r}|\mathbf{y}, \mathbf{s}|\mathbf{x}, s_0|\mathbf{x} \end{array} \right\}.$$

**Definition 6.5.1.** Given $\mathbf{r}, \mathbf{s} \in \mathbb{N}^4$ and $s_0 \in \mathbb{N}$, we define $\omega(\mathbf{r}, \mathbf{s}, s_0)$ as follows:

1. $\omega(\mathbf{r}, \mathbf{s}, s_0) = \mu(s_0) \prod_p \omega(\mathbf{r}^{[p]}, \mathbf{s}^{[p]}, 1)$. In particular, $\omega(\mathbf{1}, \mathbf{1}, s_0) = \mu(s_0)$.
2. If one of $r_1, \dots, r_4, s_1, \dots, s_4$ is not squarefree, then $\omega(\mathbf{r}, \mathbf{s}, s_0) = 0$.
3. If $\gcd(s_1, \dots, s_4) > 1$ then $\omega(\mathbf{r}, \mathbf{s}, s_0) = 0$.
4. If $\gcd(s_0, \mathbf{s}) \neq \mathbf{1}$, then $\omega(\mathbf{r}, \mathbf{s}, s_0) = 0$.
5. If $p|RS$ but $p \nmid r_i s_i$ for some $i$, then $\omega(\mathbf{r}^{[p]}, \mathbf{s}^{[p]}, 1) = 0$.
6. If $p|r_i s_i$ for every $i$, $\gcd(s_1, \dots, s_4) = 1$, $\gcd(s_0, \mathbf{s}) = \mathbf{1}$, and $r_i, s_i$ are squarefree for every $i$, then $k := \nu_p(RS)$ satisfies $4 \leqslant k \leqslant 7$. Define $\omega(\mathbf{r}^{[p]}, \mathbf{s}^{[p]}, 1) = (-1)^{k+1}$.

The motivation for this choice of $\omega$ comes from the following lemma.

**Lemma 6.5.2.** *We have*

$$N(D, B) = \sum_{\substack{\mathbf{r}, \mathbf{s} \in \mathbb{N}^4 \\ s_0 \in \mathbb{N}}} \omega(\mathbf{r}, \mathbf{s}, s_0) \# \mathscr{N}(B; \mathbf{r}, \mathbf{s}, s_0). \tag{6.5.2}$$

*Proof.* We write the right hand side of (6.5.2) as

$$\sum_{\mathbf{z}\in\mathscr{N}(B;\mathbf{1},\mathbf{1},1)} \sum_{\substack{\mathbf{r},\mathbf{s},s_0\\ \mathbf{r}|\mathbf{y},\mathbf{s}|\mathbf{x},s_0|\mathbf{x}}} \omega(\mathbf{r},\mathbf{s},s_0). \tag{6.5.3}$$

We would like to show that the inner sum is the indicator function for the condition $\gcd(z_1,\dots,z_4)=1$. If $\gcd(z_1,\dots,z_4)=1$, then by property $(5)$ of Definition 6.5.1, the only nonzero term in the inner sum of (6.5.3) is the term $\omega(\mathbf{1},\mathbf{1},1)=1$. From now on, we suppose that $\gcd(z_1,\dots,z_4)>1$. By properties $(1)$ and $(2)$ from Definition 6.5.1, it suffices to show that for any prime $p$ dividing $\gcd(z_1,\dots,z_4)$, we have

$$\sum_{\substack{\mathbf{r},\mathbf{s}\in\mathbb{N}^4,s_0\in\mathbb{N}\\ \mathbf{r}|\gcd(p,\mathbf{y}),\mathbf{s}|\gcd(p,\mathbf{x}),s_0|\gcd(p,\mathbf{x})}} \omega(\mathbf{r},\mathbf{s},s_0)=0. \tag{6.5.4}$$

The condition $s_0|\gcd(p,\mathbf{x})$ implies that $s_0=1$ or $s_0=p$. Moreover, if $s_0=p$ and $\omega(\mathbf{r},\mathbf{s},s_0)\neq 0$, then by $(4)$ and $(5)$ of Definition 6.5.1, we have $\mathbf{s}=\mathbf{1}$ and $\mathbf{r}=\mathbf{1}$ or $\mathbf{r}=(p,p,p,p)$. Therefore the left hand side of (6.5.4) becomes

$$\mu(p)(\omega(\mathbf{1},\mathbf{1},1)+\omega((p,p,p,p),\mathbf{1},1))=-(1-1)=0.$$

Now suppose that $s_0=1$. Let $k_0$ denote the number of $y_1,\dots,y_4,x_1,\dots,x_4$ that are a multiple of $p$, and let $k$ denote the number of $r_1,\dots,r_4,s_1,\dots,s_4$ that are a multiple of $p$. If $\omega(\mathbf{r},\mathbf{s},1)\neq 0$, then we have $k\leqslant k_0$ and $k_0=4,5$ or $6$. Indeed, if $p$ divides seven of $y_1,\dots,y_4,x_1,\dots,x_4$ then it must also divide the eighth, which contradicts condition $(3)$ from Definition 6.5.1, and so $k_0=7,8$ are not possible. We go through the cases $k_0=4,5,6$ in turn. For convenience we write $\omega(\mathbf{r},\mathbf{s},1)=\omega(k)$ and $\omega(\mathbf{1},\mathbf{1},1)=\omega(0)=1$.

If $k_0=4$, there is one summand of (6.5.4) with $k=0$, namely $(\mathbf{r},\mathbf{s})=(\mathbf{1},\mathbf{1})$, and one with $k=4$, and all other terms are zero. Therefore the contribution to the sum in (6.5.4) from $k_0=4$ is $\omega(0)+\omega(4)=1-1=0$. If $k_0=5$, then there is one summand in (6.5.4) with $k=0$, two with $k=4$ and one with $k=5$, and so we obtain $\omega(0)+2\omega(4)+\omega(5)=1-2+1=0$. The relevant calculation for $k=6$ is

$$\omega(0)+4\omega(4)+4\omega(5)+\omega(6)=1-4+4-1=0.$$

We have therefore established that (6.5.4) holds. □

We now use Theorem 4.5.1 to estimate $\#\mathscr{N}(B;\mathbf{r},\mathbf{s},s_0)$ for each choice of $\mathbf{r},\mathbf{s}\in\mathbb{N}^4, s_0\in\mathbb{N}$ satisfying $\omega(\mathbf{r},\mathbf{s},s_0)\neq 0$. We have

$$\#\mathscr{N}(B;\mathbf{r},\mathbf{s},s_0)=\sum_{\boldsymbol{\epsilon}\in\{\pm1\}^4}\sum_{\substack{|Y|\leqslant D,Y\neq\square\\ \operatorname{sgn} y_i=\epsilon_i\\ \mathbf{r}|\mathbf{y}}}\mu^2(y_1)\cdots\mu^2(y_4)N_{\mathbf{y}}(B;\mathbf{s},s_0),$$

where

$$N_{\mathbf{y}}(B;\mathbf{s},s_0)=\#\left\{\mathbf{x}\in\mathbb{N}^4:\ \begin{array}{l}\sum_{i=1}^4 y_i^3x_i^2=0,\mathbf{s}|\mathbf{x},s_0|\mathbf{x},\\ |x_i|\leqslant\left(\frac{B}{|y_i|^3}\right)^{1/2}\ \text{for all } i\end{array}\right\}. \tag{6.5.5}$$

We make use of condition $(4)$ from Definition 6.5.1, which allows us to make a change of variables from $x_i$ to $s_0s_ix_i$. In the notation of (6.1.8), we have $N_{\mathbf{y}}(B;\mathbf{s},s_0)=\frac{1}{16}N_{\mathbf{s}^2\mathbf{y}^3}(B/s_0^2)$, where $\mathbf{s}^2\mathbf{y}^3$ denotes the vector $(s_1^2y_1^3,\dots,s_4^2y_4^3)$, and the factor $\frac{1}{16}$ compensates for changing from counting over $\mathbb{N}^4$ to counting over $(\mathbb{Z}_{\neq 0})^4$. Assuming $Y\neq\square$, we have $S^2Y^3\neq\square$. Moreover, we note that the conditions $\omega(\mathbf{r},\mathbf{s},s_0)\neq 0$ and $\mathbf{r}|\mathbf{y}$ imply that $S|Y^3$. (Indeed, if $\omega(\mathbf{r},\mathbf{s},s_0)\neq 0$, then by conditions (2) and (3) of Definition 6.5.1, $S$ must be fourth-power free. Since condition (5) implies that every prime dividing $S$ must also divide $R$, we deduce that $S|R^3$, and together with the assumption $\mathbf{r}|\mathbf{y}$, this implies that $S|Y^3$.) Therefore $|Y|\leqslant D$ implies that $|S^2Y^3|\leqslant D^9$. In particular, we have $|S^2Y^3|\leqslant B^{4/7}$ when $D\leqslant B^{1/16}$. Hence we may apply Theorem 6.4.2 with $\mathbf{a}=\mathbf{s}^2\mathbf{y}^3$ to deduce that for any $D\leqslant B^{1/16}$,

$$\begin{aligned}&\#\mathscr{N}(B;\mathbf{r},\mathbf{s},s_0)\\&\quad=\frac{1}{16}\sum_{\boldsymbol{\epsilon}\in\{\pm1\}^4}\sum_{\substack{|Y|\leqslant D\\ \operatorname{sgn}y_i=\epsilon_i\\ \mathbf{r}|\mathbf{y},Y\neq\square\\ y_i\ \text{squarefree}}}\left(\frac{\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}\sigma_\infty(\boldsymbol{\epsilon})B}{S|Y|^{3/2}s_0^2}+O\left(\frac{B^{41/42+\epsilon}\Delta^{1/3}}{|S^2Y^3|^{11/24}}\right)\right),\end{aligned} \tag{6.5.6}$$

where as in Section 6.4, we define

$$\Delta=\Delta(\mathbf{s}^2\mathbf{y}^3)=\prod_{i=1}^4\gcd\left(s_i^2y_i^3,\prod_{j\neq i}s_j^2y_j^3\right).$$

We begin by studying the main term from (6.5.6). We would like to replace the sum over $|Y|\leqslant D$ with a sum over all $\mathbf{y}\in(\mathbb{Z}_{\neq 0})^4$ satisfying $\operatorname{sgn}y_i=\epsilon_i$ for all $i$. In order to estimate the error term in doing so, we appeal to Lemma 6.4.16. We define

$$E_1(D)=\frac{1}{16}\sum_{\substack{\mathbf{r},\mathbf{s}\in\mathbb{N}^4\\ s_0\in\mathbb{N}}}\omega(\mathbf{r},\mathbf{s},s_0)\sum_{\boldsymbol{\epsilon}\in\{\pm1\}^4}\sum_{\substack{\mathbf{y}\in(\mathbb{Z}_{\neq0})^4\\ Y>D,Y\neq\square\\ \operatorname{sgn}y_i=\epsilon_i\\ \mathbf{r}|\mathbf{y}}}\frac{\mu^2(y_1)\cdots\mu^2(y_4)\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}\sigma_\infty(\boldsymbol{\epsilon})}{S|Y|^{3/2}s_0^2}.$$

**Lemma 6.5.3.** *For any $D\geqslant 1$, we have $E_1(D)=O(D^{-1/4+\epsilon})$.*

*Proof.* From the observation $S|Y^3$ made above, and the fact that $\sigma_\infty(\boldsymbol{\epsilon})\ll 1$, we have

$$E_1(D)\ll\sum_{\boldsymbol{\epsilon}\in\{\pm1\}^4}\sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y>D,Y\neq\square}}Y^{-3/2}\sum_{\substack{\mathbf{s}\in\mathbb{N}^4\\ S|Y^3}}\frac{|\mathfrak{G}_{\boldsymbol{\epsilon}\mathbf{s}^2\mathbf{y}^3}|}{S}\sum_{s_0\in\mathbb{N}}\sum_{\substack{\mathbf{r}\in\mathbb{N}^4\\ R|Y}}\frac{|\omega(\mathbf{r},\mathbf{s},s_0)|}{s_0^2}.$$

Since $|\omega(\mathbf{r},\mathbf{s},s_0)| \leqslant 1$, the sum over $s_0$ is convergent. The sum over $\mathbf{r}$ only contributes $O(Y^\epsilon)$ by the trivial bound for the divisor function. Applying the estimate from Lemma 6.4.16, we have $|\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}| \ll (SY)^\epsilon \Delta(\mathbf{s}^2\mathbf{y}^3)^{1/4}$ whenever $Y \neq \square$. Therefore

$$E_1(D) \ll \sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y>D}} Y^{-3/2+\epsilon} \sum_{\substack{\mathbf{s}\in\mathbb{N}^4\\ S|Y^3}} \frac{\Delta(\mathbf{s}^2\mathbf{y}^3)^{1/4}}{S^{1-\epsilon}}. \tag{6.5.7}$$

From Lemma 6.4.14, we have $\Delta(\mathbf{s}^2\mathbf{y}^3) \leqslant S^4\Delta(\mathbf{y}^3)$. Continuing from (6.5.7), we obtain the estimate

$$E_1(D) \ll \sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y>D}} \frac{\Delta(\mathbf{y}^3)^{1/4}}{Y^{3/2-\epsilon}} \sum_{\substack{\mathbf{s}\in\mathbb{N}^4\\ S|Y^3}} S^\epsilon \ll \sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y>D}} \frac{\Delta(\mathbf{y})^{3/4}}{Y^{3/2-\epsilon}}.$$

We note that $\Delta(\mathbf{y})$ is always squareful. Therefore, for any $R \geqslant 1$, there are $O(R^{1/2})$ possible values for $\Delta(\mathbf{y})$ in the range $[R, 2R]$. We define the quantity $M(\mathbf{y}) = Y/\Delta(\mathbf{y})$. For a given $M, \Delta \geqslant 1$, the conditions $M = M(\mathbf{y}), \Delta = \Delta(\mathbf{y})$ uniquely determine $Y$, and so by the trivial bound for the divisor function, there are $O(Y^\epsilon) = O((M\Delta)^\epsilon)$ choices for $\mathbf{y}$ satisfying $M = M(\mathbf{y}), \Delta = \Delta(\mathbf{y})$. Breaking into dyadic intervals, we obtain

$$\begin{aligned}\sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y>D}} \frac{\Delta(\mathbf{y})^{3/4}}{Y^{3/2-\epsilon}} &\ll \sum_{\substack{R_1,R_2 \text{ dyadic}\\ R_1R_2>D/2}} R_1R_2^{1/2} \max_{\substack{\mathbf{y}\in\mathbb{N}^4\\ R_1\leqslant M(\mathbf{y})\leqslant 2R_1\\ R_2\leqslant\Delta(\mathbf{y})\leqslant 2R_2}} M(\mathbf{y})^{-3/2+\epsilon}\Delta(\mathbf{y})^{-3/4+\epsilon}\\ &\ll \sum_{\substack{R_1,R_2 \text{ dyadic}\\ R_1R_2>D/2}} R_1^{-1/2+\epsilon}R_2^{-1/4+\epsilon}\\ &\ll D^{-1/4+\epsilon},\end{aligned}$$

as required. □

We now study the error term

$$E_2(D) = \sum_{\substack{\mathbf{r},\mathbf{s}\in\mathbb{N}^4\\ s_0\in\mathbb{N}}} \omega(\mathbf{r},\mathbf{s},s_0) \sum_{\boldsymbol{\epsilon}\in\{\pm1\}^4} \sum_{\substack{|Y|\leqslant D, Y\neq\square\\ \operatorname{sgn} y_i=\epsilon_i\\ \mathbf{r}|\mathbf{y},\\ y_i \text{ squarefree}}} \frac{\Delta(\mathbf{s}^2\mathbf{y}^3)^{1/3}}{|S^2Y^3|^{11/24}}. \tag{6.5.8}$$

**Lemma 6.5.4.** *We have* $E_2(D) \ll D^{11/8+\epsilon}$.

*Proof.* We proceed in a similar fashion to the proof of Lemma 6.5.3. Let $M(\mathbf{y})$ be as defined in Lemma 6.5.3. Then

$$\begin{aligned}
E_2(D) &\ll \sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y\leqslant D}} \sum_{\substack{\mathbf{s}\in\mathbb{N}^4\\ S|Y^3}} \frac{\Delta(\mathbf{s}^2\mathbf{y}^3)^{1/3}}{(S^2Y^3)^{11/24-\epsilon}} \\
&\ll \sum_{\substack{\mathbf{y}\in\mathbb{N}^4\\ Y\leqslant D}} \frac{\Delta(\mathbf{y})}{Y^{11/8-\epsilon}} \sum_{\substack{\mathbf{s}\in\mathbb{N}^4\\ S|Y^3}} S^{5/12+\epsilon} \\
&\ll \sum_{\substack{R_1,R_2 \text{ dyadic}\\ R_1R_2\leqslant 2D}} R_1R_2^{1/2} \max_{\substack{\mathbf{y}\in\mathbb{N}^4\\ R_1\leqslant M(\mathbf{y})\leqslant 2R_1\\ R_2\leqslant \Delta(\mathbf{y})\leqslant 2R_2}} M(\mathbf{y})^{-1/8+\epsilon}\Delta(\mathbf{y})^{7/8+\epsilon} \\
&\ll \sum_{\substack{R_1,R_2 \text{ dyadic}\\ R_1R_2\leqslant 2D}} R_1^{7/8+\epsilon}R_2^{11/8+\epsilon} \\
&\ll D^{11/8+\epsilon}.
\end{aligned}$$

□

We now conclude the proof of Theorem 6.1.1. Combining (6.5.1), Lemma 6.5.2, (6.5.6), Lemma 6.5.3 and Lemma 6.5.4, for any $D \leqslant B^{1/16}$, we have

$$N(B) = cB + O(B^{1+\epsilon}D^{-1/12}) + O(B^{41/42+\epsilon}D^{11/8}),$$

where

$$c = \frac{1}{16}\sum_{\boldsymbol{\epsilon}\in\{\pm 1\}^4}\sigma_\infty(\boldsymbol{\epsilon}) \sum_{\substack{\mathbf{y}\in(\mathbb{Z}_{\neq 0})^4\\ \operatorname{sgn}(y_i)=\epsilon_i\\ Y\neq\square}} \frac{\mu^2(y_1)\cdots\mu^2(y_4)}{|Y|^{3/2}} \sum_{\substack{\mathbf{r},\mathbf{s}\in\mathbb{N}^4\\ s_0\in\mathbb{N}\\ \mathbf{r}|\mathbf{y}}} \frac{\omega(\mathbf{r},\mathbf{s},s_0)\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}}{Ss_0^2}. \tag{6.5.9}$$

Making the choice $D = B^{4/245}$, we obtain $N(B) = cB + O(B^{734/735+\epsilon})$.

## 6.6 The leading constant

The expression for the leading constant in (6.5.9) is analogous to [23, Equation (3.14)]. Similarly to [23, Equation (3.15)], we now demonstrate that the inner sum of (6.5.9) can be expressed as a product of local densities. We define

$$M_n(\mathbf{y},p) = \#\left\{\mathbf{m} \pmod{p^n} : \sum_{i=1}^4 y_i^3m_i^2 \equiv 0 \pmod{p^n}, p\nmid m_jy_j \text{ for some } j\right\}$$

for any prime $p$ and any $n \in \mathbb{N}$.

**Lemma 6.6.1.** *We have*

$$\sum_{\substack{\mathbf{r},\mathbf{s}\in\mathbb{N}^4\\ s_0\in\mathbb{N}\\ \mathbf{r}|\mathbf{y}}} \frac{\omega(\mathbf{r},\mathbf{s},s_0)\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}}{Ss_0^2} = \prod_p \lim_{N\to\infty}\left(\frac{M_N(\mathbf{y},p)}{p^{3N}}\right).$$

*Proof.* We first express the singular series $\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}$ as a product of local densities. Since $\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3} = \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0})$, and $S_{q,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0})$ is multiplicative in $q$, we have

$$\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3} = \sum_{q=1}^{\infty} q^{-4} S_{q,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0}) = \prod_{p} \left(1 + \sum_{n=1}^{\infty} p^{-4n} S_{p^n,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0})\right). \tag{6.6.1}$$

Moreover,

$$S_{p^n,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0}) = \sum_{\mathbf{b} \bmod p^n} \sum_{\substack{0 \leqslant k < p^n \\ \gcd(k,p)=1}} e_{p^n}\left(k \sum_{i=1}^{4} s_i^2 y_i^3 b_i^2\right). \tag{6.6.2}$$

Let $\alpha = \sum_{i=1}^{4} s_i^2 y_i^3 b_i^2$. The inner sum of (6.6.2) is a Ramanujan sum, which we recall is given by

$$\sum_{\substack{0 \leqslant k < p^n \\ \gcd(k,p)=1}} e_{p^n}(k\alpha) = \begin{cases} p^n - p^{n-1}, & \text{if } p^n \mid \alpha, \\ -p^{n-1}, & \text{if } p^{n-1} \mid \alpha \text{ but } p^n \nmid \alpha, \\ 0, & \text{otherwise.} \end{cases} \tag{6.6.3}$$

Let

$$N_{\mathbf{s},\mathbf{y}}(p^n) = \#\left\{\mathbf{b} \pmod{p^n} : \alpha \equiv 0 \pmod{p^n}\right\}.$$

When applying (6.6.3) to (6.6.2), $p^n$ occurs with multiplicity $N_{\boldsymbol{s},\mathbf{y}}(p^n)$ and $-p^{n-1}$ with multiplicity

$$\#\{\mathbf{b} \pmod{p^n} : \alpha \equiv 0 \pmod{p^{n-1}}\} = p^4 N_{\mathbf{s},\mathbf{y}}(p^{n-1}).$$

Therefore

$$S_{p^n,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0}) = p^n N_{\mathbf{s},\mathbf{y}}(p^n) - p^{n+3} N_{\mathbf{s},\mathbf{y}}(p^{n-1}), \tag{6.6.4}$$

and hence

$$\begin{aligned} \sum_{n=1}^{\infty} p^{-4n} S_{p^n,\mathbf{s}^2\mathbf{y}^3}(\mathbf{0}) &= \lim_{N\to\infty} \sum_{n=1}^{N} \left(p^{-3n} N_{\mathbf{s},\mathbf{y}}(p^n) - p^{-3(n-1)} N_{\mathbf{s},\mathbf{y}}(p^{n-1})\right) \\ &= \lim_{N\to\infty} \left(p^{-3N} N_{\mathbf{s},\mathbf{y}}(p^N)\right) - 1. \end{aligned}$$

Returning to (6.6.1), we conclude that

$$\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3} = \prod_{p} \left(\lim_{N\to\infty} \frac{N_{\mathbf{s},\mathbf{y}}(p^N)}{p^{3N}}\right). \tag{6.6.5}$$

For the remainder of the proof, we use a sum over $\mathbf{r}^{[p]}, \mathbf{s}^{[p]}, s_0^{[p]}$ to denote a sum over all $\mathbf{r}, \mathbf{s} \in \mathbb{N}^4, s_0 \in \mathbb{N}$, with $(\mathbf{r}, \mathbf{s}, s_0) = (\mathbf{r}^{[p]}, \mathbf{s}^{[p]}, s_0^{[p]})$ and $\mathbf{r}|\mathbf{y}$. Recalling that $\omega(\mathbf{r}, \mathbf{s}, s_0)$ is also multiplicative, we obtain

$$\sum_{\substack{\mathbf{r},\mathbf{s}\in\mathbb{N}^4 \\ s_0\in\mathbb{N} \\ \mathbf{r}|\mathbf{y}}} \frac{\omega(\mathbf{r}, \mathbf{s}, s_0)\mathfrak{G}_{\mathbf{s}^2\mathbf{y}^3}}{S s_0^2} = \prod_{p} \left(\sum_{\mathbf{r}^{[p]},\mathbf{s}^{[p]},s_0^{[p]}} \frac{\omega(\mathbf{r}^{[p]}, \mathbf{s}^{[p]}, s_0^{[p]})}{S^{[p]} {s_0^{2[p]}}} \lim_{N\to\infty} \left(\frac{N_{\mathbf{s},\mathbf{y}}(p^N)}{p^{3N}}\right)\right). \tag{6.6.6}$$

To complete the proof, it suffices to show that for a fixed prime $p$, the factor on the right hand side of (6.6.6) is equal to $\lim_{N\to\infty}(p^{-3N}M_N(\mathbf{y},p))$. We define

$$N_{\mathbf{s},s_0,\mathbf{y}}(n) = \#\left\{\mathbf{m} \pmod{p^n} : \sum_{i=1}^{4} y_i^3 m_i^2 \equiv 0 \pmod{p^n}, \mathbf{s}|\mathbf{m}, s_0|\mathbf{m}\right\}.$$

We claim that

$$M_n(\mathbf{y},p) = \sum_{\mathbf{r}^{[p]},\mathbf{s}^{[p]},s_0^{[p]}} \omega(\mathbf{r},\mathbf{s},s_0) N_{\mathbf{s},s_0,\mathbf{y}}(n). \tag{6.6.7}$$

To see this, we fix $\mathbf{m} \pmod{p^n}$ such that $\sum_{i=1}^4 y_i^3 m_i^2 \equiv 0 \pmod{p^n}$, and consider the quantity

$$\sum_{\substack{\mathbf{r}^{[p]},\mathbf{s}^{[p]},s_0^{[p]} \\ \mathbf{s}|\mathbf{m},s_0|\mathbf{m}}} \omega(\mathbf{r},\mathbf{s},s_0).$$

This expression has already been encountered in (6.5.4), and from the proof of Lemma 6.5.2, we see that it is equal to $1$ if $p \nmid y_i m_i$ for some $i$, and zero otherwise. This establishes (6.6.7).

Changing variables from $m_i$ to $s_0 s_i m_i$, we have

$$N_{\mathbf{s},s_0,\mathbf{y}}(n) = \frac{s_0^{4[p]} N_{\mathbf{s},\mathbf{y}}(p^{n-2\nu_p(s_0)})}{S^{[p]}}.$$

Therefore

$$\lim_{N\to\infty}\left(\frac{N_{\mathbf{s},s_0,\mathbf{y}}(N)}{p^{3N}}\right) = \lim_{N\to\infty}\left(\frac{N_{\mathbf{s},\mathbf{y}}(p^N)}{S^{[p]}s_0^{2[p]}}\right).$$

Combining this with (6.6.7), we deduce that $\lim_{N\to\infty}(p^{-3N}M_N(\mathbf{y},p))$ matches the Euler factor from the right hand side of (6.6.6). □

We do not expect the leading constant $c$ from (6.5.9) to agree with the constant $c_{\text{PSTV-A}}$ from Conjecture 3.0.8 without the removal of further thin sets. In Chapter 7, we study the counting problem $\#\mathscr{N}_3(B)$ from (1.2.2), which corresponds to Poonen's question [98] about the orbifold $(\mathbb{P}^1, D)$, where $D = \frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[\infty]$. The more detailed discussion around the case $k = 3$ in Chapter 7 is readily adapted to deal with the case $k = 4$ considered in this chapter. Therefore, we only give a brief summary here.

We recall that $N_{\mathbf{y}}(B)$ denotes the contribution to $N(B)$ from a fixed choice of $\mathbf{y} \in (\mathbb{Z}_{\neq 0})^4$ satisfying $Y \neq \square$ and $\mu^2(y_1) = \cdots = \mu^2(y_4) = 1$. We have shown that each $N_{\mathbf{y}}(B)$ contributes a positive proportion to $N(B)$, namely $N_{\mathbf{y}}(B) \sim c_{\mathbf{y}} B$, where

$$c_{\mathbf{y}} = \frac{\sigma_\infty(\boldsymbol{\epsilon})}{|Y|^{3/2}} \prod_p \left(\lim_{N\to\infty} \frac{M_N(\mathbf{y},p)}{p^{3N}}\right).$$

Moreover, Manin's conjecture can be applied to the quadric $Q_{\mathbf{y}}$ cut out by the equation $\sum_{i=1}^{4} y_i^3 x_i^2 = 0$, and the constant thus predicted is in agreement with $c_{\mathbf{y}}$ (as was expected due to Remark 4.5.3). Hence the expression in (6.5.9) is naturally interpreted as a sum over $\mathbf{y}$ of leading constants arising from Manin's conjecture applied to the quadrics $Q_{\mathbf{y}}$. This sum is not multiplicative in $\mathbf{y}$, and it does not appear to be possible to express (6.5.9) as an Euler product. In contrast, $c_{\text{PSTV-A}}$ is by definition an Euler product. In Chapter 7, we find that when $k = 3$, the analogous constant to (6.5.9) does not agree numerically with the leading constant $c_{\text{PSTV-A}}$ from Conjecture 3.0.8, and it seems very likely that the same will hold true for $k = 4$.

Since the PSTV-A conjecture allows for the removal of thin sets, a natural question that arises is whether thin sets could explain the discrepancy between $c$ and $c_{\text{PSTV-A}}$. We recall from Remark 3.0.9 that for our orbifold, the set of Campana points is not itself thin. However, in analogy to Theorem 7.1.3, it can be shown that any constant in $(0, c]$ could be obtained by the removal of an appropriate thin set. Most of these thin sets have no clear geometric interpretation in relation to the original orbifold. From this point of view, $c$ seems to be the most natural choice of leading constant for the orbifold considered in this chapter.

CHAPTER 7

# On the leading constant for the Manin-type conjecture for Campana points

## 7.1 Introduction

In this chapter, we investigate the leading constant $c_{\text{PSTV-A}}$ from the Manin-type conjecture for Campana points (Conjecture 3.0.8) in some concrete examples. The first example we study is the Campana orbifold $(\mathbb{P}^1, D)$ with the divisor $D = \frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[\infty]$, which corresponds to the counting problem $\#\mathscr{N}_3(B)$ from (1.2.2). This problem was posed by Poonen [98] following discussions in the Spring 2006 MSRI program on rational and integral points on higher-dimensional varieties, and was one of the motivating examples for the development of the quantitative theory of Campana points. We use the height $H$ on $\mathbb{P}^1(\mathbb{Q})$ given by

$$H(z) = \max(|z_1|, |z_2|, |z_1 + z_2|) \tag{7.1.1}$$

for $(z_1, z_2) \in \mathbb{Z}^2_{\text{prim}}$ representing $z$. Let $(\mathbb{P}^1, \mathscr{D})$ be the obvious integral model of $(\mathbb{P}^1, D)$ over $\mathbb{Z}$. Let

$$N_1(B) = \#\{P \in (\mathbb{P}^1, \mathscr{D})(\mathbb{Z}) : H(P) \leqslant B\}. \tag{7.1.2}$$

Recalling the discussion after (6.1.2), we have $N_1(B) = \frac{1}{2}\#\mathscr{N}_3(B)$. According to the PSTV-A conjecture, we should expect $\#\mathscr{N}_3(B) \sim cB^{1/2}$ for some constant $c > 0$. It is easy to show that $\#\mathscr{N}_3(B) \gg B^{1/2}$, for example by replacing the condition that $z_1, z_2$ and $z_1 + z_2$ are squareful by the stronger condition that they are squares, and counting the resulting Pythagorean triples. However, finding upper bounds is much more challenging, and the best result to

date is $\#\mathscr{N}_3(B) = O(B^{3/5+\epsilon})$, obtained by Browning and Van Valckenorgh in [22, Theorem 1.2] by applying the determinant method and the results of [62].

We recall the approach outlined in Section 4.5 to count $\mathscr{N}_k(B)$, based on a fibration into quadrics. This approach has proven successful in treating the case $k \geqslant 4$, by a result of Van Valckenborgh [117, Theorem 1.1] for $k \geqslant 5$ and by Chapter 6 of this work for $k = 4$. Following this approach for $k = 3$ yields the decomposition

$$N_1(B) = \frac{1}{2^3} \sum_{\substack{\mathbf{y} \in (\mathbb{Z}_{\neq 0})^3 \\ y_1, y_2, y_3 \text{ squarefree}}} N_{\mathbf{y}}^+(B), \tag{7.1.3}$$

where

$$N_{\mathbf{y}}^+(B) = \frac{1}{2} \# \left\{ \mathbf{x} \in (\mathbb{Z}_{\neq 0})^3 : \sum_{i=1}^{3} x_i^2 y_i^3 = 0, \begin{array}{l} \gcd(x_1 y_1, x_2 y_2, x_3 y_3) = 1 \\ \max_{1 \leqslant i \leqslant 3} |y_i^3 x_i^2| \leqslant B \end{array} \right\}.$$

With this decomposition, the leading constant for $N_1(B)$ is naturally expressed as an infinite sum of constants $c_{\mathbf{y}}$ arising from Manin's conjecture applied to $N_{\mathbf{y}}^+(B)$. This leads to the following prediction of Browning and Van Valckenborgh.

**Conjecture 7.1.1** ([22, Conjecture 1.1])**.** *We have*

$$N_1(B) \sim 3 c_{BV} B^{1/2},$$

*where the constant $c_{BV}$ is given explicitly in [22, Equation (2–12)] (and also in (7.3.11)), and is expressed as a sum over $(y_0, y_1, y_2)$ of constants arising from Manin's conjecture applied to the conics $x_0^2 y_0^3 + x_1^2 y_1^3 = x_2^2 y_2^3$.*

The reason for the factor $3$ in Conjecture 7.1.1 is explained in Lemma 7.3.1, and is due to the counting problem considered in [22] being over $\mathbb{N}^3_{\text{prim}}$ rather than $(\mathbb{Z}_{\neq 0})^3_{\text{prim}}$.

By focusing on the contribution to $N_{\mathbf{y}}^+(B)$ from the range $|\mathbf{y}| \leqslant B^\theta$, for a small absolute constant $\theta > 0$, it is possible to prove the lower bound

$$N_1(B) \geqslant 3 c_{\text{BV}} B^{1/2} (1 + o(1)), \tag{7.1.4}$$

where $c_{\text{BV}}$ is as defined in Conjecture 7.1.1. This is achieved in [22, Theorem 1.2], where it is also established that $c_{\text{BV}}$ takes the numerical value $2.68...$ correct to two decimal digits.

For the orbifold $(\mathbb{P}^1, \frac{1}{2}[0] + \frac{1}{2}[1] + \frac{1}{2}[\infty])$ corresponding to the counting problem $N_1(B)$, there does not appear to be any obvious thin set to remove. Therefore, we might naturally expect that $c_{\text{PSTV-A}}$ is the leading constant for $N_1(B)$ itself, and consequently, in view of the lower bound in (7.1.4), that $c_{\text{PSTV-A}} \geqslant 3 c_{\text{BV}}$. In Section 7.2, we shall prove the following result, which shows that in fact, $c_{\text{PSTV-A}} < 3 c_{\text{BV}}$.

**Theorem 7.1.2.** *For the orbifold corresponding to the counting problem $N_1(B)$, the leading constant predicted by the PSTV-A conjecture is*

$$c_{PSTV\text{-}A} = \frac{9}{2\pi} \prod_p \left(1 + \frac{3p^{-3/2}}{1+p^{-1}}\right). \tag{7.1.5}$$

*Moreover, $c_{PSTV\text{-}A}/3 = 2.56785632...$, accurate up to eight digits.*

We define

$$\mathscr{C} = \left\{ [z_0 : z_1] \in \mathbb{P}^1(\mathbb{Q}) : \begin{array}{l} (z_0, z_1) \in \mathbb{Z}^2_{\text{prim}}, \\ z_0, z_1, z_0 + z_1 \text{ squareful and nonzero} \end{array} \right\} \tag{7.1.6}$$

to be the set of Campana points under consideration. We recall from Remark 3.0.9 that the set of Campana points $\mathscr{C}$ is not itself thin. Hence the PSTV-A conjecture predicts that there is some thin set $\mathscr{T} \subset \mathscr{C}$ of Campana points such that the removal of $\mathscr{T}$ from the count $N_1(B)$ reduces the leading constant from $c$ to $c_{\text{PSTV-A}}$. In Section 7.4, we prove the following result.

**Theorem 7.1.3.** *Suppose that Conjecture 7.1.1 holds. Let the height function $H$ be as defined in (7.1.1). Then for any real number $\lambda \in (0, 3c_{BV}]$, there is a Campana thin subset $\mathscr{T} \subseteq \mathscr{C}$, as introduced in Definition 3.0.6, such that*

$$\#\{z \in \mathscr{C} \backslash \mathscr{T} : H(z) \leqslant B\} \sim \lambda B^{1/2}.$$

Theorem 7.1.3 demonstrates that if Conjecture 7.1.1 holds, we can obtain any leading constant in $(0, 3c_{\text{BV}}]$, including the constant $c_{\text{PSTV-A}}$, by the removal of an appropriate thin set. From this point of view, the PSTV-A conjecture as stated in [96] seems somewhat unsatisfactory, in that all points can lie on accumulating thin subsets. However, there does not appear to be any thin set with a clear geometric meaning which we can remove in order to obtain the constant $c_{\text{PSTV-A}}$, and so currently $3c_{\text{BV}}$ seems the most natural prediction for the leading constant in this example.

**Remark 7.1.4.** We have considered $N_1(B)$ for simplicity, but it seems likely that similar statements hold for the orbifold considered in Chapter 6. In this case, we know the analogue of Conjecture 7.1.1 holds, and so we could obtain unconditional analogues of Theorem 7.1.3. Similarly, this approach could be extended to the setting considered by Van Valckenborgh [117], or by Browning and Yamagishi [23].

Motivated by the above discussion, in Section 7.5 we study $c_{\text{PSTV-A}}$ in a second example, involving squareful values of a binary quadratic form. For fixed positive,

squarefree and coprime integers $a, b$ satisfying $a, b \equiv 1 \pmod 4$, we consider the counting problem

$$N(B) = \frac{1}{2}\#\left\{(x,y) \in \mathbb{Z}^2_{\text{prim}} : |x|, |y| \leqslant B, ax^2 + by^2 \text{ squareful}\right\}. \quad (7.1.7)$$

This corresponds to the Campana orbifold $(X, D) = (\mathbb{P}^1, \frac{1}{2}V(ax^2 + by^2))$ over $\mathbb{Q}$, together with the obvious $\mathbb{Z}$-model $(\mathscr{X}, \mathscr{D})$, and the height $H$ on $\mathbb{P}^1(\mathbb{Q})$ given by $H([x : y]) = \max(|x|, |y|)$ for $(x, y) \in \mathbb{Z}^2_{\text{prim}}$. By Remark 3.0.9, the set of Campana points in this example is not itself thin. In Theorem 7.5.1, we compute the constant $c_{\text{PSTV-A}}$ for this example. In Section 7.5, we also prove the following theorem, which can be thought of as an unconditional analogue of Conjecture 7.1.1 for the counting problem $N(B)$.

**Theorem 7.1.5.** *For any $\epsilon > 0$, we have $N(B) = cB + O(B^{89/90+\epsilon})$, where the implied constant depends only on $a, b$ and $\epsilon$. The leading constant $c$ is given explicitly in (7.5.19) as a sum over $v$ of constants arising from Manin's conjecture applied to the conics $ax^2 + by^2 = u^2v^3$.*

**Remark 7.1.6.** When $a = 1$, $N(B)$ counts squareful values of the norm form $x^2 + by^2$, and we have an asymptotic formula for $N(B)$ as a special case of a result by Streeter [115, Theorem 1.4]. The constant from [115, Theorem 1.4] and the constant $c$ from Theorem 7.1.5 must therefore agree. However, the constants are not immediately comparable, since the proof of [115, Theorem 1.4] proceeds via very different methods, using height zeta functions and Fourier analysis. This yields a leading constant that involves a sum of limits of global Fourier transforms of 2-torsion toric characters.

For the orbifolds considered in Theorem 7.1.5, the constants $c$ and $c_{\text{PSTV-A}}$ are often not equal. In the norm form case $a = 1$, we show that $c_{\text{PSTV-A}} < c$ whenever $b > 1$. Analogously to Theorem 7.1.3, any constant in $(0, c]$ could be obtained by the removal of an appropriate thin set. When $a, b > 1$, however, we shall show that sometimes $c < c_{\text{PSTV-A}}$. The significance of this is that thin sets cannot explain the discrepancy between the constants. Thus Theorem 7.1.5 provides the basis for the following counterexample to the leading constant predicted by the PSTV-A conjecture.

**Corollary 7.1.7.** *Let $a = 37$ and $b = 109$. Then the PSTV-A conjecture does not hold for the orbifold $(\mathscr{X}, \mathscr{D})$ and the height $H$ defined above.*

**Acknowledgements.** I would like to thank Damaris Schindler and Florian Wilsch for their helpful comments on the heights and Tamagawa measures used in Section 7.2, together with Marta Pieropan, Sho Tanimoto and Sam Streeter for providing valuable feedback on an earlier version of this work, and Tim

Browning for many useful comments and discussions during the development of this work. I am also grateful to the anonymous referees for providing many helpful comments and suggestions that improved the quality of the paper on which this chapter is based.

## 7.2 Proof of Theorem 7.1.2

In this section, we prove Theorem 7.1.2. We adopt the notation and definitions from Chapter 3. The choice of height from (7.1.1) corresponds to the ample line bundle $\mathscr{L} = \mathscr{O}_{\mathbb{P}^1}(1)$, metrized by the generating set $\{z_0, z_1, z_0 + z_1\}$ for the global sections of $\mathscr{L}$.

The computation of the exponents $a$ and $b$ from the PSTV-A conjecture is similar to Section 3.3.2. Under the isomorphism $\mathrm{Pic}(\mathbb{P}^1) \cong \mathbb{Z}$ given by the degree function, the line bundle $\mathscr{L}$ maps to $1$ and $\Lambda_{\mathrm{eff}}$ is identified with $\mathbb{R}_{\geqslant 0}$. Since $\deg D = 3/2$ and $\deg[K_{\mathbb{P}^1}] = -2$, we have

$$a = \inf\left\{t \in \mathbb{R} : t - 2 + \frac{3}{2} \geqslant 0\right\} = \frac{1}{2}.$$

The minimal supported face of $\Lambda_{\mathrm{eff}}$ which contains $a[L] + [K_{\mathbb{P}^1}] + [D] = 0$ is $\{0\}$, which has codimension $1$ in $\Lambda_{\mathrm{eff}}$, and so $b = 1$. These values of $a$ and $b$ are compatible with Conjecture 7.1.1.

It remains to compute the leading constant $c_{\text{PSTV-A}}$, as defined in Section 3.2. We recall that

$$c_{\text{PSTV-A}} = \frac{\alpha\beta\tau}{a(b-1)!}, \tag{7.2.1}$$

and we proceed to discuss each of the factors $\alpha, \beta, \tau$ in turn.

Similarly to the computation in Section 3.3.2, we have

$$\alpha = \left(\frac{1}{2}\right)^3 \int_0^\infty e^{-x}\mathrm{d}x = \frac{1}{8}$$

and $\beta = 1$. Substituting $a = \frac{1}{2}, b = 1, \alpha = \frac{1}{8}$ and $\beta = 1$ into (7.2.1), we deduce that

$$c_{\text{PSTV-A}} = \frac{\tau}{4}. \tag{7.2.2}$$

In the notation of [91, Section 2], we have $\det(1 - p^{-1}\,\mathrm{Frob}_p \,|\, \mathrm{Pic}(\overline{\mathbb{P}^1}^{I_p})) = 1 - p^{-1}$ for all primes $p$. (In fact, this is true whenever $\mathrm{Pic}(X_{\overline{\mathbb{Q}}}) = \mathbb{Z}$ [72, Chapter II, Remark 6.10].) Fixing $i \in \{0, 1, 2\}$ and writing $z_2 = z_0 + z_1$, we define sections $s_{D_i} = z_i$. We take the metrization on $\mathscr{O}_{\mathbb{P}^1}(D_i)$ obtained from pulling back the metrization on $\mathscr{O}_{\mathbb{P}^1}(1)$ via the obvious isomorphism $\mathscr{O}_{\mathbb{P}^1}(D_i) \cong \mathscr{O}_{\mathbb{P}^1}(1)$. We recall that we are using the metrization on $\mathscr{O}_{\mathbb{P}^1}(1)$

arising from the generating set $\{z_0, z_1, z_2\}$. Let $|\cdot|_v$ denote the $p$-adic metric if $v = p$ and the Euclidean metric if $v = \infty$, and let $\mathrm{Val}(\mathbb{Q})$ denote the set of places of $\mathbb{Q}$. Recalling (2.2.5), on the set $(\mathbb{P}^1\backslash D_i)(\mathbb{Q})$, may express $H_{D_i}$ as a product of local heights

$$H_{D_i}(z) = \prod_{v\in\mathrm{Val}(\mathbb{Q})} H_{D_i,v}(z) = \prod_{v\in\mathrm{Val}(\mathbb{Q})} \frac{\max(|z_0|_v, |z_1|_v, |z_2|_v)}{|z_i|_v},$$

where $[z_0 : z_1]$ represents $z$. Therefore,

$$H_D(z) = \prod_{v\in\mathrm{Val}(\mathbb{Q})} H_{D,v}(z) = \prod_{v\in\mathrm{Val}(\mathbb{Q})} \frac{\max(|z_0|_v, |z_1|_v, |z_2|_v)^{3/2}}{|z_0z_1z_2|_v^{1/2}} \tag{7.2.3}$$

on the open set $(\mathbb{P}^1\backslash \mathrm{supp}(D))(\mathbb{Q})$, where $\mathrm{supp}(D) = D_0 \cup D_1 \cup D_2$.

The property that $z \in (\mathbb{P}^1\backslash \mathrm{supp}(D))(\mathbb{Q})$ is a Campana point is a local condition. More precisely, it is the condition that for all primes $p$, we have

$$\nu_p(z_0), \nu_p(z_1), \nu_p(z_0 + z_1) \neq 1$$

for $(z_0, z_1) \in \mathbb{Z}^2_{\mathrm{prim}}$ representing $z$. Let $\Omega_p$ denote the subset of $\mathbb{P}^1(\mathbb{Q}_p)$ cut out by this local condition, and define $\Omega_\infty = \mathbb{P}^1(\mathbb{R})$. The expression (3.2.3) becomes

$$\tau = \sigma_\infty \prod_p (1 - p^{-1})\sigma_p, \tag{7.2.4}$$

where

$$\sigma_v = \int_{\Omega_v} \frac{\max(|z_0|_v, |z_1|_v, |z_0 + z_1|_v)^{3/2}}{|z_0z_1(z_0 + z_1)|_v^{1/2}} \mathrm{d}\omega_v.$$

To compute $\sigma_v$, we use the chart $U_v = \{[t : 1] : t \in \mathbb{Q}_v\}$, equipped with the natural maps $f_v \colon U_v \to \mathbb{Q}_v$ given by $[t : 1] \mapsto t$. The only point on $\Omega_v$ not in $U_v$ is $[1 : 0]$, which has measure zero, and so we may replace the range of integration with $\Omega_v \cap U_v$. A point $[z_0 : z_1]$ on $U_v$ satisfies $t = z_0/z_1$. Let $\mathrm{d}t$ denote the usual $p$-adic measure or the Lebesgue measure as appropriate. We recall that there is an isomorphism $\mathscr{K}_{\mathbb{P}^1} \cong \mathscr{O}_{\mathbb{P}^1}(-2)$, which on the chart $U_v$ is given by mapping $\mathrm{d}t$ to $z_1^{-2}$. Therefore, in the notation of [91, Section 2], we have

$$\|\mathrm{d}t\|_{\mathscr{K}_{\mathbb{P}^1},v} = \|z_1^{-2}\|_{\mathscr{O}_{\mathbb{P}^1}(-2),v} = \frac{|z_1|_v^{-2}}{\max(|z_0|_v, |z_1|_v, |z_0 + z_1|_v)^{-2}}.$$

We obtain

$$\begin{aligned} H_{D,v}\omega_v &= \frac{\max(|z_0|_v, |z_1|_v, |z_0 + z_1|_v)^{3/2}|z_1|_v^2}{|z_0z_1(z_0 + z_1)|_v^{1/2}\max(|z_0|_v, |z_1|_v, |z_0 + z_1|_v)^2}\mathrm{d}t \\ &= \frac{\mathrm{d}t}{|t(1 + t)|_v^{1/2}\max(|t|_v, 1, |1 + t|_v)^{1/2}}. \end{aligned} \tag{7.2.5}$$

When $v = \infty$, we have $f_v(\Omega_v \cap U_v) = \mathbb{R}$. Therefore

$$\begin{aligned}\sigma_\infty &= \int_{\mathbb{R}} \frac{\mathrm{d}t}{|t(1+t)|^{1/2}\max(|t|,1,|1+t|)^{1/2}} \\ &= \int_{-\infty}^{-1} \frac{\mathrm{d}t}{|1+t|^{1/2}|t|} + \int_{-1}^{0} \frac{\mathrm{d}t}{|t(1+t)|^{1/2}} + \int_{0}^{\infty} \frac{\mathrm{d}t}{t^{1/2}(1+t)}.\end{aligned}$$

Each of these integrals is equal to $\pi$, and so we conclude that $\sigma_\infty = 3\pi$. In the following lemma, we compute $\sigma_v$ when $v < \infty$.

**Lemma 7.2.1.** *We have* $\sigma_p = 1 + p^{-1} + 3p^{-3/2}$.

*Proof.* We recall that $\Omega_p$ consists of the points $[z_0 : z_1] \in \mathbb{P}^1(\mathbb{Q}_p)$ such that $\min(\nu_p(z_0), \nu_p(z_1)) = 0$ and $\nu_p(z_0), \nu_p(z_1), \nu_p(z_0 + z_1) \neq 1$. From this, we see that $f_p(\Omega_p \cap U_p)$ is the set of all $t \in \mathbb{Q}_p$ which satisfy the conditions $t, t+1 \neq 0$ and $\nu_p(t), \nu_p(1+t) \neq \pm 1$. Therefore

$$\sigma_p = \int_{\substack{t\in\mathbb{Q}_p \\ \nu_p(t),\nu_p(1+t)\neq\pm1}} \frac{\mathrm{d}t}{|t(1+t)|_p^{1/2}\max(|t|_p,1,|1+t|_p)^{1/2}}. \tag{7.2.6}$$

By the ultrametric triangle inequality, $\max(1, |t|_p, |1+t|_p) = \max(1, |t|_p)$. We now consider separately the contribution to the integral from the regions $R_1, R_2, R_3$ defined respectively by the conditions

1. $\nu_p(t) \geqslant 2$,
2. $\nu_p(t) = 0$,
3. $\nu_p(t) \leqslant -2$.

In the region $R_1$, we have $|1+t|_p = 1$ and $\max(|t|_p, 1) = 1$. We recall also that for any $j \in \mathbb{Z}$, the $p$-adic measure of the set of $t \in \mathbb{Q}_p$ with $\nu_p(t) = j$ is $(1-p^{-1})p^{-j}$. Hence the contribution to (7.2.6) from $R_1$ is

$$\int_{\substack{t\in\mathbb{Q}_p \\ \nu_p(t)\geqslant 2}} \frac{\mathrm{d}t}{|t|_p^{1/2}} = \sum_{j=2}^{\infty}(1-p^{-1})p^{-j/2} = p^{-1} + p^{-3/2}.$$

In the region $R_2$, we have $\max(1, |t|_p) = 1$. We further subdivide this region according to the value of $\nu_p(1+t)$, remembering that the case $\nu_p(1+t) = 1$ must be excluded. We define

$$S_j = \{t \in \mathbb{Z}_p^\times : \nu_p(1+t) = j\}.$$

When $j < 0$, we have $S_j = \emptyset$. When $j = 0$, the measure of $S_j$ is $1 - 2p^{-1}$, because $t \in S_0$ if and only if the reduction of $t$ modulo $p$ is not $0$ or $-1$. (In

the case $p = 2$, we have $1 - 2p^{-1} = 0$, which is consistent with the fact that it is not possible for $t$ and $1 + t$ to both be in $\mathbb{Z}_2^\times$). When $j \geqslant 2$, elements $t \in S_j$ are precisely elements of the form $t = -1 + s$ for some $s \in \mathbb{Q}_p$ with $\nu_p(s) = j$, and so $S_j$ has measure $p^{-j}(1 - p^{-1})$. We conclude that the contribution to (7.2.6) from the region $R_2$ is

$$\int_{\substack{t \in \mathbb{Z}_p^\times \\ \nu_p(1+t) \neq \pm 1}} \frac{\mathrm{d}t}{|1+t|_p^{1/2}} = 1 - 2p^{-1} + \sum_{j=2}^{\infty} (1 - p^{-1}) p^{-j/2} = 1 - p^{-1} + p^{-3/2}.$$

Finally, in the region $R_3$, we have $|1 + t|_p = 1$ and $\max(1, |t|_p) = |t|_p$, and so we obtain a contribution from $R_3$ of

$$\int_{\substack{t \in \mathbb{Q}_p \\ \nu_p(t) \leqslant -2}} \frac{\mathrm{d}t}{|t|_p^{3/2}} = \sum_{j=2}^{\infty} (1 - p^{-1}) p^{-j/2} = p^{-1} + p^{-3/2}.$$

Combining the three regions, we conclude that

$$\sigma_p = (p^{-1} + p^{-3/2}) + (1 - p^{-1} + p^{-3/2}) + (p^{-1} + p^{-3/2}) = 1 + p^{-1} + 3p^{-3/2},$$

as required. □

We now complete the proof of Theorem 7.1.2. We recall that $c_{\text{PSTV-A}} = \tau/4$, and $\sigma_\infty = 3\pi$. Together with Lemma 7.2.1 and (7.2.4), this implies that

$$\begin{aligned} c_{\text{PSTV-A}} &= \frac{1}{4} \sigma_\infty \prod_p (1 - p^{-1}) \sigma_p \\ &= \frac{1}{4} \cdot 3\pi \prod_p (1 + 3p^{-3/2} - p^{-2} - 3p^{-5/2}) \qquad (7.2.7) \\ &= \frac{1}{4} \cdot 3\pi \prod_p \left(1 + \frac{3p^{-3/2}}{1 + p^{-1}}\right) (1 - p^{-2}). \end{aligned}$$

Since $\prod_p (1 - p^{-2}) = 1/\zeta(2) = 6/\pi^2$, we obtain the expression for $c_{\text{PSTV-A}}$ claimed in (7.1.5).

In order to estimate the numerical value of $c_{\text{PSTV-A}}$, we evaluate the Euler product $\prod_p (1 - p^{-1}) \sigma_p$ by removing convergence factors. Using (7.2.7) we have

$$\begin{aligned} \prod_p (1 - p^{-1}) \sigma_p &= \prod_p (1 + 3p^{-3/2} - p^{-2} - 3p^{-5/2}) \\ &= \zeta(3/2)^3 \cdot \frac{\zeta(4)}{\zeta(2)} \cdot \left(\frac{\zeta(5)}{\zeta(5/2)}\right)^3 \prod_p f(p), \end{aligned}$$

where $f(p) = 1 + O(p^{-3})$ is an explicit polynomial in $p^{-1}$. The resulting Euler product now converges quickly enough to obtain an approximation for $c_{\text{PSTV-A}}$ accurate to eight decimal digits by taking the product over the first $1000$ primes.

## 7.3 Manin's conjecture for the family of conics

In this section, we describe the alternative approach of Browning and Van Valckenborgh [22, Section 2] for predicting the leading constant for the counting problem $N_1(B)$ from (7.1.2). The counting function considered in [22] is given by

$$\widetilde{N}_1(B) = \#\left\{(z_0,z_1,z_2)\in \mathbb{N}^3_{\mathrm{prim}}: \begin{array}{l} z_0+z_1=z_2,\ z_0,z_1,z_2\leqslant B,\\ z_0,z_1,z_2 \text{ squareful}\end{array}\right\}.$$

This is very similar to $N_1(B)$, the only differences being the presence of the factor $1/2$ in (7.1.2), and that in $\widetilde{N}_1(B)$ we require $(z_0,z_1,z_2)\in\mathbb{N}^3_{\mathrm{prim}}$, whilst in $N_1(B)$ we only require $(z_0,z_1,z_2)\in(\mathbb{Z}_{\neq 0})^3_{\mathrm{prim}}$. The following lemma compares $N_1(B)$ with $\widetilde{N}_1(B)$.

**Lemma 7.3.1.** *We have* $N_1(B)=3\widetilde{N}_1(B)$.

*Proof.* For convenience we use the notation $\widetilde{S}_1(B)$ to mean the set which $\widetilde{N}_1(B)$ enumerates. For $\boldsymbol{\epsilon}\in\{\pm 1\}^3$, we define

$$S_{\boldsymbol{\epsilon}}(B)=\left\{(z_0,z_1,z_2)\in(\mathbb{Z}_{\neq 0})^3_{\mathrm{prim}}: \begin{array}{l} z_0+z_1=z_2, |z_i|\leqslant B \text{ for all } i\\ z_i \text{ squareful},\ \mathrm{sgn}(z_i)=\epsilon_i \text{ for all } i\end{array}\right\},$$

and $N_{\boldsymbol{\epsilon}}(B)=\#S_{\boldsymbol{\epsilon}}(B)$. Then

$$2N_1(B)=\sum_{\boldsymbol{\epsilon}\in\{\pm1\}^3} N_{\boldsymbol{\epsilon}}(B). \tag{7.3.1}$$

For $\boldsymbol{\epsilon}=(1,1,-1)$ or $\boldsymbol{\epsilon}=(-1,-1,1)$, we have $N_{\boldsymbol{\epsilon}}(B)=0$. For $\boldsymbol{\epsilon}=(1,1,1)$ or $\boldsymbol{\epsilon}=(-1,-1,-1)$, we have $N_{\boldsymbol{\epsilon}}(B)=\widetilde{N}_1(B)$, and so these choices of $\boldsymbol{\epsilon}$ contribute $2\widetilde{N}_1(B)$ to the sum in (7.3.1).

For the remaining four choices of $\boldsymbol{\epsilon}$, it can be checked that there is a permutation $\sigma\in S_3$ such that the map

$$\begin{aligned} S_{\boldsymbol{\epsilon}}(B)&\to\widetilde{S}_1(B)\\ (z_0,z_1,z_2)&\mapsto\sigma(|z_0|,|z_1|,|z_2|)\end{aligned}$$

is a bijection. Therefore $N_{\boldsymbol{\epsilon}}(B)=\widetilde{N}_1(B)$, and these choices of $\boldsymbol{\epsilon}$ contribute $4\widetilde{N}_1(B)$ to the sum in (7.3.1). □

In the remainder of this section we record the explicit description of $c_{\mathrm{BV}}$ from [22], and define some notation which will be useful later.

Recalling the discussion in the introduction, for a fixed $\mathbf{y} = (y_0, y_1, y_2)$ in $(\mathbb{Z}_{\neq 0})^3$, we consider the conic $C_{\mathbf{y}}$ defined by the polynomial

$$F_{\mathbf{y}}(x_0, x_1, x_2) = y_0^3 x_0^2 + y_1^3 x_1^2 - y_2^3 x_2^2.$$

We define an anticanonical height $H_{\mathbf{y}}$ on $C_{\mathbf{y}}$ given by

$$H_{\mathbf{y}}(x) = \max\left(|y_0^3 x_0^2|, |y_1^3 x_1^2|, |y_2^3 x_2^2|\right)^{1/2}, \tag{7.3.2}$$

where $(x_0, x_1, x_2) \in (\mathbb{Z}_{\neq 0})^3_{\mathrm{prim}}$ represents the point $x \in C_{\mathbf{y}}(\mathbb{Q})$. We define

$$N_{C_{\mathbf{y}}, H_{\mathbf{y}}}(B^{1/2}) = \#\{x \in C_{\mathbf{y}}(\mathbb{Q}) : H_{\mathbf{y}}(x) \leqslant B^{1/2}\},$$

and $N^+_{C_{\mathbf{y}}, H_{\mathbf{y}}}(B^{1/2})$ in the same way, but with the additional coprimality condition $\gcd(x_0 y_0, x_1 y_1, x_2 y_2) = 1$. Then

$$\widetilde{N}_1(B) = \frac{1}{4} \sum_{\mathbf{y} \in \mathbb{N}^3} \mu^2(y_0 y_1 y_2) N^+_{C_{\mathbf{y}}, H_{\mathbf{y}}}(B). \tag{7.3.3}$$

The presence of the factor $1/4$ in (7.3.3) is due to the fact that in $N^+_{C_{\mathbf{y}}, H_{\mathbf{y}}}(B^{1/2})$ the points $x$ we count lie in $\mathbb{P}^2(\mathbb{Q})$, which allows for four choices of sign for the coordinates of $x$ corresponding to each point $(z_0, z_1, z_2)$ enumerated by $\widetilde{N}_1(B)$.

As mentioned in [22, Section 3], it is easy to show that there is an absolute constant $\delta > 0$ and an explicit constant $c_{H_{\mathbf{y}}}(C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+)$ depending on $\mathbf{y}$ such that

$$N^+_{C_{\mathbf{y}}, H_{\mathbf{y}}}(B^{1/2}) = c_{H_{\mathbf{y}}}(C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+) B^{1/2}(1 + O_{\mathbf{y}}(B^{-\delta})), \tag{7.3.4}$$

where the error term has at worst polynomial dependence on $\mathbf{y}$. The constant $c_{H_{\mathbf{y}}}(C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+)$ is a special case of the constant conjecturally formulated by Peyre [91, Définition 2.5]. Here, $C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+$ denotes the open subset of $C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})$ given by the conditions $\min_{0 \leqslant i \leqslant 2}(\nu_p(x_i y_i)) = 0$ for all primes $p$, and is intended to reflect the coprimality condition $\gcd(x_0 y_0, x_1 y_1, x_2 y_2) = 1$ imposed on $N^+_{C_{\mathbf{y}}, H_{\mathbf{y}}}(B^{1/2})$ in (7.3.3). The computation of $c_{H_{\mathbf{y}}}(C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+)$ then involves the Tamagawa measure of $C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+$ in place of the full adelic space $C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})$. In the light of (7.3.3), it is natural to predict that

$$\widetilde{N}_1(B) \sim c_{\mathrm{BV}} B^{1/2}, \tag{7.3.5}$$

with

$$c_{\mathrm{BV}} = \frac{1}{4} \sum_{\mathbf{y} \in \mathbb{N}^3} \mu^2(y_0 y_1 y_2) c_{H_{\mathbf{y}}}(C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^+). \tag{7.3.6}$$

In what follows, we shall use for brevity the notation

$$\gamma(d) := \prod_{\substack{p \mid d \\ p > 2}} \left(1 + \frac{1}{p}\right)^{-1}. \tag{7.3.7}$$

In [22, Section 2], it is established that

$$c_{H_{\mathbf{y}}}(C_{\mathbf{y}}(\mathbb{A}_{\mathbb{Q}})^{+}) = \frac{4}{\pi} \cdot \frac{\mu^2(y_0y_1y_2)\gamma(y_0y_1y_2)}{(y_0y_1y_2)^{3/2}}\sigma_{2,\mathbf{y}}\varrho(\mathbf{y}), \tag{7.3.8}$$

where

$$\varrho(\mathbf{y}) = \prod_{\substack{p\mid y_0\\ p>2}}\left(1+\left(\frac{y_1y_2}{p}\right)\right)\prod_{\substack{p\mid y_1\\ p>2}}\left(1+\left(\frac{y_0y_2}{p}\right)\right)\prod_{\substack{p\mid y_2\\ p>2}}\left(1+\left(\frac{-y_0y_1}{p}\right)\right), \tag{7.3.9}$$

$$\sigma_{2,\mathbf{y}} = \lim_{r\to\infty} 2^{-2r}\#\left\{\mathbf{x}\in(\mathbb{Z}/2^r\mathbb{Z})^3 : \begin{array}{l} y_0^3x_0^2+y_1^3x_1^2 \equiv y_2^3x_2^2 \pmod{2^r},\\ \min_{0\leqslant i\leqslant 2}(\nu_2(x_iy_i)) = 0 \end{array}\right\}. \tag{7.3.10}$$

Combining with (7.3.6), we conclude that

$$c_{\mathrm{BV}} = \frac{1}{\pi}\sum_{\mathbf{y}\in\mathbb{N}^3}\frac{\mu^2(y_0y_1y_2)\gamma(y_0y_1y_2)}{(y_0y_1y_2)^{3/2}}\sigma_{2,\mathbf{y}}\varrho(\mathbf{y}). \tag{7.3.11}$$

From [22, Lemma 2.2], we have the calculation

$$\sigma_{2,\mathbf{y}} = \begin{cases} 1, & \text{if } 2\nmid y_0y_1y_2 \text{ and } \neg\{y_0\equiv y_1\equiv -y_2 \pmod 4\},\\ 2, & \text{if } 2\mid y_0 \text{ and } y_1\equiv y_2 \pmod 8,\\ 2, & \text{if } 2\mid y_1 \text{ and } y_0\equiv y_2 \pmod 8,\\ 2, & \text{if } 2\mid y_2 \text{ and } y_0\equiv -y_1 \pmod 8,\\ 0, & \text{otherwise.}\end{cases} \tag{7.3.12}$$

As a consequence of quadratic reciprocity, it can be shown that the condition $\neg\{y_0\equiv y_1\equiv -y_2 \pmod 4\}$ is automatically satisfied whenever $\varrho(\mathbf{y})\neq 0$.

**Remark 7.3.2.** The expression for $c_{\mathrm{BV}}$ given in (7.3.11) is a sum of products of local densities arising from Manin's conjecture, but it is not multiplicative in $\mathbf{y}$, and it does not appear possible to express $c_{\mathrm{BV}}$ as a single Euler product. This is in contrast to the constant $c_{\text{PSTV-A}}$, which is defined as a product of local densities.

## 7.4 Thin sets

In this section, we prove Theorem 7.1.3. We recall the definition of the set of Campana points $\mathscr{C}$ from (7.1.6) and the corresponding counting problem $N_1(B)$ from (7.1.2), with the height $H$ as defined in (7.1.1). From Definition 3.0.6, the Campana thin subsets of $\mathscr{C}$ take the form $\mathscr{T} = T\cap\mathscr{C}$, where $T$ is a thin subset

of $\mathbb{P}^1(\mathbb{Q})$. For a set $S \subseteq \mathbb{P}^1(\mathbb{Q})$, we define $N_1(S,B) = \#\{z \in S : H(z) \leqslant B\}$. In particular, we have $N_1(\mathscr{C},B) = N_1(B)$.

For fixed integers $y_0, y_1, y_2$ satisfying $\mu^2(y_0y_1y_2) = 1$, we recall that $C_{\mathbf{y}}$ denotes the conic $y_0^3x_0^2 + y_1^3x_1^2 = y_2^3x_2^2$. Consider the morphism

$$\begin{aligned} \varphi_{\mathbf{y}} \colon C_{\mathbf{y}} &\to \mathbb{P}^1, \\ [x_0 : x_1 : x_2] &\mapsto [y_0^3x_0^2 : y_1^3x_1^2]. \end{aligned}$$

The image $T_{\mathbf{y}} := \varphi_{\mathbf{y}}(C_{\mathbf{y}})$ is a thin subset of $\mathbb{P}^1(\mathbb{Q})$. Therefore $T_{\mathbf{y}} \cap \mathscr{C}$ is a thin set of Campana points. Explicitly, $T_{\mathbf{y}} \cap \mathscr{C}$ is described by the set

$$\left\{ [z_0 : z_1] \in \mathbb{P}^1(\mathbb{Q}) : \begin{array}{l} (z_0,z_1) \in \mathbb{Z}^2_{\mathrm{prim}}, z_0, z_1, z_0+z_1 \neq 0, \\ (z_0, z_1, z_0+z_1) = (y_0^3x_0^2, y_1^3x_1^2, y_2^3x_2^2) \end{array} \right\}, \tag{7.4.1}$$

where $x_0, x_1, x_2$ are assumed to be integers. Since $\gcd(z_0,z_1) = 1$ if and only if $\gcd(z_0,z_1,z_0+z_1) = 1$, we may replace the condition $\gcd(z_0,z_1) = 1$ with $\gcd(x_0y_0, x_1y_1, x_2y_2) = 1$. Hence if $\mathbf{y} \in \mathbb{N}^3$, then $N_1(T_{\mathbf{y}} \cap \mathscr{C}, B)$ is just the quantity $\frac{1}{4}N^+_{C_{\mathbf{y}},H_{\mathbf{y}}}(B^{1/2})$ considered in Section 7.3. For $\mathbf{y} \in \mathbb{N}^3$ satisfying $\mu^2(y_0y_1y_2) = 1$, we define thin sets

$$T'_{\mathbf{y}} = \bigcup_{\substack{\mathbf{w} \in (\mathbb{Z}_{\neq 0})^3 \\ |w_i| = y_i \text{ for all } i}} T_{\mathbf{w}}.$$

By the arguments from Lemma 7.3.1, we have $N_1(T'_{\mathbf{y}} \cap \mathscr{C}, B) = 3N_1(T_{\mathbf{y}} \cap \mathscr{C}, B)$. To summarise, we have a disjoint union

$$\mathscr{C} = \bigcup_{\substack{\mathbf{y} \in \mathbb{N}^3 \\ \mu^2(y_0y_1y_2)=1}} (T'_{\mathbf{y}} \cap \mathscr{C}),$$

where from (7.3.4) and (7.3.8), each set appearing in this union satisfies

$$N_1(T'_{\mathbf{y}} \cap \mathscr{C}, B) = \frac{3}{4}N^+_{C_{\mathbf{y}},H_{\mathbf{y}}}(B^{1/2}) \sim \frac{3}{\pi}\left(\frac{\gamma(y_0y_1y_2)}{(y_0y_1y_2)^{3/2}}\sigma_{2,\mathbf{y}}\varrho(\mathbf{y})\right)B^{1/2}.$$

For a large integer $M$, we define

$$\mathscr{T}_M = \bigcup_{\substack{\mathbf{y} \in \mathbb{N}^3 \\ \mu^2(y_0y_1y_2)=1 \\ y_0,y_1,y_2 \leqslant M}} (T'_{\mathbf{y}} \cap \mathscr{C}). \tag{7.4.2}$$

This is a thin set of Campana points, because it is a finite union of the thin sets $T'_{\mathbf{y}} \cap \mathscr{C}$. We now assume Conjecture 7.1.1 holds, namely that $N_1(B) \sim$

$3c_{\mathrm{BV}}B^{1/2}$. We deduce that

$$\begin{aligned}\frac{N_1(\mathscr{C}\setminus\mathscr{T}_M,B)}{B^{1/2}} &= \frac{N_1(B)-N_1(\mathscr{T}_M,B)}{B^{1/2}}\\ &\sim 3c_{\mathrm{BV}}-\frac{3}{\pi}\sum_{\substack{\mathbf{y}\in\mathbb{N}^3\\ y_0,y_1,y_2\leqslant M}}\frac{\mu^2(y_0y_1y_2)\gamma(y_0y_1y_2)}{(y_0y_1y_2)^{3/2}}\sigma_{2,\mathbf{y}}\varrho(\mathbf{y})\\ &= \frac{3}{\pi}\sum_{\substack{\mathbf{y}\in\mathbb{N}^3\\ \max(y_0,y_1,y_2)>M}}\frac{\mu^2(y_0y_1y_2)\gamma(y_0y_1y_2)}{(y_0y_1y_2)^{3/2}}\sigma_{2,\mathbf{y}}\varrho(\mathbf{y}).\end{aligned}$$

Since the sum is convergent, this quantity tends to zero as $M\to\infty$. Therefore, we have shown that we can obtain an arbitrarily small positive constant by removing a thin set. We can now complete the proof of Theorem 7.1.3.

*Proof of Theorem 7.1.3.* We fix $\lambda\in(0,3c_{\mathrm{BV}}]$. For a subset $S\subset\mathscr{C}$, we define

$$S(B)=\{z\in S : H(z)\leqslant B\},$$

so that $\#S(B)=N_1(S,B)$ in our earlier notation. We require a Campana thin subset $\mathscr{T}\subseteq\mathscr{C}$ with $\#\mathscr{T}(B)\sim(3c_{\mathrm{BV}}-\lambda)B^{1/2}$.

For an appropriate choice of $M$, the thin set $\mathscr{T}_M$ defined in (7.4.2) satisfies $\#\mathscr{T}_M(B)\sim(3c_{\mathrm{BV}}-\lambda_0)B^{1/2}$ for some $\lambda_0\leqslant\lambda$. By definition, any subset of $\mathscr{T}_M$ is also thin. Therefore, it suffices to find a subset $\mathscr{T}\subseteq\mathscr{T}_M$ such that

$$\frac{\#\mathscr{T}_M(B)}{\#\mathscr{T}(B)}\sim\frac{3c_{\mathrm{BV}}-\lambda_0}{3c_{\mathrm{BV}}-\lambda}. \tag{7.4.3}$$

To achieve this, we take any subset $A\subseteq\mathbb{N}$ of the desired asymptotic density

$$\frac{A\cap[1,B]}{B}\sim\frac{3c_{\mathrm{BV}}-\lambda_0}{3c_{\mathrm{BV}}-\lambda}.$$

We enumerate the elements of $\mathscr{T}_M(B)$ by writing $\mathscr{T}_M(B)=\{t_1,t_2,\dots,t_R\}$, with $H(t_i)\leqslant H(t_j)$ whenever $i\leqslant j$. Then the set

$$\mathscr{T}=\{t_i\in\mathscr{T}_M : i\in A\}$$

is thin and satisfies (7.4.3), as required. □

## 7.5 Squareful values of binary quadratic forms

In this section, we study the constant $c_{\text{PSTV-A}}$ for an orbifold corresponding to squareful values of the binary quadratic form $ax^2+by^2$. We recall the setup from the introduction to this chapter. Throughout this section, $a$ and $b$ denote

positive integers satisfying $\mu^2(ab) = 1$ and $a, b \equiv 1 \pmod 4$. We consider the Campana orbifold $(X, D)$ over $\mathbb{Q}$, where $X = \mathbb{P}^1$ and $D$ is the divisor $\frac{1}{2}V(ax^2 + by^2)$, with the obvious good integral model $(\mathscr{X}, \mathscr{D})$. The set of Campana points in this example is not itself thin, as can be seen by combining [90, Theorem 1.1] and [90, Proposition 3.15]. Hence the PSTV-A conjecture applies to this orbifold. We take the naive height $H$ on $\mathbb{P}^1$, which is given by $H([x : y]) = \max(|x|, |y|)$ for $(x, y) \in \mathbb{Z}^2_{\text{prim}}$. The resulting counting problem, as given in (7.1.7), is

$$N(B) = \frac{1}{2}\#\left\{(x, y) \in \mathbb{Z}^2_{\text{prim}} : |x|, |y| \leqslant B, ax^2 + by^2 \text{ squareful}\right\}.$$

This section is organized as follows. In Section 7.5.1, we compute $c_{\text{PSTV-A}}$ for the orbifold $(\mathscr{X}, \mathscr{D})$ and the height $H$. In Section 7.5.2, we prove the asymptotic formula for $N(B)$ given in Theorem 7.1.5. Finally, in Section 7.5.3, we prove Corollary 7.1.7 by comparing the constants obtained in Sections 7.5.1 and 7.5.2.

### 7.5.1 Computation of the constant $c_{\text{PSTV-A}}$

The aim of this section is to prove the following theorem. We recall the notation $\gamma(n)$ from (7.3.7).

**Theorem 7.5.1.** *For the orbifold and the height function defined above, the constant $c_{PSTV\text{-}A}$ is equal to*

$$\frac{4\gamma(ab)}{\pi^2}\left(\frac{\sinh^{-1}\left(\sqrt{a/b}\right)}{\sqrt{a}} + \frac{\sinh^{-1}\left(\sqrt{b/a}\right)}{\sqrt{b}}\right)\prod_{p\nmid 2ab}\left(1 + \frac{1 + \left(\frac{-ab}{p}\right)}{(1 + p^{-1})p^{3/2}}\right).$$

To prove Theorem 7.5.1, we follow a similar framework to Section 3.3.2 and Section 7.2. We keep the convention from Section 7.2 that $p$ ranges over all primes, and $v$ is either a prime or $\infty$. We have $\alpha = 1/2$ and $\beta = 1$, and so $c_{\text{PSTV-A}} = \tau/2$. The divisor $V(ax^2+by^2)$ on $\mathbb{P}^1$ has degree 2, and corresponds to the line bundle $\mathscr{O}_{\mathbb{P}^1}(2)$. With the usual metrization, this line bundle determines the height function $\max(|x^2|, |y^2|)$ for $(x, y) \in \mathbb{Z}^2_{\text{prim}}$. Choosing the section $ax^2 + by^2$, we obtain

$$H_D = \prod_v H_{D,v},$$

where

$$H_{D,v} = \frac{\max(|x|_v, |y|_v)}{|ax^2 + by^2|_v^{1/2}}.$$

We use the chart $y \neq 0$, and take $z = x/y$. Then for any prime $p$, we have $\nu_p(az^2 + b) = \nu_p(ax^2 + by^2) - 2\nu_p(y)$. Consequently, the local Campana

condition that $\nu_p(ax^2+by^2)-2\min(\nu_p(x),\nu_p(y))\neq 1$ is equivalent to the condition that $\nu_p(az^2+b)$ is not equal to $1$ or a negative odd integer. Below, we denote by $\Omega_p$ the set of elements $z\in\mathbb{Q}_p$ satisfying this local Campana condition, and we set $\Omega_\infty=\mathbb{R}$. We let $\mathrm{d}z$ denote the usual $p$-adic measure or the Lebesgue measure, as appropriate. We obtain

$$c_{\text{PSTV-A}}=\frac{1}{2}\sigma_\infty\prod_p(1-p^{-1})\sigma_p, \tag{7.5.1}$$

where

$$\sigma_v=\int_{\Omega_v}\frac{\mathrm{d}z}{\max(|z|_v,1)|az^2+b|_v^{1/2}}. \tag{7.5.2}$$

To compute $\sigma_\infty$, we divide into regions $|z|\leqslant 1$ and $|z|>1$. This yields

$$\begin{aligned}\sigma_\infty&=\int_{|z|\leqslant 1}\frac{\mathrm{d}z}{(az^2+b)^{1/2}}+\int_{|z|>1}\frac{\mathrm{d}z}{|z|(az^2+b)^{1/2}}\\&=2\left(\frac{\sinh^{-1}\left(\sqrt{a/b}\right)}{\sqrt{a}}+\frac{\sinh^{-1}\left(\sqrt{b/a}\right)}{\sqrt{b}}\right).\end{aligned} \tag{7.5.3}$$

**Lemma 7.5.2.** *We have*

$$\sigma_p=\begin{cases}1+p^{-1}+\left(1+\left(\frac{-ab}{p}\right)\right)p^{-3/2}, & \text{if } p\nmid 2ab\\ 1, & \text{if } p\mid 2ab.\end{cases}$$

*Proof.* We split $\Omega_p$ into three regions $R_1,R_2,R_3$, defined respectively by the conditions

1. $\nu_p(z)\geqslant 1$,
2. $\nu_p(z)<0$,
3. $\nu_p(z)=0$.

We also divide into four cases $p\nmid 2ab$, $p|a$, $p\mid b$, and $p=2$. We let $\mu_p$ denote the usual $p$-adic measure.

*Case 1.* $p\nmid 2ab$: On $R_1$, we have $|az^2+b|_p=1$ and $\max(|z|_p,1)=1$, so

$$\int_{R_1}\frac{\mathrm{d}z}{\max(|z|_p,1)|az^2+b|_p^{1/2}}=\int_{\substack{z\in\mathbb{Q}_p\\ \nu_p(z)\geqslant 1}}1\,\mathrm{d}z=p^{-1}.$$

On $R_2$, we have $|az^2+b|_p = |z|_p^2$ and $\max(|z|_p,1) = |z|_p$, so we obtain a contribution of

$$\begin{aligned}\int_{\substack{z\in\mathbb{Q}_p\\ \nu_p(z)<0}} \frac{\mathrm{d}z}{|z|_p^2} &= \sum_{j=-\infty}^{-1} p^{2j}\mu_p(\{z\in\mathbb{Q}_p : \nu_p(z)=j\})\\ &= \sum_{j=1}^{\infty}(1-p^{-1})p^{-j}\\ &= p^{-1}.\end{aligned}$$

On $R_3$, we have $|az^2+b|_p \leqslant 1$ and $\max(|z|_p,1)=1$. For $j\geqslant 0$, we define

$$\begin{aligned}f(j) &= \mu_p(\{z\in\mathbb{Z}_p^\times : \nu_p(az^2+b)=j\}),\\ g(j) &= \mu_p(\{z\in\mathbb{Z}_p^\times : \nu_p(az^2+b)\geqslant j\}).\end{aligned}$$

We have

$$\int_{R_3}\frac{\mathrm{d}z}{\max(|z|_p,1)|az^2+b|_p^{1/2}} = \int_{z\in\mathbb{Z}_p^\times\cap\Omega_p}\frac{\mathrm{d}z}{|az^2+b|_p^{1/2}} = \sum_{\substack{j\geqslant 0\\ j\neq 1}} p^{j/2}f(j). \quad (7.5.4)$$

Clearly $f(j)=g(j)-g(j+1)$ for any $j\geqslant 0$. We now compute $g(j)$. We have $g(0)=\mu_p(\mathbb{Z}_p^\times)=1-p^{-1}$. By Hensel's Lemma, for $j\geqslant 1$, we have

$$\begin{aligned}g(j) &= p^{-j}\#\{z \pmod{p^j} : az^2\equiv -b \pmod{p^j}\}\\ &= p^{-j}\left(1+\left(\frac{-ab}{p}\right)\right).\end{aligned}$$

Therefore, the right hand side of (7.5.4) equals

$$\begin{aligned}&1-p^{-1}-p^{-1}\left(1+\left(\frac{-ab}{p}\right)\right)+\sum_{j\geqslant 2}(1-p^{-1})p^{-j/2}\left(1+\left(\frac{-ab}{p}\right)\right)\\ &= 1-p^{-1}+\left(1+\left(\frac{-ab}{p}\right)\right)p^{-3/2}.\end{aligned}$$

Combining the three regions, we have completed the proof for primes $p\nmid 2ab$.

*Case 2.* $p\mid b$: This time, the region $R_1$ contributes zero, because if $p\mid b$ and $\nu_p(z)\geqslant 1$ then $\nu_p(az^2+b)=1$ (by the assumption that $b$ is squarefree), and so $z\notin\Omega_p$. The region $R_2$ contributes $p^{-1}$ to the integral in (7.5.2) by the same calculation as in Case 1. On the region $R_3$ we have $\nu_p(az^2+b)=0$, and so

$$\int_{R_3}\frac{\mathrm{d}z}{\max(|z|_p,1)|az^2+b|_p^{1/2}} = \int_{z\in\mathbb{Z}_p^\times} 1\,\mathrm{d}z = 1-p^{-1}.$$

Hence $\sigma_p = p^{-1} + 1 - p^{-1} = 1$.

*Case 3.* $p \mid a$: The region $R_1$ contributes $p^{-1}$ by the same calculation as in Case 1. On $R_2$, we have $\nu_p(az^2+b) = 2\nu_p(z)+1$, which is an odd negative integer, and so the contribution is zero. On $R_3$, we have $\nu_p(az^2+b) = 0$ (since $p \nmid b$ by the assumptions $p \mid a$ and $\mu^2(ab) = 1$), and so we obtain a contribution of $1 - p^{-1}$ as in Case 2. Combining, we have $\sigma_p = p^{-1} + 1 - p^{-1} = 1$.

*Case 4.* $p = 2$: Regions $R_1$ and $R_2$ contribute $p^{-1}$ to the integral in (7.5.2) as in Case 1. The region $R_3$ contributes zero. To see this, we note that if $z \in \mathbb{Z}_2^\times$, then $z^2 \equiv 1 \pmod 4$. However, since $a, b \equiv 1 \pmod 4$, we have $az^2+b \equiv 2 \pmod 4$, and hence $\nu_p(az^2+b) = 1$. Hence $\sigma_2 = 2^{-1}+2^{-1} = 1$. □

Let $\sigma_\infty$ be as given in (7.5.3). We conclude from (7.5.1) and Lemma 7.5.2 that

$$\begin{aligned} c_{\text{PSTV-A}} &= \frac{\sigma_\infty}{2} \prod_{p \nmid 2ab} (1-p^{-1}) \left(1 + p^{-1} + \left(1 + \left(\frac{-ab}{p}\right)\right) p^{-3/2}\right) \prod_{p \mid 2ab} (1-p^{-1}) \\ &= \frac{\sigma_\infty}{2} \cdot \frac{6}{\pi^2} \prod_{p \nmid 2ab} \left(1 + \frac{1 + \left(\frac{-ab}{p}\right)}{(1+p^{-1})p^{3/2}}\right) \prod_{p \mid 2ab} \frac{1}{1+p^{-1}} \\ &= \frac{2\sigma_\infty \gamma(ab)}{\pi^2} \prod_{p \nmid 2ab} \left(1 + \frac{1 + \left(\frac{-ab}{p}\right)}{(1+p^{-1})p^{3/2}}\right). \end{aligned} \tag{7.5.5}$$

This completes the proof of Theorem 7.5.1.

## 7.5.2 The asymptotic formula for $N(B)$

In this section, we prove Theorem 7.1.5. We write $ax^2+by^2 = u^2v^3$ for $v \in \mathbb{Z}_{\neq 0}$ squarefree and $u \in \mathbb{N}$. If $\gcd(x,y) = 1$, then $\gcd(a,v) = 1$ and $\gcd(b,v) = 1$. This is because if $p \mid \gcd(a,v)$ then $p \mid by^2$, and since $\gcd(a,b) = 1$, this implies that $p \mid y$. But then $p^2 \mid ax^2$, and since $a$ is squarefree, we have $p \mid x$. This contradicts the assumption $\gcd(x,y) = 1$. The argument to show that $\gcd(b,v) = 1$ is the same by symmetry. Hence $a, b$ and $v$ are squarefree and pairwise coprime, in other words $\mu^2(abv) = 1$. Moreover, the assumptions $a, b > 0$ imply that $v > 0$. Therefore, we have

$$N(B) = \frac{1}{2} \sum_{v=1}^{\infty} \mu^2(abv) N_v(B),$$

where

$$N_v(B) = \frac{1}{2} \# \left\{ (x,y,u) \in \mathbb{Z}^3 : \begin{array}{l} \gcd(x,y) = 1, |x|, |y| \leqslant B \\ ax^2+by^2 = u^2v^3 \end{array} \right\}.$$

The factor $1/2$ comes from the fact that there are two choices for the sign of $u$ in $[x : y : u]$ corresponding to each point $[x : y]$ enumerated by $N(B)$.

Throughout this section, all implied constants depend only on $a, b$ and $\epsilon$. We split the sum over $v$ into ranges $v < B^\delta$ and $v \geqslant B^\delta$, for a fixed $\delta > 0$. To deal with the range $v \geqslant B^\delta$, we note that $ax^2+by^2 = u^2v^3$ and $|x|, |y| \leqslant B$ together imply that $u^2v^3 \ll B^2$, so $u \ll Bv^{-3/2}$. Therefore, there are $O(Bv^{-3/2})$ choices for $u$. Applying a result of Browning and Gorodnik [13, Theorem 1.11], for any fixed $u, v$, we have

$$\#\left\{(x, y) \in \mathbb{Z}^2_{\text{prim}} : ax^2 + by^2 = u^2v^3\right\} = O(B^\epsilon).$$

Hence $N_v(B) \ll B^{1+\epsilon}v^{-3/2}$. Taking a sum over $v \geqslant B^\delta$, we obtain

$$\sum_{v \geqslant B^\delta} \mu^2(abv)N_v(B) \ll B^{1+\epsilon-\delta/2}, \tag{7.5.6}$$

and so the contribution from the range $v \geqslant B^\delta$ is negligible.

For the range $v < B^\delta$, we view the equation $ax^2 + by^2 = u^2v^3$ as a conic, with $a, b$ and $v$ fixed. Sofos [111] counts rational points on isotropic conics by using a birational map from the conic to $\mathbb{P}^1$ in order to parameterise the solutions as lattice points. Unfortunately, we cannot apply [111, Theorem 1.1] directly, since the coprimality condition $\gcd(x, y, u) = 1$ is used instead of $\gcd(x, y) = 1$. However, the argument can be adapted to deal with this alternative coprimality condition. We summarise the main alterations required.

Let $Q$ be a non-singular quadratic form in $3$ variables with integer coefficients. Let $\Delta_Q$ denote the discriminant of $Q$, and $\langle Q\rangle$ the maximum modulus of the coefficients of $Q$. Suppose that $\|\cdot\|$ is a norm isometric to the supremum norm. For convenience, below we use variables $\mathbf{x} = (x_1, x_2, x_3)$ in place of $(x, y, u)$. We define

$$N_{\|\cdot\|}(Q, B) = \#\{\mathbf{x} \in \mathbb{Z}^3 : \gcd(x_1, x_2) = 1, Q(\mathbf{x}) = 0, \|\mathbf{x}\| \leqslant B\}.$$

This is the same as the counting function from [111], but with the condition $\gcd(x_1, x_2) = 1$ instead of $\gcd(x_1, x_2, x_3) = 1$. We let $Q_v(\mathbf{x}) = ax_1^2 + bx_2^2 - v^3x_3^2$, and define a norm $\|\cdot\|$ by $\|\mathbf{x}\| = \max(|x_1|, |x_2|)$. There is a constant $C$, depending only on $a$ and $b$, such that $\|\mathbf{x}\| = \max(|x_1|, |x_2|, Cv^{3/2}|x_3|)$, and so $\|\cdot\|$ is isometric to the supremum norm. In our earlier notation, we have $N_v(B) = N_{\|\cdot\|}(Q_v, B)$.

As in [111, Section 6], the first stage is to apply a linear change of variables in order to transform $Q_v$ into a quadratic form $Q$ satisfying $Q(0, 1, 0) = 0$. We assume that $N_v(B) > 0$, so that there exists $(t_{12}, t_{22}, t_{32}) \in \mathbb{Z}^3$ with $Q_v(t_{12}, t_{22}, t_{32}) = 0$ and $\gcd(t_{12}, t_{22}) = 1$; we shall choose the smallest such

solution. Then we can find integers $t_{11}, t_{21}$ such that $t_{11}t_{22} - t_{21}t_{12} = 1$ and $|t_{11}|, |t_{21}| \leqslant \max(|t_{12}|, |t_{22}|)$. Let

$$M = \begin{pmatrix} t_{11} & t_{12} & 0 \\ t_{21} & t_{22} & 0 \\ 0 & t_{32} & 1 \end{pmatrix}.$$

We define $Q(\mathbf{x}) = Q_v(M\mathbf{x})$ and $\|\mathbf{x}\|' = \|M\mathbf{x}\|$. Since the first $2 \times 2$ minor of $M$ is an element of $SL_2(\mathbb{Z})$, the coprimality condition $\gcd(x_1, x_2) = 1$ is preserved under this transformation. Therefore $N_{\|\cdot\|}(Q_v, B) = N_{\|\cdot\|'}(Q, B)$, which we shall abbreviate to $N(Q, B)$.

The forms $L(s,t)$ and $g(s,t)$ defined in [111, Equation (2.3)] can be written explicitly as

$$L(s,t) = (2at_{11}t_{12} + 2bt_{21}t_{22})s - 2v^3t_{32}t, \tag{7.5.7}$$
$$g(s,t) = (at_{11}^2 + bt_{21}^2)s^2 - v^3t^2. \tag{7.5.8}$$

As in [111, Equation (2.4)], we let $\boldsymbol{q} = (q_1, q_2, q_3) = (q_1(s,t), q_2(s,t), q_3(s,t))$, where

$$q_1(s,t) = sL(s,t), \qquad q_2(s,t) = -g(s,t), \qquad q_3(s,t) = tL(s,t).$$

By applying the parameterisation argument from [111, Lemma 3.1], we find that $N(Q,B) = \mathscr{N}(Q,B) + O(1)$, where

$$\mathscr{N}(Q,B) = \#\left\{(s,t) \in \mathbb{Z}^2_{\text{prim}} : t > 0, \|\boldsymbol{q}\|' \leqslant \lambda B, \gcd\left(\frac{q_1}{\lambda}, \frac{q_2}{\lambda}\right) = 1\right\} \tag{7.5.9}$$

and $\lambda = \gcd(q_1, q_2, q_3)$.

We now take a sum over the possible values of $\lambda$. Due to our alternative coprimality condition, in (7.5.9) we have the stronger condition $\gcd(\frac{q_1}{\lambda}, \frac{q_2}{\lambda}) = 1$ in place of $\gcd(\frac{q_1}{\lambda}, \frac{q_2}{\lambda}, \frac{q_3}{\lambda}) = 1$, and so when applying Möbius inversion we take a sum over a variable $r$ with $r \mid \left(\frac{q_1}{\lambda}, \frac{q_2}{\lambda}\right)$ in place of Sofos' sum over $k \mid \left(\frac{q_1}{\lambda}, \frac{q_2}{\lambda}, \frac{q_3}{\lambda}\right)$. As in [111, Equation (3.2)], we define

$$M^*_{\sigma,\tau}(T,n) = \#\{(s,t) \in \mathbb{Z}^2_{\text{prim}} : (s,t) \equiv (\sigma,\tau) \pmod n, t > 0, \|\boldsymbol{q}\|' \leqslant T\}.$$

Then similarly to [111, Lemma 3.2], we obtain

$$\mathscr{N}(Q,B) = \sum_{\lambda \mid \Delta_Q} \sum_r \mu(r) \sideset{}{^+}\sum_{\sigma,\tau} M^*_{\sigma,\tau}(B\lambda, r\lambda), \tag{7.5.10}$$

where $\sum^+$ denotes a sum over residues $\sigma, \tau$ modulo $r\lambda$ such that $\lambda \mid \boldsymbol{q}(\sigma,\tau)$, $r\lambda \mid (q_1(\sigma,\tau), q_2(\sigma,\tau))$ and $\gcd(\sigma, \tau, r\lambda) = 1$.

We now explain why with our choice of $Q$, we may restrict the $r$-sum in (7.5.10) to divisors of $\lambda$. Since $r$ is squarefree, it suffices to show that for any prime $p \mid (q_1, q_2)$, we also have $p \mid q_3$. (In general, $\gcd(q_1, q_2)$ can still be larger than $\lambda$ since its prime factors can occur with higher multiplicity.) Suppose that $p \mid (q_1, q_2)$. We immediately deduce that $p \mid q_3$ if $p \mid L(s,t)$, and so using $p \mid q_1$ we may assume that $p \mid s$. Since $\gcd(s,t) = 1$ and $p \mid q_2$, we see from (7.5.8) that $p \mid v$. However, then from (7.5.7) we have that $p \mid L(s,t)$ after all, and so $p \mid q_3$, as desired.

An asymptotic formula for $N(Q,B)$ can now be deduced by applying the lattice counting results from [111, Section 4] to estimate $M^*_{\sigma,\tau}(B\lambda, r\lambda)$. We maintain control over the resulting error terms after performing the summations in (7.5.10) thanks to the restriction on the $r$-sum. Similarly to [111, Proposition 2.1], we obtain

$$N(Q,B) = c_v B + O((BK)^{1/2+\epsilon}(|\Delta_Q| + \langle Q \rangle)^{1+\epsilon}) \tag{7.5.11}$$

for some constant $c_v > 0$, where

$$K = \sup_{\mathbf{x} \neq \mathbf{0}} \left(1 + \frac{\|\mathbf{x}\|_\infty}{\|\mathbf{x}\|'}\right)$$

and $\|\mathbf{x}\|_\infty = \max(|x_1|, |x_2|, |x_3|)$ denotes the supremum norm of $\mathbf{x}$.

We have $\Delta_Q = \Delta_{Q_v} = abv^3 \ll v^3$. Let $\|M\|_\infty$ denote the maximum modulus of the entries of $M$. Then $\langle Q \rangle \ll \|M\|_\infty^2$. Moreover, making a change of variables from $\mathbf{x}$ to $M^{-1}\mathbf{x}$ in the definition of $K$, we have

$$K = \sup_{\mathbf{x} \neq \mathbf{0}} \left(1 + \frac{\|M^{-1}\mathbf{x}\|_\infty}{\|\mathbf{x}\|}\right) \ll \|M^{-1}\|_\infty \sup_{\mathbf{x} \neq \mathbf{0}} \left(1 + \frac{\|\mathbf{x}\|_\infty}{\|\mathbf{x}\|}\right) \ll \|M^{-1}\|_\infty.$$

Using the bound $\|M^{-1}\|_\infty \ll \|M\|_\infty^2$, we conclude that

$$N(Q,B) = c_v B + O((B\|M\|_\infty^2)^{1/2+\epsilon}(v^3 + \|M\|_\infty^2)^{1+\epsilon}). \tag{7.5.12}$$

We recall that $\|M\|_\infty = \max(|t_{12}|, |t_{22}|, |t_{32}|)$ is the size of the least integral solution to $Q_v(\mathbf{x}) = 0$ with $\gcd(x_1, x_2) = 1$. Cassels [27] establishes an upper bound for the smallest integral solution to a quadratic form. In the following lemma, we find a bound for the least solution satisfying our additional coprimality condition.

**Lemma 7.5.3.** *Suppose that $a, b, v$ are integers with $\mu^2(abv) = 1$. Let $Q_v$ denote the quadratic form $ax_1^2 + bx_2^2 - v^3x_3^2$. Then if the system*

$$\begin{cases} Q_v(\mathbf{x}) = 0, \\ \mathbf{x} \in \mathbb{Z}^3,\ \gcd(x_1, x_2) = 1 \end{cases} \tag{7.5.13}$$

*has a nontrivial solution, it has a solution satisfying $\|\mathbf{x}\|_\infty \ll |v|^7$.*

**Remark 7.5.4.** The bound $\|\mathbf{x}\|_\infty \ll |v|^7$ is much weaker than the corresponding bound found by Cassels [27], who established that without the coprimality condition $\gcd(x_1, x_2) = 1$, the smallest nontrivial solution $\mathbf{x}$ to (7.5.13) satisfies $\|\mathbf{x}\|_\infty \ll |v|^3$ (i.e., the maximum modulus of the coefficients of the quadratic form).

We deduce Lemma 7.5.3 from the following result of Dietmann, which generalises Cassel's argument by imposing congruence conditions on the variables.

**Lemma 7.5.5.** *[45, Proposition 1] Let $Q$ be a non-degenerate quadratic form in $3$ variables with integral coefficients. Let $\boldsymbol{\xi} \in \mathbb{Z}^3$ and $\eta \in \mathbb{N}$. Suppose that there exists an integral solution to the system*

$$\begin{cases} Q(\mathbf{x}) = 0, \\ \mathbf{x} \equiv \boldsymbol{\xi} \pmod{\eta}. \end{cases} \tag{7.5.14}$$

*Then there exists an integral solution to this system satisfying*

$$\|\mathbf{x}\|_\infty \ll \max\{\eta^3 |\Delta_Q|^2 \langle Q \rangle^2, \eta^3 |\Delta_Q|^3\}.$$

*Proof of Lemma 7.5.3.* Suppose that $\mathbf{y} = (y_1, y_2, y_3)$ is a solution to (7.5.13). Let $Q_0$ denote the quadratic form $ax_1^2 + bx_2^2 - vx_3^2$. Then clearly $Q_0(y_1, y_2, vy_3) = 0$. Let $\eta = |v|$ and let $\boldsymbol{\xi} = (\xi_1, \xi_2, 0)$ denote the residues of $(y_1, y_2, vy_3)$ modulo $\eta$. We have $\gcd(y_1, v) = 1$, because if $p \mid (y_1, v)$ then $p \mid by_2^2$, but since $\mu^2(abv) = 1$ this implies $p \mid y_2$, contradicting the assumption $\gcd(y_1, y_2) = 1$. Consequently, $\xi_1$ is invertible modulo $\eta$.

Since $\Delta_{Q_0} \ll |v|$ and $\langle Q_0 \rangle \ll |v|$, we find from Lemma 7.5.5 an integral solution $\mathbf{z} = (z_1, z_2, z_3)$ to (7.5.14) with the above choice of $Q_0, \eta, \boldsymbol{\xi}$, and with $\|\mathbf{z}\|_\infty \ll |v|^7$. Choose $\mathbf{x} = (z_1, z_2, z_3/v)/\lambda$, where $\lambda = \gcd(z_1, z_2, z_3/v)$. This is an integral solution to $Q_v = 0$ because $z_3 \equiv 0 \pmod{v}$. Additionally, the bound $\|\mathbf{z}\|_\infty \ll |v|^7$ implies that $\|\mathbf{x}\|_\infty \ll |v|^7$. To complete the proof, it suffices to show that $\gcd(x_1, x_2) = 1$, or equivalently that $\gcd(z_1, z_2) = \lambda$. Clearly $\lambda \mid \gcd(z_1, z_2)$. Conversely, suppose that $h \mid (z_1, z_2)$. From $Q_0(\mathbf{z}) = 0$, we see that $h \mid vz_3$. However, since $z_1 \equiv \xi_1 \pmod{\eta}$ and $\xi_1$ is invertible modulo $\eta$, we have $\gcd(h, v) = 1$. Therefore, $h \mid z_3/v$, and so $h \mid \lambda$, as required. □

Substituting the bound $\|M\|_\infty \ll v^7$ from Lemma 7.5.3 into (7.5.12) we conclude that

$$N_v(B) = c_v B + O(B^{1/2+\epsilon} v^{21}).$$

The leading constant $c_v$ could be computed explicitly from the above method. However, we note that by [94, Example 3.2], equidistribution holds for smooth

isotropic conics, and so $c_v$ is known to be the constant predicted in Manin's conjecture. More precisely, we have

$$c_v = \frac{1}{2}\sigma_{\infty,v}\prod_p \sigma_{p,v},$$

where $\sigma_{\infty,v}$ is the real density from Manin's conjecture applied to $N_v(B)$, and

$$\begin{aligned}\sigma_{p,v} &= \lim_{n\to\infty}\frac{M_v(p^n)}{p^{2n}},\\ M_v(p^n) &= \#\left\{(x,y) \pmod{p^n} : p\nmid \gcd(x,y), ax^2+by^2\equiv u^2v^3\right\}.\end{aligned}$$

Combining with (7.5.6) and choosing $\delta = 1/45$, we obtain

$$N(B) = \frac{1}{2}\sum_{v\leqslant B^\delta}\mu^2(abv)c_vB + O(B^{89/90+\epsilon}). \tag{7.5.15}$$

We are now in a very similar situation to the one encountered in Section 7.3, but with coefficients $(a,b,v^3)$ in place of $(y_0^3,y_1^3,y_2^3)$. Analogously to (7.3.8), we define

$$c_{H_{(a,b,v)}}(C_{(a,b,v)}(\mathbb{A}_{\mathbb{Q}})^+) = \frac{4}{\pi}\cdot\frac{\mu^2(abv)\gamma(abv)}{(abv^3)^{1/2}}\sigma_{2,(a,b,v)}\varrho(a,b,v).$$

The only difference between $c_v$ and $c_{H_{(a,b,v)}}(C_{(a,b,v)}(\mathbb{A}_{\mathbb{Q}})^+)$ lies in the computation of the density at the infinite place. This difference stems from the height $H$ in the definition of $N(B)$ being used in place of the height $H_{(a,b,v)}$ from (7.3.2). Replacing the real density $\pi/(abv^3)^{1/2}$ appearing in [22, Section 2.3] with the appropriate real density $\sigma_{\infty,v}$ for our setup, we have

$$c_v = \frac{(abv^3)^{1/2}}{\pi}\sigma_{\infty,v}c_{H_{(a,b,v)}}(C_{(a,b,v)}(\mathbb{A}_{\mathbb{Q}})^+). \tag{7.5.16}$$

To compute $\sigma_{\infty,v}$, we use the Leray form as in [22, Section 2.3] to obtain

$$\begin{aligned}\sigma_{\infty,v} &= \frac{1}{2v^{3/2}}\int_{[-1,1]^2}\frac{\mathrm{d}x\,\mathrm{d}y}{\sqrt{ax^2+by^2}}\\ &= \frac{1}{2v^{3/2}}\int_{-1}^{1}\frac{2}{\sqrt{a}}\sinh^{-1}\left(\frac{1}{y}\sqrt{\frac{a}{b}}\right)\mathrm{d}y\\ &= \frac{2}{v^{3/2}a^{1/2}}\left(\sinh^{-1}\left(\sqrt{\frac{a}{b}}\right)+\frac{\sinh^{-1}\left(\sqrt{\frac{b}{a}}\right)}{\sqrt{b/a}}\right)\\ &= \frac{2}{v^{3/2}}\left(\frac{\sinh^{-1}\left(\sqrt{a/b}\right)}{\sqrt{a}}+\frac{\sinh^{-1}\left(\sqrt{b/a}\right)}{\sqrt{b}}\right).\end{aligned} \tag{7.5.17}$$

Hence $\sigma_{\infty,v} = \sigma_\infty v^{-3/2}$, where $\sigma_\infty$ is the real density from the PSTV-A conjecture, as computed in (7.5.3). Due to the assumptions $a \equiv b \equiv 1 \pmod 4$, the density at the prime $2$ from (7.3.12) simplifies to

$$\sigma_{2,(a,b,v)} = \begin{cases} 1, & \text{if } v \equiv 1 \pmod 4, \\ 0, & \text{otherwise.} \end{cases}$$

Combining this with (7.5.16) and (7.3.8), we conclude that

$$c_v = \begin{cases} \frac{4\sigma_\infty \gamma(abv)\varrho(a,b,v)}{\pi^2 v^{3/2}}, & \text{if } v \equiv 1 \pmod 4, \\ 0, & \text{otherwise.} \end{cases} \tag{7.5.18}$$

In particular, $c_v \ll v^{-3/2+\epsilon}$. This allows us to extend the sum in (7.5.15) to an infinite sum over $v$, with the same error term $O(B^{1+\epsilon-\delta/2})$ that is already present in (7.5.15). We conclude that $N(B) = cB + O(B^{89/90+\epsilon})$, where

$$c = \frac{2\sigma_\infty}{\pi^2} \sum_{v \equiv 1 \pmod 4} \frac{\mu^2(abv)\gamma(abv)\varrho(a,b,v)}{v^{3/2}}. \tag{7.5.19}$$

This completes the proof of Theorem 7.1.5.

### 7.5.3 Comparison of $c$ and $c_{\text{PSTV-A}}$

Continuing from (7.5.19), we pull out a factor $\gamma(ab)$, and replace $\mu^2(abv)$ with $\mu^2(v)$ and the condition $\gcd(v, ab) = 1$. This allows us to rewrite $c$ as

$$c = R \sum_{\substack{v \equiv 1 \pmod 4 \\ \gcd(v,ab)=1}} \frac{\mu^2(v)\gamma(v)\varrho(a,b,v)}{v^{3/2}}, \tag{7.5.20}$$

where $R := 2\sigma_\infty \gamma(ab)/\pi^2$ is the same factor that appears in $(7.5.5)$. It remains to compare the sum in (7.5.20) with the Euler product from (7.5.5).

If $\varrho(a,b,v) \neq 0$ and $v$ is odd, then using (7.3.12) and the assumption $a, b \equiv 1 \pmod 4$, we have $v \equiv 1 \pmod 4$. Hence we may relax the condition in the $v$-sum of (7.5.20) to $\gcd(v, 2ab) = 1$. We define

$$f(v) = \frac{\mu^2(v)\gamma(v)}{v^{3/2}} \prod_{p \mid v} \left(1 + \left(\frac{-ab}{v}\right)\right).$$

The function $f$ is multiplicative in $v$. Therefore, from (7.5.20), we have

$$\begin{aligned} \frac{c}{R} &= \sum_{\gcd(v,2ab)=1} f(v) \prod_{p \mid a} \left(1 + \left(\frac{bv}{p}\right)\right) \prod_{p \mid b} \left(1 + \left(\frac{av}{p}\right)\right) \\ &= \sum_{k \mid a} \sum_{l \mid b} \sum_{\gcd(v,2ab)=1} f(v) \left(\frac{bv}{k}\right) \left(\frac{av}{l}\right), \end{aligned}$$

where the summand is multiplicative in $v$. We conclude that

$$\frac{c}{R} = \sum_{k|a} \sum_{l|b} \prod_{p \nmid 2ab} \left( \left(\frac{b}{k}\right) \left(\frac{a}{l}\right) + \frac{\left(\frac{bp}{k}\right) \left(\frac{ap}{l}\right) \left(1 + \left(\frac{-ab}{p}\right)\right)}{(1+p^{-1})p^{3/2}} \right). \tag{7.5.21}$$

We recognise the contribution to (7.5.21) from $k = l = 1$ as precisely the Euler product $c_{\text{PSTV-A}}/R$ from (7.5.5). If $a = 1$, which is a special case of the norm forms considered in [115], then (7.5.21) simplifies to

$$\frac{c}{R} = \sum_{l|b} \prod_{p \nmid 2b} \left( 1 + \frac{\left(\frac{p}{l}\right) \left(1 + \left(\frac{-b}{p}\right)\right)}{(1+p^{-1})p^{3/2}} \right).$$

The contribution from each divisor $l$ is positive. We summarize as follows.

**Lemma 7.5.6.** *Suppose that $a = 1$, $\mu^2(b) = 1$ and $b \equiv 1 \pmod 4$. Then*

*i)* $c_{PSTV\text{-}A} = c$ *if* $b = 1$,

*ii)* $c_{PSTV\text{-}A} < c$ *if* $b > 1$.

Similarly to the situation from Section 7.4, we can obtain any constant in $(0, c]$, including $c_{\text{PSTV-A}}$ itself, by the removal of an appropriate thin set.

Finally, we show that when $a, b > 1$, it is possible that $c < c_{\text{PSTV-A}}$. Since the removal of thin sets can only reduce the constant $c$, this provides a counterexample to the leading constant predicted by the PSTV-A conjecture.

*Proof of Corollary 7.1.7.* We take $a, b > 7$ to be distinct primes satisfying the following conditions.

1. $a, b \equiv 1 \pmod 4$.
2. $\left(\frac{a}{b}\right) = -1$.
3. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$ for $p \in \{3, 7\}$.
4. $\left(\frac{a}{5}\right) = -1$ and $\left(\frac{b}{5}\right) = 1$.

The pair $a = 37, b = 109$ satisfies conditions $(1)$–$(4)$. In fact, $(1)$–$(4)$ are equivalent to $a, b$ lying in certain congruence classes, and so by Dirichlet's theorem on primes in arithmetic progressions, these conditions are satisfied by infinitely many pairs of distinct primes $a, b$.

Using conditions $(1)$ and $(2)$, the right hand side of (7.5.21) simplifies to

$$\frac{c}{R} = S(\chi_0) - S(\chi_1) - S(\chi_2) + S(\chi_3), \tag{7.5.22}$$

where

$$S(\chi_0) = \prod_{p\nmid 2ab}\left(1+\frac{1+\left(\frac{-ab}{p}\right)}{(1+p^{-1})p^{3/2}}\right), \quad S(\chi_1) = \prod_{p\nmid 2ab}\left(1+\frac{\left(\frac{a}{p}\right)\left(1+\left(\frac{-ab}{p}\right)\right)}{(1+p^{-1})p^{3/2}}\right),$$
$$S(\chi_2) = \prod_{p\nmid 2ab}\left(1+\frac{\left(\frac{b}{p}\right)\left(1+\left(\frac{-ab}{p}\right)\right)}{(1+p^{-1})p^{3/2}}\right), \quad S(\chi_3) = \prod_{p\nmid 2ab}\left(1+\frac{\left(\frac{ab}{p}\right)\left(1+\left(\frac{-ab}{p}\right)\right)}{(1+p^{-1})p^{3/2}}\right).$$

Since $S(\chi_0) = c_{\text{PSTV-A}}/R$, it suffices to show that $S(\chi_3) - S(\chi_1) - S(\chi_2) < 0$. From conditions $(3)$ and $(4)$, we have that all the Euler factors for $S(\chi_1), S(\chi_2)$ and $S(\chi_3)$ are equal to 1 for $p \leqslant 7$. For $p > 7$, we estimate the Euler factors trivially to obtain

$$\begin{aligned} S(\chi_3) - S(\chi_1) - S(\chi_2) & \\ &\leqslant \prod_{p>7}\left(1+\frac{2}{(1+p^{-1})p^{3/2}}\right) - 2\prod_{p>7}\left(1-\frac{2}{(1+p^{-1})p^{3/2}}\right). \end{aligned}$$

Similarly to the end of Section 7.2, we can use convergence factors to compute numerically that

$$\prod_{p}\left(1+\frac{2}{(1+p^{-1})p^{3/2}}\right)\left(1-\frac{2}{(1+p^{-1})p^{3/2}}\right)^{-1} = 15.206698... < 16.$$

On the other hand, it can be computed that

$$\prod_{p\leqslant 7}\left(1+\frac{2}{(1+p^{-1})p^{3/2}}\right)\left(1-\frac{2}{(1+p^{-1})p^{3/2}}\right)^{-1} = 8.231089... > \frac{16}{2}.$$

It follows that $S(\chi_3) - S(\chi_1) - S(\chi_2) < 0$, as required. □

**Remark 7.5.7.** In the examples considered above, the divisor $D$ does not have strict normal crossings at the primes dividing $ab$. From this point of view, it seems natural to ask whether counting Campana $\mathbb{Z}[1/ab]$-points instead of Campana $\mathbb{Z}$-points reconciles the two leading constants $c$ and $c_{\text{PSTV-A}}$. However, it can be checked that in this setup, by a similar argument to the proof of Corollary 7.1.7, there are still values of $a, b$ which provide a counterexample to the PSTV-A conjecture.

CHAPTER 8

# Polynomials represented by norm forms via the beta sieve

## 8.1 Introduction

Let $K$ be a number field of degree $n$, and let $f \in \mathbb{Z}[t]$ be a polynomial. A central problem in Diophantine geometry is to determine under what conditions $f$ can take values equal to a norm of an element of $K$. In order to address this question, we take an integral basis $\omega_1, \dots, \omega_n$ for $K$, viewed as a vector space over $\mathbb{Q}$, and define the *norm form* as $\mathbf{N}(\mathbf{x}) = N_{K/\mathbb{Q}}(\omega_1 x_1 + \cdots + \omega_n x_n)$, where $N_{K/\mathbb{Q}}(\cdot)$ is the field norm. We then seek to understand when the equation

$$f(t) = \mathbf{N}(\mathbf{x}) \neq 0 \tag{8.1.1}$$

has a solution with $(t, x_1, \dots, x_n) \in \mathbb{Q}^{n+1}$. We recall from the Introduction that the *Hasse principle* holds for (8.1.1) if having solutions over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime $p$ is enough to guarantee existence of a solution to (8.1.1) over $\mathbb{Q}$.

Local to global questions for (8.1.1) have received much attention over the years. The first case to consider is when $f$ is a nonzero constant polynomial. Here, the Hasse principle for (8.1.1) is known as the *Hasse norm principle*. More precisely, we say that the *Hasse norm principle* holds for the extension $K/\mathbb{Q}$ if $\mathbb{Q}^\times \cap N_{K/\mathbb{Q}}(I_K) = N_{K/\mathbb{Q}}(K^\times)$, where $I_K = \mathbb{A}_K^\times$ is the group of ideles of $K$. The Hasse norm principle has been extensively studied, beginning with the work of Hasse himself, who established that it holds for cyclic extensions $K/\mathbb{Q}$ (a result known as the *Hasse norm theorem*), but does not hold for certain biquadratic extensions, such as $K = \mathbb{Q}(\sqrt{13}, \sqrt{-3})$. The Hasse norm principle is also known to hold if the degree of $K$ is prime (Bartels [2]), or if the normal

closure of $K$ has Galois group $S_n$ (Kunyavskiĭ and Voskresenskiĭ [76]) or $A_n$ (Macedo [83]).

When $[K : \mathbb{Q}] = 2$ and $f$ is irreducible of degree $3$ or $4$, (8.1.1) defines a Châtelet surface. There are now many known counterexamples to the Hasse principle for Châtelet surfaces, including one by Iskovskikh [70], which we discuss in more detail in Example 8.3.4. However, Colliot-Thélène, Sansuc and Swinnerton-Dyer [37] prove that the Brauer–Manin obstruction accounts for all failures of the Hasse principle. A similar result holds when $f$ is an irreducible polynomial of degree at most $3$ and $[K : \mathbb{Q}] = 3$, as proved by Colliot-Thélène and Salberger in [32]. Both of these results make use of fibration and descent methods.

In the case when $f$ is an irreducible quadratic and $K$ is a quartic extension containing a root of $f$, the Hasse principle and weak approximation are known to hold for (8.1.1) thanks to the work of Browning and Heath-Brown [14]. This result was generalised by Derenthal, Smeets and Wei in [44, Theorem 2], to prove that the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation for irreducible quadratics $f$ and arbitrary number fields $K$. Moreover, in [44, Theorem 4] they give an explicit description of the Brauer groups that can be obtained in this family.

Results when $f$ is not irreducible have so far been limited to products of linear polynomials. Suppose that $f$ takes the form

$$f(t) = c\prod_{i=1}^{r}(t - e_i)^{m_i}, \tag{8.1.2}$$

for some $c \in \mathbb{Q}^*, e_1, \dots, e_r \in \mathbb{Q}$ and $m_1, \dots, m_r \in \mathbb{N}$. When $r = 1$, the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation for any smooth projective model of (8.1.1). This is a special case of the work of Colliot-Thélène and Sansuc [33] on principal homogeneous spaces under algebraic tori. Heath-Brown and Skorobogatov [65] treat the case $r = 2$ by combining descent methods with the Hardy–Littlewood circle method, under the assumption that $\gcd(m_1, m_2, \deg K) = 1$. This assumption was later removed by Colliot-Thélène, Harari and Skorobogatov [36]. Thanks to the work of Browning and Matthiesen [19], it is now settled that for any number field $K$ and and polynomial $f$ of the form (8.1.2) (for arbitrary $r \geqslant 1$), the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation for any smooth projective model of (8.1.1). Their result is inspired by additive combinatorics results of Green, Tao and Ziegler [54], [55], combined with "vertical" torsors introduced by Schindler and Skorobogatov [102].

In general, it has been conjectured by Colliot-Thélène [31] that all failures of the Hasse principle for any smooth projective model of (8.1.1) are explained by

the Brauer–Manin obstruction. Assuming Schinzel's hypothesis, this holds true for $f$ an arbitrary polynomial and $K/\mathbb{Q}$ a cyclic extension, as demonstrated by work of Colliot-Thélène and Swinnerton-Dyer on pencils of Severi–Brauer varieties [38]. Recently, Skorobogatov and Sofos also establish unconditionally that when $K/\mathbb{Q}$ is cyclic, (8.1.1) satisfies the Hasse principle for a positive proportion of polynomials $f$ of degree $d$, when their coefficients are ordered by height [110, Theorem 1.3].

In [69], Irving introduces an entirely new approach to studying the Hasse principle for (8.1.1), which rests on sieve methods. Irving's main result [69, Theorem 1.1] states that if $f \in \mathbb{Z}[t]$ is an irreducible cubic, then the Hasse principle holds for (8.1.1) under the following assumptions:

1. $K$ satisfies the Hasse norm principle.
2. There exists a prime $q \geqslant 7$, and a finite set of primes $S$, such that for all $p \notin S$, either $p \equiv 1 \pmod{q}$ or the inertia degrees of $p$ in $K/\mathbb{Q}$ are coprime.
3. The number field generated by $f$ is not contained in the cyclotomic field $\mathbb{Q}(\zeta_q)$.

An example provided by Irving in [69] is the number field $\mathbb{Q}(\alpha)$, where $\alpha$ is a root of $x^q - 2$ and $q \geqslant 7$ is prime. We shall comment on this further in Example 8.3.5.

In this chapter, we generalize Irving's arguments to establish the Hasse principle for a wide new family of polynomials and number fields. Our results cover for the first time polynomials of arbitrarily large degree which are not a product of linear factors. In fact, under suitable assumptions on $K$, we can deal with polynomials that are products of arbitrarily many linear, quadratic and cubic factors.

Throughout this chapter, we let $\widehat{K}$ denote the Galois closure of $K$, and we let $G = \mathrm{Gal}(\widehat{K}/\mathbb{Q})$, viewed as a permutation group on $n$ letters. We define

$$T(G) = \frac{1}{\#G}\#\{\sigma \in G : \text{ the cycle lengths of } \sigma \text{ are not coprime}\}. \quad (8.1.3)$$

We now state our main results. The following theorems are slight generalisations of Theorems A and C from the Introduction.

**Theorem 8.1.1.** *Let $K$ be a number field satisfying the Hasse norm principle. Let $f \in \mathbb{Z}[t]$ be a polynomial, all of whose irreducible factors have degree at most 2. Let $k$ denote the number of distinct irreducible factors of $f$, and let $j$ denote the number of distinct irreducible quadratic factors of $f$ which generate a quadratic field contained in $\widehat{K}$. Suppose that $T(G) < \frac{0.39006\ldots}{k+j+1}$. Then the Hasse principle holds for (8.1.1).*

In practice, the constant $0.39006...$ can be improved slightly, particularly when the majority of the factors of $f$ are linear, although it will always be less than $1/2$. The precise optimal constant is obtained by finding the maximal value of $\kappa$ such that (8.2.51) holds.

Our second main result allows $f$ to contain irreducible cubic factors, but requires more restrictive assumptions on the number field $K$, more similar to Irving's setup in [69].

**Theorem 8.1.2.** *Let $f \in \mathbb{Z}[t]$ be a polynomial, all of whose irreducible factors have degree at most $3$. Then the Hasse principle holds for (8.1.1) under the following assumptions for $K$.*

1. *$K$ satisfies the Hasse norm principle.*
2. *There exists a prime $q \geqslant (4.08825...) \deg f + 1$, such that for all but finitely many primes $p \not\equiv 1 \pmod{q}$, the inertia degrees of $p$ in $K/\mathbb{Q}$ are coprime.*

The constant $4.08825...$ could likely be improved with more work, and in specific examples, the required bound on $q$ could be computed more precisely using (8.2.55). We remark that we have also dropped the assumption made in [69] that the number field generated by $f$ is not contained in $\mathbb{Q}(\zeta_q)$. This assumption is not essential to Irving's argument, but allows for the treatment of smaller values of $q$. Reinserting this assumption and optimising (8.2.55), we could recover Irving's result from our work.

We recall from the Introduction that Theorem A has the following corollary, which is a restatement of Corollary B, included for convenience.

**Corollary 8.1.3.** *Let $f \in \mathbb{Z}[t]$ be a product of two non-proportional irreducible quadratic polynomials. Let $K$ be a number field of degree $n$ with $G = S_n$. Let $L$ be the biquadratic number field generated by $f$. Suppose that $L \cap \widehat{K} = \mathbb{Q}$. Then the Hasse principle holds for (8.1.1), provided that*

$$n \notin \{2, 3, \dots, 10, 12, 14, 15, 16, 18, 20, 22, 24, 26, 28, 30, 36, 42, 48\}.$$

We remark that without the assumption $L \cap \widehat{K} = \mathbb{Q}$, a similar result to Corollary 8.1.3 still holds, although a larger list of degrees $n$ would need to be excluded. For example, if $L \cap \widehat{K}$ is quadratic, then the Hasse principle holds for (8.1.1) for all primes $n \geqslant 11$ and all integers $n > 90$, whilst if $L \cap \widehat{K} = L$, then the Hasse prinicple holds for all primes $n \geqslant 13$ and all integers $n > 150$.

We cannot hope to deal with all small values of $n$ in Corollary 8.1.3. For example, the work of Iskovskikh [70] shows that the Hasse principle can fail when $n = 2$ (see Example 8.3.4). However, as we shall discuss in the Appendix,

in the case $n \geqslant 3$, there is no Brauer–Manin obstruction to the Hasse principle, and so according to the conjecture of Colliot-Thélène mentioned above we should expect the Hasse principle to hold.

In Section 8.4, we find a second application of Theorem 5.7.1 to a conjecture of Harpaz and Wittenberg [57, Conjecture 9.1], which we restate in Conjecture 8.4.1 and henceforth refer to as the *Harpaz–Wittenberg conjecture*. The conjecture concerns a collection of number field extensions $L_i/k_i/k$, $i \in \{1, \dots, n\}$, where $k_i \cong k[t]/(P_i(t))$ for monic irreducible polynomials $P_i \in k[t]$. Roughly speaking, the conjecture predicts, under certain hypotheses, the existence of an element $t_0 \in k$ such that $P_1(t_0), \dots, P_n(t_0)$ are locally split, i.e., each place in $k_i$ dividing $P_i(t_0)$, has a degree $1$ place of $L_i$ above it.

A major motivation for the conjecture is the development of the theory of rational points in fibrations. Given a fibration $\pi : X \to \mathbb{P}^1_k$, a natural question is to what extent we can deduce arithmetic information about $X$ from arithmetic information about the fibres of $\pi$. A famous conjecture of Colliot-Thélène [31, p.174] predicts that for any smooth, proper, geometrically irreducible, rationally connected variety $X$ over a number field $k$, the rational points $X(k)$ are dense in the Brauer–Manin set $X(\mathbb{A}_k)^{\mathrm{Br}}$. (In other words, the Brauer–Manin obstruction is the only obstruction to weak approximation.) Applied to this conjecture, the above question becomes whether density of $X(k)$ in $X(\mathbb{A}_k)^{\mathrm{Br}}$ follows from density of $X_c(k)$ in $X_c(\mathbb{A}_k)^{\mathrm{Br}}$ for a general fibre $X_c := \pi^{-1}(c)$ of $\pi$ (see [58, Question 1.2]). Applications of the Harpaz–Wittenberg conjecture to this question are studied in [57] and [58].

Harpaz and Wittenberg [57, Section 9.2] demonstrate that their conjecture follows from the homogeneous version of Schinzel's hypothesis (commonly reffered to as $(\mathrm{HH}_1)$) in the case of abelian extensions $L_i/k_i$, or more generally, almost abelian extensions (see [57, Definition 9.4]). Examples of almost abelian extensions include cubic extensions, and extensions of the form $k(c^{1/p})/k$ for $c \in k$ and $p$ prime. The work of Heath-Brown and Moroz [63] establishes $(\mathrm{HH}_1)$ for primes represented by binary cubic forms, from which the Harpaz–Wittenberg conjecture can be deduced in the case $k = \mathbb{Q}, n = 1$ and $\deg P_1 = 3$. Using a geometric reformulation of [57, Conjecture 9.1], the authors establish their conjecture in low degree cases, namely when $\sum_{i=1}^n [k_i : k] \leqslant 2$ or $\sum_{i=1}^n [k_i : k] = 3$ and $[L_i : k_i] = 2$ for all $i$.

The Harpaz–Wittenberg conjecture is related to the study of polynomials represented by norm forms. As a consequence of the work of Matthiesen [85] on norms as products of linear polynomials, the Harpaz–Wittenberg conjecture holds in the case $k_1 = \cdots = k_n = k = \mathbb{Q}$ [57, Theorem 9.14]. Similarly, we can deduce from [69, Theorem 1.1] that the Harpaz–Wittenberg conjecture holds in the case $n = 2, k = \mathbb{Q}, k_1 = K, k_2 = \mathbb{Q}, L_1 = K(2^{1/q})$ and $L_2 = \mathbb{Q}(2^{1/q})$, where $q \geqslant 7$ is a prime such that $K \not\subseteq \mathbb{Q}(\zeta_q)$ [57, Theorem 9.15].

Besides the work of Matthiesen [85] for $k_1 = \cdots = k_n = k = \mathbb{Q}$, the aforementioned results apply only to the case $n \leqslant 2$. In Section 8.4, we prove the following theorem, which establishes the Harpaz–Wittenberg conjecture in a new family of extensions $k_1/\mathbb{Q}, \ldots, k_n/\mathbb{Q}$, where $n$ may be arbitrarily large, and each extension $k_i/\mathbb{Q}$ may have degree up to 3.

**Theorem 8.1.4.** *Let $n \geqslant 1$. Let $k = \mathbb{Q}$, and for $i \in \{1, \ldots, n\}$, let $k_i, M_i$ be number fields with $k_i \cap M_i = \mathbb{Q}$. Let $L_i = M_i k_i$ be the compositum of $k_i$ and $M_i$. Define*

$$T_i = \frac{1}{\#Gal(\widehat{M_i}/\mathbb{Q})} \#\{\sigma \in Gal(\widehat{M_i}/\mathbb{Q}) : \sigma \text{ has no fixed point}\}. \quad (8.1.4)$$

*Let $d = \sum_{i=1}^{n} [k_i : \mathbb{Q}]$. Then the Harpaz–Wittenberg conjecture holds in the following cases.*

1. *$[k_i : \mathbb{Q}] \leqslant 2$ for all $i \in \{1, \ldots, n\}$ and $\sum_{i=1}^{n} T_i < 0.39006.../d$.*
2. *$[k_i : \mathbb{Q}] \leqslant 3$ for all $i \in \{1, \ldots, n\}$, and there exist primes $q_i$ satisfying $\sum_{i=1}^{n} 1/(q_i - 1) < 0.28371.../d$, and such that for all but finitely many primes $p \not\equiv 1 \pmod{q_i}$, there is a place of degree 1 in $M_i$ above $p$.*

**Corollary 8.1.5.** *Let $q_1, \ldots, q_n$ be distinct primes, and let $r_1, \ldots, r_n \in \mathbb{N}$ be such that $g_i(x) = x^{q_i} - r_i$ is irreducible for all $i$. Let $M_i = \mathbb{Q}[x]/(g_i)$ and let $k_i, L_i$ and $d$ be as in Theorem 8.1.4. Suppose that one of the following holds:*

1. *$[k_i : \mathbb{Q}] \leqslant 2$ for all $i \in \{1, \ldots, n\}$ and $\sum_{i=1}^{n} 1/q_i < 0.39006.../d$,*
2. *$[k_i : \mathbb{Q}] \leqslant 3$ for all $i \in \{1, \ldots, n\}$ and $\sum_{i=1}^{n} 1/(q_i - 1) < 0.28371.../d$.*

*Then the Harpaz–Wittenberg conjecture holds for $k = \mathbb{Q}$ and for such choices of $k_i$ and $L_i$.*

We remark that when applied to the setting of [57, Theorem 9.15], the above result requires a stronger bound on $q$. However, with a more careful optimisation of (8.2.54), it should be possible to recover [57, Theorem 9.15] from our approach.

By combining Theorem 8.1.4 with [57, Theorem 9.17] (with the choice $B = 0, M'' = \emptyset$ and $M' = \mathbb{P}^1_k \backslash U$), we obtain the following result about rational points in fibrations.

**Theorem 8.1.6.** *Let $X$ be a smooth, proper, geometrically irreducible variety over $\mathbb{Q}$. Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a dominant morphism whose general fibre is rationally connected. Let $k_1, \ldots, k_n$ denote the residue fields of the closed points of $\mathbb{P}^1_{\mathbb{Q}}$ above which $\pi$ has nonsplit fibres, and let $L_i/k_i$ be finite extensions which split these nonsplit fibres. Assume that*

1. *The smooth fibres of $\pi$ satisfy the Hasse principle and weak approximation.*
2. *The hypotheses of Theorem 8.1.4 hold.*

*Then $X(\mathbb{Q})$ is dense in $X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X)}$.*

It would be interesting to investigate whether Condition $(1)$ in Theorem 8.1.6 could be relaxed to the assumption that the smooth fibres $X_c(\mathbb{Q})$ are dense in $X_c(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X_c)}$, as in the setting of [58, Question 1.2] discussed above. This would require an extension of Theorem 8.1.4 to cover a stronger version of the Harpaz–Wittenberg conjecture, involving strong approximation of an auxiliary variety $W$ off a finite set of places [58, Proposition 6.1]. Strong approximation of $W$ was studied by Browning and Schindler [21] for example, who established [58, Question 1.2] in the case when the rank of $\pi$ is at most $3$, and at least one of its nonsplit fibres lies above a rational of $\mathbb{P}^1_{\mathbb{Q}}$.

**Acknowledgements.** I am grateful to Jean-Louis Colliot-Thélène for providing the statements and proofs in the Appendix, and to Julian Lyczak and Alexei Skorobogatov for helpful discussions on Brauer groups. I would also like to thank Olivier Wittenberg for many useful comments on the Harpaz–Wittenberg conjecture.

## 8.2 Application of the beta sieve

In this section, we prove Theorem 5.7.1 and Theorem 5.7.2 by combining the level of distribution results from Section 5.9 with the beta sieve of Rosser and Iwaniec, as stated in Theorem 5.6.1.

We recall some of the notation from Section 5.7. We fix a region $\mathscr{R} = \mathscr{B}N$ for some $\mathscr{B} \subseteq [-1,1]^2$ of volume $\gg 1$ and with a piecewise smooth boundary of perimeter $\ll 1$. Then $\mathscr{R}$ has volume $\gg N^2$ and perimeter $\ll N$. Let $d$ denote the largest degree among the irreducible factors of $f$. (We specialise to the cases $d = 2$ and $d = 3$ later. The reason our methods are unable to deal with larger values of $d$ is explained in Remark 8.2.3.) Then there exists $x \ll N^d$ such that the largest prime factor of $f(a,b)$ for $(a,b) \in \mathscr{R} \cap \mathbb{Z}^2$ is bounded by $x$. Let $S$ be a finite set of primes, including all primes dividing the discriminant of $f(x,y)$. In Section 8.2.5, we also append to $S$ all primes bounded by some constant $P_1$. We assume throughout this section that $\mathscr{P}$ is a set of primes disjoint from $S$ and satisfying (5.7.6) and (5.7.7). We also define $\mathscr{P}'$ to be the set of primes not in $\mathscr{P} \cup S$. Let $P(x)$ denote the product of primes in $\mathscr{P}_{<x}$, and similarly for $P'(x)$.

Let $\mathscr{A} = (a_n)$ be the sequence given by

$$a_n = \#\{(a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : C(a,b), f(a,b) = n\}.$$

We define a sifting function

$$\begin{aligned} S(\mathscr{A}, \mathscr{P}, x) &= \sum_{\gcd(n, P(x))=1} a_n \\ &= \#\{(a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : C(a,b), \gcd(f(a,b), P(x)) = 1\}. \end{aligned} \tag{8.2.1}$$

Our aim is to prove that $S(\mathscr{A}, \mathscr{P}, x) > 0$ for sufficiently large $N$. We recall from (5.7.3) that we have a decomposition

$$f(x,y) = \prod_{i=0}^{m} f_i(x,y) \prod_{i=m+1}^{k} f_i(x,y) \tag{8.2.2}$$

of $f$ into a product of irreducible binary forms, where $f_i$ are linear for $i \leqslant m$ and degree at least two for $i > m$. For a prime $p \in \mathscr{P}$ and for any $i \in \{0, \dots, k\}$, we additionally define

$$S(\mathscr{A}_p, \mathscr{P}, p) = \# \left\{ (a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : \begin{array}{l} C(a,b),\, p \mid f(a,b) \\ \gcd(f(a,b), P(p)) = 1 \end{array} \right\},$$

$$S(\mathscr{A}_p^{(i)}, \mathscr{P}, p) = \# \left\{ (a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : \begin{array}{l} C(a,b),\, p \mid f_i(a,b) \\ \gcd(f(a,b), P(p)) = 1 \end{array} \right\}.$$

Using the Buchstab identity, we have

$$S(\mathscr{A}, \mathscr{P}, x) = S(\mathscr{A}, \mathscr{P}, N^\gamma) - \sum_{\substack{N^\gamma < p \leqslant x \\ p \in \mathscr{P}}} S(\mathscr{A}_p, \mathscr{P}, p),$$

for a parameter $\gamma \in (0,1)$ to be chosen later. We denote the quantity $S(\mathscr{A}, \mathscr{P}, N^\gamma)$ by $S_1$. If $p \mid f(a,b)$ then $p \mid f_i(a,b)$ for some $i$. Therefore, we have the decomposition

$$S(\mathscr{A}, \mathscr{P}, x) \leqslant S_1 - \sum_{i=0}^{m} S_2^{(i)} - \sum_{i=m+1}^{k} \left( S_3^{(i)} + S_4^{(i)} \right),$$

where

$$\begin{aligned} S_2^{(i)} &= \sum_{\substack{N^\gamma < p \leqslant N \\ p \in \mathscr{P}}} S(\mathscr{A}_p^{(i)}, \mathscr{P}, p), \\ S_3^{(i)} &= \sum_{\substack{N^\gamma < p \leqslant N^{\beta_i} \\ p \in \mathscr{P}}} S(\mathscr{A}_p^{(i)}, \mathscr{P}, p), \\ S_4^{(i)} &= \sum_{\substack{N^{\beta_i} < p \leqslant x \\ p \in \mathscr{P}}} S(\mathscr{A}_p^{(i)}, \mathscr{P}, p), \end{aligned} \tag{8.2.3}$$

for parameters $\beta_i \geqslant \gamma$ to be chosen later.

For $i \in \{0, \dots, k\}$, we define multiplicative functions

$$\begin{aligned}\varrho_i(d_1, d_2) &= \#\{a, b \pmod{d_1 d_2} : d_1 \mid f_i(a,b), d_2 \mid f(a,b)\},\\ \varrho_i(d) &= \#\{a, b \pmod{d} : f_i(a,b) \equiv 0 \pmod{d}\},\\ \varrho(d) &= \#\{a, b \pmod{d} : f(a,b) \equiv 0 \pmod{d}\}.\end{aligned}$$

We note that the function $\varrho_i(d_1, d_2)$ is the same as the function $\varrho(d_1, d_2)$ from (5.9.2) with $g_1(x,y) = f_i(x,y)$ and $g_2(x,y) = f(x,y)$, but in this section, we add a subscript to keep track of the dependence on $i$.

When $\gcd(d_1, d_2) = 1$, we have $\varrho_i(d_1, d_2) = \varrho_i(d_1)\varrho(d_2)$. Moreover, for any $i \in \{1, \dots, k\}$ and any prime $p \notin S$, we have

$$\varrho_i(p) = \nu_i(p)(p-1) + 1, \tag{8.2.4}$$

$$\varrho(p) = \nu(p)(p-1) + 1, \tag{8.2.5}$$

where $\nu_i(p)$ and $\nu(p)$ are as defined in (5.7.4) and (5.7.5).

### 8.2.1 Sieve dimensions

The sieve dimension, as introduced in Section 5.5, plays a crucial role in the analysis of the beta sieve. The sieve dimensions which we shall use are governed by Lemma 8.2.1 below, and are

$$\kappa := \alpha\theta, \qquad \kappa_i := 1 - \alpha\theta_i,$$

for $\alpha, \theta_i$ and $\theta$ as defined in (5.7.6), (5.7.7) and (5.7.8). For convenience, we recall that (5.7.6), (5.7.7) and (5.7.8) are the estimates

$$\sum_{p \in \mathscr{P}_{\leqslant x}} 1 = \alpha\pi(x)\left(1 + O_A\left((\log x)^{-A}\right)\right), \tag{8.2.6}$$

$$\sum_{p \in \mathscr{P}_{\leqslant x}} \nu_i(p) = \alpha\theta_i\pi(x)\left(1 + O_A\left((\log x)^{-A}\right)\right). \tag{8.2.7}$$

$$\sum_{p \in \mathscr{P}_{\leqslant x}} \nu(p) = \alpha\theta\pi(x)\left(1 + O_A\left((\log x)^{-A}\right)\right), \tag{8.2.8}$$

We assume throughout this section that $\kappa < 1/2$, and so $\kappa_i > 1/2$. We denote the upper and lower bound sieve constants of dimension $\kappa$ by $A, B$ respectively, and the upper bound sieve constant for dimension $\kappa_i$ by $A_i$. We recall from Section 5.6 that in all applications of the main theorem of the beta sieve (Theorem 5.6.1), we shall have $f(s) = B$ and $F(s) = A$ or $F(s) = A_i$.

Moreover, $A$ and $B$ are defined in [52, Equations (11.62), (11.63)], and $A_i$ is defined in [52, Equations (11.44), (11.57)]. A table of numerical values of these constants can be found in [52, Section 11.19].

When applying the beta sieve, we use the multiplicative functions

$$g(p) = \begin{cases} \frac{\varrho(p)}{p^2}, & \text{if } p \in \mathscr{P}, \\ 0, & \text{otherwise}, \end{cases} \qquad g_i(p) = \begin{cases} \frac{\varrho_i(p)}{p^2}, & \text{if } p \in \mathscr{P}', \\ 0, & \text{otherwise}, \end{cases} \tag{8.2.9}$$

and the functions

$$V(x) = \prod_{p \in \mathscr{P}_{\leqslant z}} \left(1 - \frac{\varrho(p)}{p^2}\right), \qquad V_i(x) = \prod_{p \in \mathscr{P}'_{\leqslant z}} \left(1 - \frac{\varrho_i(p)}{p^2}\right) \tag{8.2.10}$$

for $i \in \{1, \dots, k\}$.

**Lemma 8.2.1.** *Let $x \geqslant 1$. For $i \in \{1, \dots, k\}$, and $V, V_i$ as in (8.2.10), there exist constants $c, c_i > 0$ such that*

$$V(x) = \frac{c}{(\log x)^{\kappa}} \left(1 + O((\log x)^{-1})\right), \tag{8.2.11}$$

$$V_i(x) = \frac{c_i}{(\log x)^{\kappa_i}} \left(1 + O((\log x)^{-1})\right). \tag{8.2.12}$$

*The asymptotic in (8.2.12) also holds for $i = 0$ when $f_0 \not\equiv 1$. In particular, the hypothesis (5.6.1) of the main theorem of the beta sieve holds for $g$ and $g_i$.*

*Proof.* We follow a similar approach to the proof of Corollary 5.5.5 (see also [69, Lemma 4.2]). Below, we denote by $C$ a constant which is allowed to vary from line to line. We have

$$\log V(x) = -\sum_{p \in \mathscr{P}_{\leqslant x}} \left(\sum_{m=1}^{\infty} \frac{\varrho(p)^m}{m p^{2m}}\right) \tag{8.2.13}$$

$$= -\sum_{p \in \mathscr{P}_{\leqslant x}} \frac{\nu(p)(p-1)+1}{p^2} + C + O((\log x)^{-1}). \tag{8.2.14}$$

$$= -\sum_{p \in \mathscr{P}_{\leqslant x}} \frac{\nu(p)}{p} + C + O((\log x)^{-1}), \tag{8.2.15}$$

where in (8.2.15) we have used that $\nu(p) \leqslant \deg f$ for all but finitely many primes $p$. To estimate the sum in (8.2.15), we apply partial summation, together with our assumption (5.7.8). For $t \geqslant 2$, we define

$$A_t = \sum_{p \in \mathscr{P}_{\leqslant t}} \nu(p). \tag{8.2.16}$$

Then

$$\begin{aligned}\sum_{p\in\mathscr{P}_{\leqslant x}}\frac{\nu(p)}{p} &= \frac{A_x}{x}+\int_2^x\frac{A_t}{t^2}\mathrm{d}t\\ &= \kappa\int_2^x\frac{\pi(t)\left(1+O\left((\log x)^{-1}\right)\right)}{t^2}\mathrm{d}t+O((\log x)^{-1})\\ &= \kappa\int_2^x\frac{\mathrm{d}t}{t\log t}+C+O((\log x)^{-1})\\ &= \kappa\log\log x+C+O((\log x)^{-1}).\end{aligned}\tag{8.2.17}$$

We deduce (8.2.11) by taking the exponential of (8.2.17).

We can prove (8.2.12) in a similar way. When $i=0$ and $f_0\not\equiv 1$, we have $\varrho_0(p)=p$, and so the result is a consequence of Mertens' theorem. For any $i\in\{1,\dots,k\}$, we have

$$\begin{aligned}\log V_i(x) &= \sum_{p\in\mathscr{P}'_{\leqslant x}}\frac{\nu_i(p)}{p}+C+O((\log x)^{-1})\\ &= \sum_{p\leqslant x\text{ prime}}\frac{\nu_i(p)}{p}-\sum_{p\in\mathscr{P}_{\leqslant x}}\frac{\nu_i(p)}{p}+C+O((\log x)^{-1}).\end{aligned}\tag{8.2.18}$$

Similarly to above, using partial summation and (5.7.7), we have

$$\sum_{p\in\mathscr{P}_{\leqslant x}}\frac{\nu_i(p)}{p}=\alpha\theta_i\log\log x+C+O((\log x)^{-1}).\tag{8.2.19}$$

To treat the first sum in (8.2.18), we define $L$ to be the number field generated by $f_i$. For all but finitely many primes $p$, the quantity $\nu(p)$ is equal to the number of prime ideals $\mathfrak{p}$ in $L$ above $p$, and so

$$\sum_{p\leqslant x\text{ prime}}\nu(p)=\pi_L(x)+C,$$

where $\pi_L(x)$ denotes the number of prime ideals in $L$ of norm at most $x$. Using partial summation, as above, together with the Prime ideal theorem [88], we deduce that

$$\sum_{p\leqslant x\text{ prime}}\frac{\nu_i(p)}{p}=\log\log x+C+O((\log x)^{-1}).\tag{8.2.20}$$

Combining this with (8.2.19) and taking exponentials, we deduce the asymptotic in (8.2.12). □

In the following lemma, we record three more useful estimates following similar arguments to Lemma 8.2.1.

**Lemma 8.2.2.** *There exists constants $C, C_i > 0$ such that*

$$\sum_{p\in\mathscr{P}_{\leqslant x}} \frac{\varrho_i(p)}{p^2} = (1-\kappa_i)\log\log x + C + O((\log x)^{-1}), \tag{8.2.21}$$

$$\sum_{p\in\mathscr{P}'_{\leqslant x}} \frac{\varrho_i(p)}{p^2} = \kappa_i \log\log x + C_i + O((\log x)^{-1}), \tag{8.2.22}$$

$$\sum_{p\in\mathscr{P}'_{\leqslant x}} \frac{\varrho_i(p)}{p^2}\log p = \kappa_i \log x + O(1). \tag{8.2.23}$$

*Proof.* The estimates (8.2.21) and (8.2.22) are immediate consequences of (8.2.17), (8.2.19) and (8.2.20), together with fact that

$$\frac{\varrho_i(p)}{p^2} = \frac{(p-1)\nu_i(p)+1}{p^2} = \frac{\nu_i(p)}{p} + O(p^{-2}).$$

To prove (8.2.23), we proceed via partial summation in a very similar manner to (8.2.17). We recall from the prime number theorem that

$$\pi(t) = \frac{t}{\log t} + \frac{t}{(\log t)^2} + O\left(\frac{t}{(\log t)^3}\right). \tag{8.2.24}$$

For $A_t$ as defined in (8.2.16), we have

$$\begin{aligned}
\sum_{p\in\mathscr{P}'_{\leqslant x}} \frac{\varrho_i(p)}{p^2}\log p &= \sum_{p\in\mathscr{P}'_{\leqslant x}} \frac{\nu_i(p)}{p}\log p + O(1)\\
&= \frac{A_x \log x}{x} - \int_2^x A_t \left(\frac{\log t}{t}\right)' \mathrm{d}t + O(1)\\
&= \kappa_i \int_2^x \frac{(\log t - 1)\pi(t)(1+O((\log t)^{-A})}{t^2}\mathrm{d}t + O(1)\\
&= \kappa_i \int_2^x \frac{1}{t} + O\left(\frac{1}{t(\log t)^2}\right)\mathrm{d}t + O(1) \quad \text{(from (8.2.24))}\\
&= \kappa_i \log x + O(1),
\end{aligned}$$

as required. □

## 8.2.2 The sum $S_1$

We apply the lower bound sieve of level $N^\gamma$, and the level of distribution result from Corollary 5.9.2 with $g_1(x,y) = 1, g_2(x,y) = f(x,y), D_1 = 1$ and $D_2 = N^\gamma$. The hypotheses of Corollary 5.9.2 require that $\gamma < 1$. Recalling the notation $V(z)$ from (8.2.10), we obtain

$$S_1 \geqslant \frac{(B+o(1))\operatorname{Vol}(\mathscr{R})V(N^\gamma)}{\Delta^2}. \tag{8.2.25}$$

By Lemma 8.2.1, we have

$$V(N^\gamma) \sim \frac{c}{(\log N^\gamma)^\kappa}.$$

For any $\epsilon > 0$, taking $\gamma$ sufficiently close to 1, we obtain

$$S_1 \geqslant \frac{(cB - \epsilon + o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2 (\log N)^\kappa}. \tag{8.2.26}$$

### 8.2.3 The sums $S_2^{(i)}$

We write $f_i(a,b) = pr$, for $p \in \mathscr{P}$ and $N^\gamma < p \leqslant N$. We apply the *switching principle*, which transforms the sum over $p$ defining $S_2^{(i)}$ into a much shorter sum over the variable $r$.

Let $R = N^{1-\gamma}$. The sums $S_2^{(i)}$ only involve linear factors $f_i(x,y)$, since we assume $i \in \{0,\dots,m\}$. Therefore, for $(a,b) \in \mathscr{R} \cap \mathbb{Z}^2$ we have $f_i(a,b) \ll N$, and so $|r| \leqslant R$. Let $z = N^{1/3}$. We shall take $\gamma$ arbitrarily close to 1; for now, we assume that $\gamma > 2/3$. Then by definition of $S(\mathscr{A}_p^{(i)}, \mathscr{P}, p)$, we know that $\gcd(r, P(R)) = 1$ and $\gcd(f(a,b), P(z)) = 1$. We replace the condition $p \in \mathscr{P}$ by the weaker condition $\gcd(p, \mathscr{P}'(z)) = 1$.

Let $r' = |r|/\gcd(r, \Delta)$. Then

$$S_2^{(i)} \leqslant \sum_{\substack{r' \leqslant R \\ \gcd(r', P(R)\Delta) = 1}} S_2^{(i)}(r'),$$

where

$$S_2^{(i)}(r') = \#\left\{ (a,b) \in \mathscr{R} \cap \mathbb{Z}^2 : \begin{array}{l} C(a,b), r' \mid f_i(a,b), \\ \gcd(f_i(a,b)/r, P'(z)) = 1 \\ \gcd(f(a,b), P(z)) = 1 \end{array} \right\}.$$

The prime factors of $\Delta$ are contained in $S$, which is disjoint from $\mathscr{P}$, so $\gcd(f_i(a,b)/r, \mathscr{P}'(z)) = \gcd(f_i(a,b)/r', \mathscr{P}'(z))$. Below, for convenience, we change notation from $r'$ back to $r$.

Let $\mu_1^+, \mu_2^+$ be upper bound beta sieves of level $D = N^{1/3}$. Then

$$S_2^{(i)}(r) \leqslant \sum_{\substack{d \mid P'(z) \\ \gcd(d,r)=1}} \sum_{e \mid P(z)} \mu_1^+(d)\mu_2^+(e) R(dr, e),$$

where $R(dr,e)$ is as in Section 5.9 with $g_1(x,y) = f_i(x,y)$ and $g_2(x,y) = f(x,y)$. Define a multiplicative function $h_i(r)$ which is zero unless all the prime factors of $r$ are in $\mathscr{P}'$, and

$$h_i(r) = \frac{\varrho_i(r)}{r^2} \prod_{p \mid r} \left(1 - \frac{\varrho_i(p)}{p^2}\right)^{-1} \tag{8.2.27}$$

otherwise. Since $\gamma > 2/3$, Lemma 5.9.5 applies, with $D_1 = DR = N^{4/3-\gamma}$ and $D_2 = D = N^{1/3}$. From Lemma 8.2.1, we obtain

$$\begin{aligned} S_2^{(i)} &\leqslant \sum_{r\leqslant R} \frac{(AA_i + o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2} h_i(r) V(N^{1/3}) V_i(N^{1/3}) \\ &\leqslant \frac{(cc_i AA_i + o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2 (\log N^{1/3})^{\kappa+\kappa_i}} \sum_{r\leqslant R} h_i(r). \end{aligned} \tag{8.2.28}$$

To deal with the sum over $h_i(r)$, we note that

$$\sum_{r\leqslant R} h_i(r) \leqslant \prod_{\substack{p\in\mathscr{P}' \\ p\leqslant R}} \left(1 + \sum_{m=1}^{\infty} h_i(p^m)\right) = \prod_{\substack{p\in\mathscr{P}' \\ p\leqslant R}} \left(1 - \frac{\varrho_i(p)}{p^2}\right)^{-1} (1 + O(p^{-2})). \tag{8.2.29}$$

Applying Lemma 8.2.1 to the product, we obtain

$$\sum_{r\leqslant R} h_i(r) \ll (\log R)^{\kappa_i}.$$

Since $R = N^{1-\gamma}$, we deduce that

$$S_2^{(i)} \ll \frac{cc_i AA_i \operatorname{Vol}(\mathscr{R})}{\Delta^2 (\log N)^{\kappa}} \left(\frac{(1-\gamma)^{\kappa_i}}{(1/3)^{\kappa_i+\kappa}}\right).$$

Therefore, $S_2^{(i)}$ can be made negligible compared to $S_1$ by taking $\gamma$ arbitrarily close to 1.

### 8.2.4 The sums $S_3^{(i)}$

We first deal with the primes $p$ in the interval $I := (N^{\gamma}, N^{2-\gamma-\epsilon}]$. For any $p \in I$, the upper bound beta sieve of level $D_2$ yields

$$\begin{aligned} S(\mathscr{A}_p^{(i)}, \mathscr{P}, p) &\leqslant S(\mathscr{A}_p^{(i)}, \mathscr{P}, N^{\gamma}) \\ &\leqslant \frac{(A + o(1))\operatorname{Vol}(\mathscr{R}) V(D_2)}{\Delta^2} \left(\frac{\varrho_i(p)}{p^2}\right) + R^+(p, D_2), \end{aligned} \tag{8.2.30}$$

where

$$R^+(p, D_2) = \sum_{\substack{d\leqslant D_2 \\ \gcd(d, p\Delta)=1}} \left| R(p, d) - \frac{\varrho_i(p, d)\operatorname{Vol}(\mathscr{R})}{p^2 d^2 \Delta^2} \right|. \tag{8.2.31}$$

We apply Corollary 5.9.2 with $g_1(x, y) = f_i(x, y), g_2(x, y) = f(x, y), D_1 = N^{2-\gamma-\epsilon}$ and $D_2 = N^{\gamma}$. These choices of $D_1, D_2$ satisfy the hypotheses of

Corollary 5.9.2. Taking a sum over $p \in I$, the contribution from the term $R^+(p, D_2)$ in (8.2.30) is negligible. We obtain

$$\sum_{\substack{p\in I\\ p\in\mathscr{P}}} S(\mathscr{A}_p^{(i)}, \mathscr{P}, p) \leqslant \frac{(A+o(1))\operatorname{Vol}(\mathscr{R})V(N^\gamma)}{\Delta^2} \sum_{\substack{p\in I\\ p\in\mathscr{P}}} \frac{\varrho_i(p)}{p^2}. \tag{8.2.32}$$

It follows from Lemma 8.2.2 that

$$\begin{aligned}\sum_{N^\gamma<p\ll N^{2-\gamma-\epsilon}} \frac{\varrho_i(p)}{p^2} &= \log\log N^{2-\gamma-\epsilon} - \log\log N^\gamma + o(1)\\ &= \log(2-\gamma-\epsilon) - \log\gamma + o(1).\end{aligned}$$

Therefore, the contribution to $S_3^{(i)}$ from this range is negligible if we take $\gamma$ arbitrarily close to 1.

In the remaining range $N^{2-\gamma-\epsilon} < p \leqslant N^{\beta_i}$, we split into dyadic intervals $(R, 2R]$. For each dyadic interval, we apply a similar argument to above, but with $D_1 = 2R$ and $D_2 = N^{2-\epsilon}/R$. At this point we need to assume that $\beta_i < 2$ for all $i$, so that $D_2 \geqslant 1$. We obtain

$$\begin{aligned}&\sum_{\substack{N^{2-\gamma-\epsilon}<p\leqslant N^{\beta_i}\\ p\in\mathscr{P}}} S(\mathscr{A}_p^{(i)}, \mathscr{P}, p) \qquad (8.2.33)\\
&\leqslant \sum_{\substack{R \text{ dyadic}\\ N^{2-\gamma-\epsilon}<R\leqslant N^{\beta_i}}} \sum_{\substack{p\in(R,2R]\\ p\in\mathscr{P}}} S(\mathscr{A}_p^{(i)}, \mathscr{P}, R)\\
&\leqslant \frac{(A+o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2} \sum_{\substack{R \text{ dyadic}\\ N^{2-\gamma-\epsilon}<R\leqslant N^{\beta_i}}} V(N^{2-\epsilon}/R) \sum_{\substack{p\in(R,2R]\\ p\in\mathscr{P}}} \frac{\varrho_i(p)}{p^2}\\
&\leqslant \frac{(cA+o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^\kappa} \sum_{\substack{N^{2-\gamma-\epsilon}\leqslant p<N^{\beta_i}\\ p\in\mathscr{P}}} \frac{\varrho_i(p)}{p^2(2-\epsilon-\frac{\log p}{\log N})^\kappa}, \qquad (8.2.34)\end{aligned}$$

where the last line follows from Lemma 8.2.1 and the fact that $V(N^{2-\epsilon}/R) < V(N^{2-\epsilon-\log p/\log N})$ for all $p \in (R, 2R]$.

We denote the sum in (8.2.34) by $T(\beta_i, \kappa)$. Since $\gamma < 1$, we have $2-\gamma-\epsilon > 1$ for sufficiently small $\epsilon$, and so we may upper bound $T(\beta_i, \kappa)$ by enlarging its range of summation to $N < p \leqslant N^{\beta_i}$. Define

$$A(t) = \sum_{p\in\mathscr{P}_{\leqslant t}} \frac{\varrho_i(p)}{p^2}, \qquad h(t) = \left(2-\epsilon-\frac{\log t}{\log N}\right)^{-\kappa}.$$

From Lemma 8.2.2, we have $A(t) = (1-\kappa_i)\log\log t + C + o(1)$ for some constant $C$. In particular, for any $r > 0$, we have $A(N^r) - A(N) = (1-\kappa_i)\log r + o(1)$.

Applying summation by parts, followed by the substitution $t = N^s$, we obtain

$$\begin{aligned}
&T(\beta_i, \kappa) \\
&\quad \leqslant (A(N^{\beta_i}) - A(N))h(N^{\beta_i}) - \int_N^{N^{\beta_i}} (A(t) - A(N))h'(t)\mathrm{d}t + o(1) \\
&\quad = (A(N^{\beta_i}) - A(N))h(N^{\beta_i}) - \int_1^{\beta_i} (A(N^s) - A(N))\frac{\partial h(N^s)}{\partial s}\mathrm{d}s + o(1) \\
&\quad = (1-\kappa_i)\log\beta_i h(N^{\beta_i}) - (1-\kappa_i)\int_1^{\beta_i} (\log s)\frac{\partial h(N^s)}{\partial s}\mathrm{d}s + o(1) \\
&\quad = (1-\kappa_i)\int_1^{\beta_i} \frac{h(N^s)}{s}\mathrm{d}s + o(1).
\end{aligned}$$

Finally, combining with (8.2.34), we conclude that for any $\epsilon > 0$,

$$S_3^{(i)} \leqslant \frac{(cA - \epsilon + o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^\kappa} \cdot (1-\kappa_i)\int_1^{\beta_i} (2-s)^{-\kappa}\frac{\mathrm{d}s}{s}. \tag{8.2.35}$$

Due to the factor $1 - \kappa_i = \alpha\theta_i$ appearing in the above estimate, $S_3^{(i)}$ becomes negligible compared to $S_1$ as $\alpha \to 0$. We perform a more precise quantitative comparison in Section 8.2.6.

## 8.2.5 The sums $S_4^{(i)}$

We begin in a similar manner to the sums $S_2^{(i)}$, by writing $f_i(a,b) = pr$, for $p \in \mathscr{P}$, where now $N^{\beta_i} < p \leqslant x$ and $R = x/N^{\beta_i}$. Let $D_1 = N^{\eta_1}$ and $D_2 = N^{\eta_2}$ for parameters $\eta_1, \eta_2$ (which may depend on $r$ and $i$) to be chosen later. We recall the definition of $h_i(r)$ from (8.2.27). Similarly to (8.2.28), we obtain

$$S_4^{(i)}(r) \leqslant \frac{(AA_i + o(1))\operatorname{Vol}(\mathscr{R})h_i(r)V_i(N^{\eta_1})V(N^{\eta_2})}{\Delta^2}, \tag{8.2.36}$$

provided that $D_2 \ll N^{1-\delta}$ and $D_1D_2 \ll N^{2-\delta}$ for some $\delta > 0$. In order to ensure the error terms from applying the level of distribution result from Corollary 5.9.2 are negligible after summing over $r$, we need $\eta_1, \eta_2$ to satisfy

$$\eta_1, \eta_2 > 0, \quad \eta_2 \leqslant 1 - \delta \qquad (\text{for all } r \leqslant R), \tag{8.2.37}$$

$$\sum_{r \leqslant R} N^{\eta_1+\eta_2} \leqslant N^{2-\delta}. \tag{8.2.38}$$

**Remark 8.2.3.** There are no $\eta_1, \eta_2$ satisfying the inequalities in (8.2.37) unless $R \leqslant N^{2-\delta}$, i.e., $x \leqslant N^{2-\delta+\beta_i}$. Since we had to assume $\beta_i < 2$ in the treatment of the sums $S_3^{(i)}$ in Section 8.2.4, this means our approach cannot handle the case $d \geqslant 4$, in which $f(x,y)$ has an irreducible factor of degree $\geqslant 4$. Therefore, we proceed with the additional assumption that $d \leqslant 3$.

Using Lemma 8.2.1 to estimate the products in (8.2.36), and taking a sum over $r$, we obtain

$$S_4^{(i)} \leqslant \frac{(cc_iAA_i + o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^{\kappa_i+\kappa}} \sum_{r\leqslant R} \frac{h_i(r)}{\eta_1^{\kappa_i}\eta_2^{\kappa}}. \tag{8.2.39}$$

We divide the sum over $r$ into dyadic intervals $r \in (R_1, 2R_1]$, and take $\eta_1, \eta_2$ depending only on $R_1$ and $i$. To obtain a good estimate for (8.2.39), we maximise $\eta_1^{\kappa_i}\eta_2^{\kappa}$ subject to the constraints

$$\eta_1, \eta_2 > 0, \qquad \eta_2 \leqslant 1-\delta, \qquad \eta_1 + \eta_2 \leqslant 2 - \delta - \frac{\log R_1}{\log N}.$$

By a similar computation to [69, Section 6.5], the optimal solution is

$$\eta_1 = \frac{\kappa_i}{\kappa+\kappa_i}\left(2-\delta-\frac{\log R_1}{\log N}\right),$$
$$\eta_2 = \frac{\kappa}{\kappa+\kappa_i}\left(2-\delta-\frac{\log R_1}{\log N}\right).$$

We note that this solution satisfies $\eta_2 \leqslant 1-\delta$ due to the assumption $\kappa < 1/2$. Substituting this choice of $\eta_1, \eta_2$ into (8.2.39), we obtain

$$\sum_{r\leqslant R} \frac{h_i(r)}{\eta_1^{\kappa_i}\eta_2^{\kappa}} \leqslant \sum_{r\leqslant R} w(r,\delta)h_i(r), \tag{8.2.40}$$

where

$$w(r,\delta) = \left(\frac{\kappa}{\kappa+\kappa_i}\right)^{-\kappa}\left(\frac{\kappa_i}{\kappa+\kappa_i}\right)^{-\kappa_i}\left(2-\delta-\frac{\log r}{\log N}\right)^{-(\kappa+\kappa_i)}. \tag{8.2.41}$$

We treat the sum in (8.2.40) using partial summation, for which we require estimates for $\sum_{r\leqslant t} h_i(r)$. For the case $d=2$, the estimate already found in (8.2.29) is sufficient. Below, we find a more refined estimate which we use in the case $d=3$.

We first consider the contribution to (8.2.40) from squarefree values of $r$. We would like to apply [52, Theorem A.5], which states that under certain hypothesis on the function $h_i(r)$, we have

$$\sum_{\substack{m\leqslant x\\ \mu^2(m)=1}} h_i(m) = c_{h_i}(\log x)^{\kappa_i} + O((\log x)^{\kappa_i-1}), \tag{8.2.42}$$

where

$$c_{h_i} = \frac{1}{\Gamma(\kappa_i+1)}\prod_p \left(1-\frac{1}{p}\right)^{\kappa_i}(1+h_i(p)).$$

In the following lemma, we verify that the function $h_i(r)$ satisfies the required hypotheses for [52, Theorem A.5].

**Lemma 8.2.4.** *For any $x \geqslant 1$ and any $2 \leqslant w < z$, the function $h_i(r)$ satisfies the following estimates.*

$$\prod_{w\leqslant p<z} (1+h_i(p)) \ll \left(\frac{\log z}{\log w}\right), \tag{8.2.43}$$

$$\sum_p h_i(p)^2 \log p < \infty, \tag{8.2.44}$$

$$\sum_{p\leqslant x} h_i(p)\log p = \kappa_i \log x + O(1). \tag{8.2.45}$$

*Proof.* To prove (8.2.43), we note that $1+h_i(p) = \left(1-\frac{\varrho_i(p)}{p^2}\right)^{-1}$ for all $p \in \mathscr{P}'$. The result is then immediate from Lemma 8.2.1. To prove (8.2.44), we recall that $\varrho_i(p) \ll p$, and so $h_i(p) \ll p^{-1}$. Therefore

$$\sum_p h_i(p)^2 \log p \ll \sum_p \frac{\log p}{p^2} < \infty.$$

Finally, we note that

$$\sum_{p\leqslant x} h_i(p)\log p = \sum_{\substack{p\leqslant x\\ p\in\mathscr{P}'}} \frac{\varrho_i(p)}{p^2}\log p + O(1),$$

so that (8.2.45) follows by applying Lemma 8.2.2. □

We can now evaluate the sum in (8.2.40) using partial summation. We obtain

$$\begin{aligned}
&\sum_{\substack{r\leqslant R\\ \mu^2(r)=1}} w(r,\delta)g_i(r)\\
&\qquad = w(R,\delta)\sum_{\substack{r\leqslant R\\ \mu^2(r)=1}} g_i(r) - \int_1^R \left(\sum_{\substack{r\leqslant t\\ \mu^2(r)=1}} g_i(r)\right) w'(t,\delta)\mathrm{d}t\\
&\qquad = c_{g_i}\left[(\log R)^{\kappa_i} w(R,\delta) - \int_1^R w'(t,\delta)(\log t)^{\kappa_i}\mathrm{d}t\right]\\
&\qquad\quad + o(1)\left[(\log R)^{\kappa_i} w(R,\delta) + \int_1^R w'(t,\delta)(\log t)^{\kappa_i}\mathrm{d}t\right]\\
&\qquad = c_{g_i}\kappa_i \int_1^R w(t,\delta)(\log t)^{\kappa_i-1}t^{-1}\mathrm{d}t + o\left((\log R)^{\kappa_i}\right)\\
&\qquad = c_{g_i}\kappa_i (\log N)^{\kappa_i}\int_0^{\log R/\log N} w(N^s,\delta)s^{\kappa_i-1}\mathrm{d}s + o\left((\log R)^{\kappa_i}\right)\\
&\qquad \leqslant (c_{g_i}\kappa_i + o(1))(\log N)^{\kappa_i}\int_0^{d-\beta_i} W(s)\mathrm{d}s,
\end{aligned}$$

where $W(s) = w(N^s,0)s^{\kappa_i-1}$.

We now consider the contribution to (8.2.27) from those $r$ which are not squarefree. Let $d_i$ denote the degree of $f_i$. From [40, Lemma 3.1], we have $\varrho_i(p^\alpha) \ll p^{2\alpha(1-1/d_i)}$ for all primes $p \notin S$ and any positive integer $\alpha$. By the multiplicativity of $h_i(r)$, it follows that $h_i(r) \ll r^{-2/d_i+\epsilon}$.

We recall that a positive integer $n$ is *squareful* if for any prime $p \mid n$, we also have $p^2 \mid n$. Since $d_i \leqslant 3$, we have

$$\sum_{r \text{ squareful}} h_i(r) \ll \sum_{r \text{ squareful}} r^{-2/d_i+\epsilon} \leqslant \sum_{r \text{ squareful}} r^{-2/3+\epsilon} < \infty,$$

where the last inequality follows from partial summation together with the fact that there are $O(M^{1/2})$ squareful positive integers less than $M$. Since $h_i(r)$ is supported on integers with no prime factors in $S$, for any $\epsilon > 0$, by adding into $S$ sufficiently many primes, we obtain

$$\sum_{\substack{r \text{ squareful} \\ r>1}} h_i(r) < \epsilon.$$

Proceeding as in [69, Lemma 6.2], we use that $w(r, \delta) \ll 1$, and decompose each non-squarefree $r$ into $r = r_1 r_2$, where $r_1$ is squarefree and $r_2 > 1$ is squareful. We have

$$\sum_{\substack{r \leqslant R \\ \mu^2(r)=0}} w(r, \delta) h_i(r) \ll \sum_{\substack{r_1 \leqslant R \\ \mu^2(r_1)=1}} h_i(r_1) \sum_{\substack{r_2 \text{ squareful} \\ r_2>1}} h_i(r_2).$$

Combining with (8.2.42), we deduce that for any $\epsilon > 0$, there is a choice of $S$ such that

$$\sum_{\substack{r \leqslant R \\ \mu^2(r)=0}} w(r, \delta) h_i(r) \leqslant (\epsilon + o(1))(\log N)^{\kappa_i}.$$

In conclusion, we have the upper bound

$$S_4^{(i)} \leqslant \frac{(cc_i A A_i c_{h_i} \kappa_i + \epsilon + o(1)) \operatorname{Vol}(\mathscr{R})}{\Delta^2 (\log N)^{\kappa}} \int_0^{d-\beta_i} W(s) \mathrm{d}s, \tag{8.2.46}$$

where

$$W(s) = \left(\frac{\kappa}{\kappa + \kappa_i}\right)^{-\kappa} \left(\frac{\kappa_i}{\kappa + \kappa_i}\right)^{-\kappa_i} (2-s)^{-(\kappa+\kappa_i)} s^{\kappa_i - 1}. \tag{8.2.47}$$

## 8.2.6 Proof of Theorem 5.7.1

We now suppose that $d = 2$, i.e., $f(x, y)$ consists of irreducible factors of degree at most 2. We first obtain a qualitative result by considering the limit as $\alpha \to 0$. As $\alpha \to 0$, we have $\kappa \to 0$ and $\kappa_i \to 1$. Therefore, we have $A_i \to A(1)$,

which is equal to $2e^{\gamma}$, where $\gamma = 0.57721...$ is the Euler–Mascheroni constant. Moreover, by [52, Equation (11.62)], we have $A(\kappa), B(\kappa) \to 1$ as $\kappa \to 0$. By a very similar computation to [69, p. 248], we have

$$c_i c_{h_i} = \frac{e^{-\gamma\kappa_i}}{\Gamma(1+\kappa_i)}. \tag{8.2.48}$$

Consequently, $\kappa_i c_i c c_{h_i} A A_i \ll B$ as $\alpha \to 0$, where the implied constant is absolute. Also,

$$\lim_{\alpha\to 0} W(s) = (2-s)^{-1}.$$

Therefore,

$$\lim_{\alpha\to 0} S_4^{(i)} \ll \frac{(B+o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^{\kappa}} (\log 2 - \log \beta_i). \tag{8.2.49}$$

For all $\epsilon > 0$, by choosing $\beta_i$ sufficiently close to 2, we have the bound

$$\lim_{\alpha\to 0} S_4^{(i)} \leqslant \frac{(\epsilon B+o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^{\kappa}} \ll \epsilon S_1. \tag{8.2.50}$$

We recall from Sections 8.2.3 and 8.2.4 that $S_2^{(i)}$ and $S_3^{(i)}$ are also negligible compared to $S_1$ as $\alpha \to 0$. Therefore, we see that $S(\mathscr{A}, \mathscr{P}, x) > 0$ for sufficiently small $\alpha$ and sufficiently large $N$.

To obtain the best quantitative bounds, the choices of $\beta_i \in (1,2)$ should be optimised so as to minimise $S_3^{(i)} + S_4^{(i)}$. However, in practice, numerical computations suggest that the optimal choices for $\beta_i$ are extremely close to 2, and little is lost in taking them arbitrarily close to 2, as above. In this case, the contributions from the sums $S_4^{(i)}$ are negligible. Taking a sum over $i$ of the estimates from (8.2.35) and combining with (8.2.26), we have

$$S(\mathscr{A}, \mathscr{P}, x) \geqslant \left(\frac{(c-\epsilon+o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^{\kappa}}\right)\left(B - A\alpha \sum_{i=m+1}^{k} \theta_i \int_1^2 (2-s)^{-\kappa}\frac{\mathrm{d}s}{s}\right)$$

for any $\epsilon > 0$. Let $r(\kappa) = B/A$. Then we have established that $S(\mathscr{A}, \mathscr{P}, x) > 0$ provided that

$$\alpha \sum_{i=m+1}^{k} \theta_i \int_1^2 (2-s)^{-\kappa}\frac{\mathrm{d}s}{s} < r(\kappa). \tag{8.2.51}$$

We recall that $\theta = \theta_0 + \cdots + \theta_k$ and $\kappa = \alpha\theta$. Therefore, we may replace $\alpha\sum_{i=m+1}^{k}\theta_i$ with the trivial upper bound $\kappa$, after which we find by numerical computations that the largest value of $\kappa$ we can take in (8.2.51) is $\kappa = 0.39006....$ Thus the condition $\alpha\theta < 0.39006...$ is enough to ensure that $S(\mathscr{A}, \mathscr{P}, x) > 0$ for sufficiently large $N$. This completes the proof of Theorem 5.7.1.

### 8.2.7 Proof of Theorem 5.7.2

We conclude this section by discussing the case $d = 3$, where $f(x, y)$ may contain irreducible factors of degree up to $3$. We recall in the case $d = 2$, the sums $S_4^{(i)}$ could be made negligible compared to $S_1$ by choosing $\beta_i$ arbitrarily close to $2$, due to the factor $\log 2 - \log \beta_i$ appearing in (8.2.49). When $d = 3$, we obtain the same bound as in (8.2.49), but with $\log 2 - \log \beta_i$ replaced with $\log 2 - \log(\beta_i - 1)$. Consequently, $S_4^{(i)}$ is no longer negligible, even when $\alpha \to 0$ and $\beta_i$ is arbitrarily close to $2$. In fact, it can be checked that its limit as $\alpha \to 0$ and $\beta_i \to 2$ is larger than $S_1$, and so the above methods break down in this case.

However, we recall the additional hypothesis in Theorem 5.7.2 that $\mathscr{P} \subseteq \{p \notin S : p \equiv 1 \pmod q\}$. By enlarging $\mathscr{P}$ if necessary, we may assume that $\mathscr{P} = \{p \notin S : p \equiv 1 \pmod q\}$. Then (5.7.6) holds with $\alpha = 1/(q-1)$, by Dirichlet's theorem on primes in arithmetic progressions. Moreover, it follows from Lemma 5.8.5 (a version of the Chebotarev density theorem) that (5.7.7) holds for some $\theta_i \leqslant 3$. We now explain why this choice of $\mathscr{P}$ is easier to handle than arbitrary choices of $\mathscr{P}$ of the same density $1/(q-1)$.

When applying the switching principle for $S_4^{(i)}$, we wrote $f_i(a, b) = pr$ for $p \in \mathscr{P}$. Since we may assume $q \in S$, the congruence condition $C(a, b)$ forces $f_i(a, b)$ to lie in a particular congruence class modulo $q$. Combined with the fact that $p \equiv 1 \pmod q$, we deduce that $r \equiv r_0 \pmod q$ for some $r_0$ depending only on $C(a, b)$ and $f_i$. Adding this congruence condition into (8.2.39) and (8.2.40), we obtain

$$S_4^{(i)} \leqslant \frac{(cc_iAA_i + o(1))\operatorname{Vol}(\mathscr{R})}{\Delta^2(\log N)^{\kappa_i+\kappa}} \sum_{\substack{r \leqslant R \\ r \equiv r_0 \pmod q}} w(r, \delta)h_i(r). \tag{8.2.52}$$

As demonstrated by Irving in [69, Lemma 6.1], the argument based on [52, Theorem A.5] we used to obtain (8.2.42) can be generalised to give

$$\sum_{\substack{r \leqslant x \\ \mu^2(r)=1 \\ r \equiv r_0 \pmod q}} h_i(r) = \frac{c_{h_i}}{q-1}(\log x)^{\kappa_i} + O((\log x)^{\kappa_i - 1}). \tag{8.2.53}$$

Proceeding as before, we then deduce the same estimate for $S_4^{(i)}$ as in (8.2.46), but with an additional factor $\alpha = 1/(q-1)$. It is now clear qualitatively that for sufficiently large $q$ (i.e., as $\alpha \to 0$), the sums $S_4^{(i)}$ are once again negligible compared to $S_1$.

We now make the above discussion more quantitative in order to complete the proof of Theorem 5.7.2. Combining everything, we see that $S(\mathscr{A}, \mathscr{P}, x) > 0$

for sufficiently large $N$ provided that

$$r(\kappa) - \sum_{i\,:\,\deg f_i=2} \alpha\theta_i \int_1^2 (2-s)^{-\kappa}\frac{\mathrm{d}s}{s} - \sum_{i\,:\,\deg f_i=3} \alpha A_i\kappa_i c_i c_{h_i} \int_0^1 W(s)\mathrm{d}s > 0. \tag{8.2.54}$$

We denote the left hand side of (8.2.54) by $F(\boldsymbol{\theta})$. Recalling (8.2.47) and (8.2.48), we have

$$\begin{aligned} &A_i\kappa_i c_i c_{h_i} \int_0^1 W(s)\mathrm{d}s \\ &\qquad = \frac{A_i\kappa_i e^{-\gamma\kappa_i}\kappa^{-\kappa}\kappa_i^{-\kappa_i}(\kappa+\kappa_i)^{\kappa+\kappa_i}}{\Gamma(1+\kappa_i)} \int_0^1 (2-s)^{-(\kappa+\kappa_i)} s^{\kappa_i-1}\mathrm{d}s. \end{aligned} \tag{8.2.55}$$

For a fixed choice of $\kappa < 1/2$, the integrand is a decreasing function of $\kappa_i$, because $0 \leqslant \frac{s}{(2-s)} \leqslant 1$ for any $s \in [0,1]$. The functions $\Gamma(1+\kappa_i)^{-1}$, $\kappa_i^{-\kappa_i}$ and $e^{-\gamma\kappa_i}$ are also decreasing in $\kappa_i$ in the range $\kappa_i \in (1/2, 1)$. Let $t = \alpha \deg f$. Since $\kappa_i \geqslant 1-\kappa \geqslant 1-t$, we therefore obtain an upper bound by replacing $\kappa_i$ with $1-t$ in all these terms. The remaining terms in (8.2.55) are all increasing in $\kappa_i$, and we apply the trivial bound $\kappa_i \leqslant 1$. Finally, we note that $\kappa^{-\kappa}(\kappa+\kappa_i)^{\kappa+\kappa_i}$ is an increasing function in $\kappa$ for $\kappa < 1/2$, and so we may replace $\kappa$ by $t$ in this expression. Therefore, (8.2.55) can be bounded by

$$\frac{A(1)e^{\gamma(t-1)}t^{-t}(t+1)^{t+1}}{\Gamma(2-t)} \int_0^1 (2-s)^{-1}s^{-\kappa}\mathrm{d}s. \tag{8.2.56}$$

We denote the factor outside the integral in (8.2.56) by $H(t)$. The integral in (8.2.56) is equal to the first integral in (8.2.54), as can be seen by making the substitution $u = 2-s$. Therefore,

$$F(\boldsymbol{\theta}) \geqslant r(\kappa) - \left(\sum_{i\,:\,\deg f_i=2} \alpha\theta_i + \sum_{i\,:\,\deg f_i=3} \alpha H(t)\right) \int_0^1 (2-s)^{-1}s^{-\kappa}\mathrm{d}s.$$

Recalling that $A(1) = 2e^{\gamma}$, it can be checked that $H(t) > 4$ for all $t > 0.2$, and so in particular $H(t) > 2\theta_i$ whenever $\deg f_i = 2$. Moreover, $r$ is a decreasing function of $\kappa$, so $r(\kappa) \geqslant r(t)$. We obtain

$$\begin{aligned} F(\boldsymbol{\theta}) &\geqslant r(t) - H(t)\int_0^1 (2-s)^{-1}s^{-t}\mathrm{d}s \left(\sum_{i\,:\,\deg f_i=2} \alpha/2 + \sum_{i:\deg f_i=3} \alpha\right) \\ &\geqslant r(t) - \frac{tH(t)}{3}\int_0^1 (2-s)^{-1}s^{-t}\mathrm{d}s \end{aligned}$$

for any $t > 0.2$. We find by numerical computations that the above expression is positive provided that $t < 0.32380....$ Since $t = \alpha\deg f$ and $\alpha = 1/(q-1)$, this gives the condition $q \geqslant (3.08825...)\deg f + 1$ claimed in Theorem 5.7.2.

## 8.3 Application to the Hasse principle

In this section, we apply the main sieve results (Theorem 5.7.1 and Theorem 5.7.2) obtained in Section 8.2 in order to prove Theorem 8.1.1 and Theorem 8.1.2.

### 8.3.1 Algebraic reduction of the problem

Let $K$ be a number field of degree $n$ satisfying the Hasse norm principle. In [69, Lemma 2.6], Irving turns the problem of establishing the Hasse principle for

$$f(t) = \mathbf{N}(x_1, \dots, x_n) \neq 0 \tag{8.3.1}$$

into a sieve problem. Irving assumes that $f(t) \in \mathbb{Z}[t]$ is an irreducible cubic polynomial. However, in the following result, we demonstrate that Irving's strategy can be applied to establish a similar result for an arbitrary polynomial $f \in \mathbb{Z}[t]$. We recall that $f(x, y)$ denotes the homogenisation of $f$. Throughout this section, we make the choice

$$\mathscr{P} = \{p \notin S : \text{ the inertia degrees of } p \text{ in } K/\mathbb{Q} \text{ are not coprime}\} \tag{8.3.2}$$

for a finite set of primes $S$ containing all ramified primes in $K/\mathbb{Q}$.

**Proposition 8.3.1.** *Suppose that (8.3.1) has solutions over $\mathbb{Q}_p$ for every $p$ and over $\mathbb{R}$. Let $\mathscr{P}$ and $S$ be as in (8.3.2). Then there exists $\Delta \in \mathbb{N}$, divisible only by primes in $S$, integers $a_0, b_0$, and real numbers $r, \xi > 0$ such that the following implication holds:*

*Suppose that $a, b$ are integers for which*

1. $a \equiv a_0 \pmod{\Delta}$ *and* $b \equiv b_0 \pmod{\Delta}$,
2. $|a/b - r| < \xi$,
3. $bf(a, b)$ *has no prime factors in* $\mathscr{P}$.

*Then* $(8.3.1)$ *has a solution over* $\mathbb{Q}$.

By multiplicativity of norms, it suffices to find integers $a, b$ such that $b$ and $f(a, b)$ are in $N_{K/\mathbb{Q}}(K^*)$. Since $K$ satisfies the Hasse norm principle, we have $\mathbb{Q}^* \cap N_{K/\mathbb{Q}}(K^*) = N_{K/\mathbb{Q}}(I_K)$, where $I_K$ denote the ideles of $K$. Consequently, to show that $c \in \mathbb{Q}^*$ is a norm from $K$, it suffices to find elements $x_v \in K_v^*$ for each place $v$ of $K$, such that

1. For all but finitely many places $v$ of $K$, we have $x_v \in \mathscr{O}_v^*$ (this ensures that $(x_v) \in I_K$).

2. For all places $w$ of $\mathbb{Q}$, we have

$$\prod_{v|w} N_{K_v/\mathbb{Q}_w}(x_v) = c. \tag{8.3.3}$$

The arguments in [69, Lemma 2.2, Lemma 2.3, Lemma 2.4] go through without changes. We summarise them below.

**Lemma 8.3.2.** *Suppose $c \neq 0$ is an integer. Then*

1. *If $p \nmid c$ and $K/\mathbb{Q}$ is unramified at $p$, then there exist $x_v \in \mathscr{O}_v^*$ for each place $v$ of $K$ above $p$, such that $\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = c$.*
2. *Suppose that $K/\mathbb{Q}$ is unramified at $p$, and that the inertia degrees above $p$ in K are coprime. Then there exist $x_v \in K_v^*$ for each place $v$ of $K$ above $p$, such that $\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = c$.*
3. *Let $p$ be a place of $\mathbb{Q}$. Suppose that there exists $x_1, \dots, x_n \in \mathbb{Q}_p$ such that $c = \mathbf{N}(x_1, \dots, x_n)$. Then there exists $x_v \in K_v^*$ for each place $v$ of $K$ above $p$, such that $\prod_{v|p} N_{K_v/\mathbb{Q}_p}(x_v) = c$.*

We now give a slight generalisation of [69, Lemma 2.5] to the case of an arbitrary polynomial $f$.

**Lemma 8.3.3.** *Let $p$ be a prime for which $f(t) = \mathbf{N}(x_1, \dots, x_n) \neq 0$ has a solution over $\mathbb{Q}_p$. Then there exists $a_0, b_0 \in \mathbb{Z}$ and $l \in \mathbb{N}$ (all depending on $p$) such that for any $a, b \in \mathbb{Z}$ satisfying $a \equiv a_0 \pmod{p^l}, b \equiv b_0 \pmod{p^l}$, we have $b, f(a,b) \in \mathbf{N}(\mathbb{Q}_p^n)\backslash\{0\}$.*

*Proof.* We define $N = \mathbf{N}(\mathbb{Q}_p^n)\backslash\{0\}$. Let $t_1 \in \mathbb{Q}_p$ be such that $f(t_1) = \mathbf{N}(x_1, \dots, x_n) \neq 0$ has a solution over $\mathbb{Q}_p$. Choose $a_1, b_1 \in \mathbb{Z}_p$ such that $\nu_p(b_1)$ is a multiple of $n$, and $a_1/b_1 = t_1$. Then $b_1 \in N$ and $f(a_1, b_1) \in N$.

The set $N \subseteq \mathbb{Q}_p$ is open, and so $N \times N \subseteq \mathbb{Q}_p^2$ is open. Moreover, the map $\varphi : \mathbb{Q}_p^2 \to \mathbb{Q}_p^2$ sending $(a, b)$ to $(f(a, b), b)$ is continuous in the $p$-adic topology. Therefore, the set $\varphi^{-1}(N \times N)$ is open, and contains the element $(a_1, b_1)$. Hence there is a small $p$-adic ball with center $(a_1, b_1)$, all of whose elements $(a, b)$ satisfy $b, f(a, b) \in N$. This ball can be described by congruence conditions $a \equiv a_0 \pmod{p^l}, b \equiv b_0 \pmod{p^l}$ for a sufficiently large integer $l$, as claimed in the lemma. □

*Proof of Proposition 8.3.1.* The proof closely follows the argument in [69, Lemma 2.6]. By the Hasse norm principle, to find solutions to (8.3.1) it suffices to find integers $a, b$ such that properties (1) and (2) stated before Lemma 8.3.2 hold with $c = b$ and $c = f(a, b)$. We divide the places of $\mathbb{Q}$ into four sets:

1. $p \in S$. Here, Lemma 8.3.3 gives congruence conditions $a \equiv a_{0,p} \pmod{p^l}$, $b \equiv b_{0,p} \pmod{p^l}$ which ensure that $b, f(a,b) \in N(\mathbb{Q}_p^n)\backslash\{0\}$. By part (3) of Lemma 8.3.2, we deduce that property (2) stated before Lemma 8.3.2 holds with $c = b$ and $c = f(a,b)$. The congruence conditions at each prime $p \in S$ can be merged into one congruence condition $a \equiv a_0 \pmod{\Delta}, b \equiv b_0 \pmod{\Delta}$ using the Chinese remainder theorem.

2. $p \notin S$ and $p \notin \mathscr{P}$. If $p \nmid b$, we apply part (1) of Lemma 8.3.2 with $c = b$. If $p \mid b$ we apply part (2) of Lemma 8.3.2 with $c = b$. The same argument works for $f(a,b)$ by choosing $c = f(a,b)$.

3. $p \in \mathscr{P}$. Since we are assuming that $bf(a,b)$ has no prime factors in $\mathscr{P}$, for these primes, part (1) of Lemma 8.3.2 applies with $c = bf(a,b)$.

4. $p = \infty$. We follow a similar argument to Lemma 8.3.3. We may assume that (8.3.1) is everywhere locally soluble, so in particular there exists $r \in \mathbb{R}$ such that $f(r) \in \mathbf{N}(\mathbb{R}^n)\backslash\{0\}$. Since $f$ is continuous and $\mathbf{N}(\mathbb{R}^n)\backslash\{0\}$ is open in the Euclidean topology, we can find $\xi > 0$ such that $f(t) \in \mathbf{N}(\mathbb{R}^n)\backslash\{0\}$ whenever $|t - r| < \xi$. Clearly solubility of $f(t) = \mathbf{N}(\mathbf{x}) \neq 0$ and $f(-t) = \mathbf{N}(\mathbf{x}) \neq 0$ over $\mathbb{Q}$ are equivalent; consequently, we may assume $r > 0$. Suppose in addition that $t \in \mathbb{Q}$, and write $t = a/b$ for $a, b \in \mathbb{N}$. Since $b$ is positive, it is automatically in $\mathbf{N}(\mathbb{R}^n)\backslash\{0\}$. By multiplicativity of norms, we conclude that $b, f(a,b) \in \mathbf{N}(\mathbb{R}^n)\backslash\{0\}$. The condition (8.3.3) now follows from part (3) of Lemma 8.3.2. □

**Example 8.3.4.** Let $f(t) = (t^2 - 2)(-t^2 + 3)$ and $K = \mathbb{Q}(i)$, so that

$$\begin{aligned} f(x,y) &= (x^2 - 2y^2)(-x^2 + 3y^2) \\ N_{K/\mathbb{Q}}(u,v) &= u^2 + v^2. \end{aligned}$$

It is known that there is a Brauer–Manin obstruction to the Hasse principle for the equation $(t^2 - 2)(-t^2 + 3) = u^2 + v^2 \neq 0$ by the work of Iskovskikh [70]. However, Proposition 8.3.1 still applies.

When $p \equiv 1 \pmod{4}$, the prime $p$ splits in $K/\mathbb{Q}$, and so the inertia degrees of $p$ in $K/\mathbb{Q}$ are coprime. On the other hand, when $p \equiv 3 \pmod{4}$, the prime $p$ is inert in $K/\mathbb{Q}$ and has degree 2, so the inertia degrees are not coprime. Therefore, we have $\mathscr{P} = \{p : p \equiv 3 \pmod{4}\}$. We choose $S = \{2\}$. In this example, it can be checked that the congruence conditions $a \equiv 8 \pmod{16}$ and $b \equiv 1 \pmod{16}$ are sufficient. Finally, for the infinite place, we just have the condition $f(a,b) > 0$. The sieve problem we obtain is to find integers $a, b$ such that

1. $a \equiv 8 \pmod{16}, b \equiv 1 \pmod{16}$,

2. $f(a,b) > 0$,

3. $f(a,b)$ has no prime factors $p \equiv 3 \pmod 4$.

We remark that $f(a/b) = b^{-4}f(a,b)$, and since $2 = [K:\mathbb{Q}]$ divides $4$, $b^{-4}$ is automatically a norm from $K$. This explains why in (3) above, we can consider prime factors of $f(a,b)$ rather than $bf(a,b)$.

An integer is the sum of two squares if and only if it is non-negative and all prime factors $p \equiv 3 \pmod 4$ occur with an even exponent. The above conditions are stronger than this, so the algebraic reduction performed in Proposition 8.3.1 is consistent with what we already knew for this example.

Since the Hasse principle fails for this example, we know that the above sieve problem cannot have a solution. This is indeed the case, since condition (1) implies that $-a^2+3b^2 \equiv 3 \pmod 4$, and so $f(a,b)$ must contain a prime factor $p \equiv 3 \pmod 4$.

The fact that the above sieve problem has no solutions also does not contradict Theorem 5.7.1. For a prime $p > 3$, we have that $\nu_1(p)$ is 2 if $p \equiv \pm 1 \pmod 8$ and zero otherwise, and $\nu_2(p)$ is 2 if $p \equiv \pm 1 \pmod{12}$ and zero otherwise. Consequently, by Dirichlet's theorem on primes in arithmetic progressions, for $i \in \{1,2\}$, asymptotically one half of the primes $p \in \mathscr{P}$ have $\nu_i(p) = 2$ and half have $\nu_i(p) = 0$. We conclude that $\theta_1 = \theta_2 = 1$, so that $\theta = 2$. Theorem 5.7.1 therefore requires the density of $\mathscr{P}$ to be less than $0.39006.../\theta = 0.19503....$ However, the density of $\mathscr{P}$ here is $1/2$, and so Theorem 5.7.1 does not apply to this example.

### 8.3.2 Proof of Theorem 8.1.1 and Theorem 8.1.2

*Proof of Theorem 8.1.1.* Since $K$ satisfies the Hasse norm principle, we may apply the algebraic reduction from Proposition 8.3.1. We take the sifting set $\mathscr{P}$ as defined in (8.3.2). We recall that we may exclude from $\mathscr{P}$ any finite set of primes, and so we may assume that $\mathscr{P}$ does not include the set of primes $S$ in the statement of Theorem 5.7.1, or any primes which are ramified in $K/\mathbb{Q}$. We make the choice $\mathscr{R} = \mathscr{B}N$, where $\mathscr{B}$ takes the form (5.7.1) for the parameters $r, \xi > 0$ coming from the application of Proposition 8.3.1. Let $F(x,y)$ be the binary form obtained from $yf(x,y)$ after removing any repeated factors. Clearly to prove $bf(a,b)$ is free from prime factors in $\mathscr{P}$, it suffices to prove $F(a,b)$ is, and so we may replace $bf(a,b)$ with $F(a,b)$ in condition (2) of Proposition 8.3.1. We apply Theorem 5.7.1 to the binary form $F(x,y)$, which has nonzero discriminant.

It remains only to check that (5.7.6) and (5.7.7) hold with $\alpha\theta < 0.39006....$ By Lemma 5.8.5, (5.7.6) holds with $\alpha = T(G)$. We now compute the quantity $\theta$. We claim that $\theta \leqslant k + j + 1$. Let $L$ denote the quadratic number field generated by $f$. We recall that $\theta$ is a sum over the quantities $\theta_i$ associated to

each irreducible factor of $f$, plus an additional term $\theta_0 = 1$ coming from the homogenising factor $f_0(x, y) = y$. We may therefore reduce to the case where $f$ is itself irreducible of degree at most 2, with the goal of proving that

$$\theta \leqslant \begin{cases} 3, & \text{if } f \text{ is quadratic and } L \subseteq \widehat{K}, \\ 2, & \text{if } f \text{ otherwise.} \end{cases}$$

If $f$ is linear, then $\nu_f(p) = 1$ for all $p \notin S$, and so $\theta = \theta_0 + 1 = 2$, as required. We now consider the case where $f$ is an irreducible quadratic. Let

$$\nu_f(p) = \#\{t \pmod p : f(t) \equiv 0 \pmod p\}.$$

If $L \subseteq \widehat{K}$, then Lemma 5.8.5 could be applied to compute $\theta$, with the desired error terms from (5.7.8). However, we apply the trivial bound $\nu_f(p) \leqslant 2$ for $p \notin S$, since it is not possible to improve on this in general. We therefore obtain $\theta \leqslant \theta_0 + 2 = 1 + 2 = 3$, which is satisfactory.

We now assume that $L \not\subseteq \widehat{K}$. We want to show that $\theta = 2$, or equivalently that $\nu_f(p) = 1$ on average over $p \in \mathscr{P}$. Let $M = \widehat{K}L$ be the compositum of $\widehat{K}$ and $L$. Since $\widehat{K} \cap L = \mathbb{Q}$, we have by [78, Ch. VI, Theorem 1.14] that $M/\mathbb{Q}$ is Galois, and

$$\mathrm{G}al(M/\mathbb{Q}) \cong \mathrm{G}al(L/\mathbb{Q}) \times \mathrm{G}al(\widehat{K}/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathrm{G}al(\widehat{K}/\mathbb{Q}).$$

We have $\nu_f(p) = 2$ if $p$ is split in $L$, and $\nu_f(p) = 0$ if $p$ is inert in $L$, and so

$$\theta = 1 + 2 \lim_{x \to \infty} \left( \frac{\#\{p \leqslant x : p \in \mathscr{P},\, p \text{ split in } L\}}{\#\{p \leqslant x : p \in \mathscr{P}\}} \right). \tag{8.3.4}$$

Let $\sigma' = (\tau, \sigma)$ be an element of $\mathrm{G}al(M/\mathbb{Q})$, where $\tau \in \mathrm{G}al(L/\mathbb{Q})$ and $\sigma \in \mathrm{G}al(\widehat{K}/\mathbb{Q})$. Applying Lemma 5.8.4, the primes $p \in \mathscr{P}$ correspond to the $\sigma'$ for which $\sigma$ has non-coprime cycle lengths (so these primes have density $T(G)$ as mentioned above). If in addition, the prime $p$ is split in $L$, then we require that $\tau = \mathrm{id}$. Therefore, by Lemma 5.8.5, asymptotically as $x \to \infty$, one half of the primes in $\mathscr{P}$ are also split in $L$. We conclude from (8.3.4) that (5.7.8) holds with $\theta = 1 + 2(1/2) = 2$. □

*Proof of Theorem 8.1.2.* We begin in the same manner as in the proof of Theorem 8.1.1, by appealing to Proposition 8.3.1 to reduce to a sieve problem. The binary form $F(x, y)$ has degree at most one higher than the degree of $f$. Therefore, we deduce from Theorem 5.7.2 that the Hasse principle holds for (8.1.1) provided that $q \geqslant (1 + 3.08825...) \deg f + 1$. □

**Remark 8.3.5.** Let $K = \mathbb{Q}(2^{1/q})$, where $q$ is prime. We recall from Example 5.8.8 that $G := \mathrm{G}al(\widehat{K}/\mathbb{Q})$ is isomorphic to the group $\mathrm{AGL}(1, q)$ of affine linear

transformations on $\mathbb{F}_q$, and from Table 5.2 we have $T(G) = 1/q$. From this, we see that Irving's choice of $\mathscr{P} = \{p \notin S : p \equiv 1 \pmod{q}\}$ is not quite optimal, because it has density $\alpha = 1/(q-1)$, whereas the set of primes we actually need to sift out has density $T(G) = 1/q$. In fact, we can see directly that even when $p \equiv 1 \pmod{q}$, there is sometimes a solution to $x^q - 2 \equiv 0 \pmod{p}$ (e.g. $q = 3$, $p = 31$, $x = 4$). However, it can be checked that even with this smaller sieve dimension, we are still not able to handle the cases $q = 5$ or $q = 3$ when $f$ is an irreducible cubic.

### 8.3.3 Proof of Corollary 8.1.3

We now consider the case when $[K : \mathbb{Q}] = n$ and $G = S_n$, with a view to proving Corollary 8.1.3. Such number fields automatically satisfy the Hasse principle by the work of Kunyavskiĭ and Voskresenskiĭ [76]. To ease notation, we shall write $T(n)$ in place of $T(S_n)$. In the following lemma, we find an estimate for $T(n)$.

**Lemma 8.3.6.** *For all $n \geqslant 1$, we have*

$$T(n) = 1 - \sum_{k|n} \frac{\mu(k)\Gamma((n+1)/k)}{\Gamma(1/k)\Gamma(n/k+1)}, \tag{8.3.5}$$

$$T(n) < \frac{2}{\sqrt{\pi}} n^{1/r-1}\omega(n), \tag{8.3.6}$$

*where $r$ is the smallest prime factor of $n$ and $\omega(n)$ is the number of prime factors of $n$.*

*Proof.* Define

$$T_k(n) = \frac{1}{n!}\#\{\sigma \in G : \text{ the cycle lengths of } \sigma \text{ are all divisible by } k\}.$$

By Möbius inversion, we have $T(n) = 1 - \sum_{k|n} \mu(k)T_k(n)$. We now find an explicit formula for $T_k(n)$. For $j \geqslant 1$, let $a_{jk}$ denote the number of cycles of length $jk$ in $\sigma$. The cycle lengths of $\sigma$ are all a multiple of $k$ if and only if $\sum_{j=1}^{n/k} jka_{jk} = n$. We apply the well-known formula for the number of permutations of $S_n$ with a given cycle shape from (5.8.1) to obtain

$$\begin{aligned} T_k(n) &= \frac{1}{n!} \sum_{\substack{a_k, a_{2k}, \ldots, a_n \\ \sum_{j=1}^{n/k} jka_{jk} = n}} \frac{n!}{\prod_{j=1}^{n/k} (jk)^{a_{jk}} a_{jk}!} \\ &= \sum_{\substack{b_1, \ldots, b_{n/k} \\ \sum_{j=1}^{n/k} jb_j = n/k}} \frac{1}{\prod_{j=1}^{n/k} (jk)^{b_j} b_j!} \\ &= \sum_{i=1}^{n/k} k^{-i} \sum_{\substack{b_1, \ldots, b_{n/k} \\ \sum_{j=1}^{n/k} jb_j = n/k \\ \sum_{j=1}^{n/k} b_j = i}} \frac{1}{\prod_{j=1}^{n/k} j^{b_j} b_j!} \\ &= \frac{1}{m!} \sum_{i=1}^{m} k^{-i} c(m,i), \end{aligned} \tag{8.3.7}$$

where $m = n/k$ and $c(m,i)$ is the number of $\sigma' \in S_m$ with exactly $i$ cycles. The quantity $c(m,i)$ is called the *Stirling number of the first kind*. In order to evaluate (8.3.7), we follow the argument from [49, Example II.12]. We define a bivariate generating function

$$P(w,z) := \sum_{i=0}^{\infty} w^i \sum_{m=0}^{\infty} \frac{z^m}{m!} c(m,i). \tag{8.3.8}$$

By [49, Proposition II.4], we have

$$\sum_{m=0}^{\infty} \frac{z^m}{m!} c(m,i) = \frac{1}{i!} \left( \log \left( \frac{1}{1-z} \right) \right)^i.$$

Therefore,

$$P(w,z) = \sum_{i=0}^{\infty} \frac{w^i}{i!} \left( \log \left( \frac{1}{1-z} \right) \right)^i = \exp \left( w \log \left( \frac{1}{1-z} \right) \right) = (1-z)^{-w}.$$

Applying the Binomial theorem, we find that the $z^m$ coefficient of $P(w,z)$ is equal to $w(w+1)\cdots(w+m-1)/m!$. On the other hand, if we substitute $w = 1/k$, the $z^m$ coefficient of (8.3.8) is precisely (8.3.7). We conclude that

$$\begin{aligned} \frac{1}{m!} \sum_{i=1}^{m} k^{-i} c(m,i) &= (1/k)(1+1/k)\cdots(m-1+1/k)/m! \\ &= \frac{\Gamma(m+1/k)}{\Gamma(1/k)\Gamma(m+1)}, \end{aligned}$$

which completes the proof of (8.3.5).

We now establish the upper bound in (8.3.6). A basic bound on the gamma function is that for any real $s \in (0,1)$ and any positive real number $x$, we have

$$x^{1-s} < \frac{\Gamma(x+1)}{\Gamma(x+s)} < (1+x)^{1-s}.$$

Applying this with $x = m$ and $s = 1/k$, we have

$$\frac{\Gamma(m+1/k)}{\Gamma(m+1)} < m^{1/k-1}.$$

Moreover, we have

$$\frac{1}{\Gamma(1/k)} = \frac{1}{\Gamma(1+1/k)} \frac{\Gamma(1+1/k)}{\Gamma(1/k)} \leqslant \frac{2}{\sqrt{\pi}k},$$

since $\Gamma(1+1/k)$ for integers $k \geqslant 2$ achieves its minimum at $k = 2$, where we have $\Gamma(1+1/k) = \Gamma(3/2) = \sqrt{\pi}/2$. We conclude that

$$T_k(n) < \frac{2}{\sqrt{\pi}k}(n/k)^{1/k-1} = \frac{2}{\sqrt{\pi}} n^{1/k-1} k^{-1/k} < \frac{2}{\sqrt{\pi}} n^{1/k-1}.$$

Taking a sum over $k = p$ prime, we obtain

$$T(n) < \sum_{p|n} T_p(n) \leqslant \frac{2}{\sqrt{\pi}} n^{1/r-1} \omega(n),$$

as required. □

*Proof of Corollary 8.1.3.* We recall the setting of Corollary 8.1.3. We assume that $G = S_n$, and $f$ is a product of two distinct irreducible quadratics. We apply Theorem 5.7.1 to the binary form $\prod_{i=0}^{2} f_i(x,y)$, where $f_0(x,y) = y$ and $f_1(x,y), f_2(x,y)$ are the homogenisations of the two quadratic factors of $f$. We also assume that the biquadratic extension $L$ generated by $f$ satisfies $L \cap \widehat{K} = \mathbb{Q}$, and so by the proof of Theorem 8.1.1, we have $\theta_0 = \theta_1 = \theta_2 = 1$, and $\theta = 3$. By maximising the value of $\kappa$ in (8.2.51) directly, we find by numerical computations that the largest value of $\kappa$ we can take here is $0.42221...$. (The slight improvement over $\kappa < 0.39006...$ for the general case comes from computing $\alpha \sum_{i=m+1}^{k} \theta_i = 2\alpha$ in our example, whilst in the proof of Theorem 8.1.1, we applied the trivial bound $\alpha \sum_{i=m+1}^{k} \theta_i \leqslant \kappa = 3\alpha$.) Hence the Hasse principle holds for $f(t) = \mathbf{N}(\mathbf{x}) \neq 0$ provided that $T(n) < 0.42221.../3 = 0.14073...$.

We use the upper bound (8.3.6) from Lemma 8.3.6 to reduce the $n$ for which $T(n) \geqslant 0.14073...$ to finitely many cases, and then the exact formula (8.3.5) to find precisely which $n$ satisfy $T(n) \geqslant 0.14073...$. We find that $T(n) < 0.14073...$ unless $n \in \{2, 3, \dots, 10, 12, 14, 15, 16, 18, 20, 22, 24, 26, 28, 30, 36, 42, 48\}$. □

## 8.4 Application to the Harpaz–Wittenberg conjecture

In this section, we apply the sieve result from Theorem 5.7.1 to prove Theorem 8.1.4. We recall the statement of [57, Conjecture 9.1] (we shall only work with the ground field $\mathbb{Q}$).

**Conjecture 8.4.1** (Harpaz, Wittenberg). *Let $P_1, \dots, P_n \in \mathbb{Q}[t]$ be pairwise distinct irreducible monic polynomials. Let $k_i = \mathbb{Q}[t]/(P_i(t))$ be the corresponding number fields. Let $a_i \in k_i$ denote the class of $t$. For each $i \in \{1, \dots, n\}$, let $L_i/k_i$ be a finite extension, and let $b_i \in k_i^*$. Let $S_0$ be a finite set of places of $\mathbb{Q}$ including the archimedean place, and all finite places above which, for some $i$, either $b_i$ is not a unit or $L_i/k_i$ is ramified. For each $v \in S_0$, fix an element $t_v \in \mathbb{Q}_v$. Suppose that for every $i \in \{1, \dots, n\}$ and every $v \in S_0$, there exists $x_{i,v} \in (L_i \otimes_{\mathbb{Q}} \mathbb{Q}_v)^*$ such that $b_i(t_v - a_i) = N_{L_i \otimes_{\mathbb{Q}} \mathbb{Q}_v / k_i \otimes_{\mathbb{Q}} \mathbb{Q}_v}(x_{i,v})$ in $k_i \otimes_{\mathbb{Q}} \mathbb{Q}_v$. Then there exists $t_0 \in \mathbb{Q}$ satisfying the following conditions.*

1. *$t_0$ is arbitrarily close to $t_v$ for all $v \in S_0$.*
2. *For every $i \in \{1, \dots, n\}$ and every place $\mathfrak{p}$ of $k_i$ with $\mathrm{ord}_{\mathfrak{p}}(t_0 - a_i) > 0$, either $\mathfrak{p}$ lies above a place of $S_0$ or the field $L_i$ possesses a place of degree $1$ over $\mathfrak{p}$.*

We remark that below, the $b_i$ and $x_{i,v}$ appearing in Conjecture 8.4.1 do not play a role, and so in the cases that Theorem 8.1.4 applies, it establishes a stronger version of Conjecture 8.4.1, where the assumption on the existence of the elements $x_{i,v}$ is removed.

We can reduce Conjecture 8.4.1 to a sieve problem as follows. Let $f_i(x, y) = c_i N_{k_i/\mathbb{Q}}(x - a_i y)$, where $c_i \in \mathbb{Q}$ is chosen such that the coefficients of $f_i(x, y)$ are coprime integers. Then $f_i(x, y)$ is an irreducible polynomial in $\mathbb{Z}[x, y]$.

Below, we suppose that $S$ is a finite set of primes containing all primes in $S_0$ and all primes dividing any of the denominators $c_1, \dots, c_n$. For $i \in \{1, \dots, n\}$, we define $\mathscr{P}_i$ to be the set of primes $p \notin S$, such that for some place $\mathfrak{p}$ of $k_i$ above $p$, $L_i$ does not possess a place of degree $1$ above $\mathfrak{p}$.

**Lemma 8.4.2.** *Let $k_1, \dots, k_n$ and $L_1, \dots, L_n$ and $S_0$ be as in Conjecture 8.4.1, and let $\mathscr{P}_i$ and $f_i(x, y)$ be as defined above. Suppose that there exists a finite set of primes $S$ as above, such that for any congruence condition $C(x, y)$ on $x, y$ modulo an integer $\Delta$ with only prime factors in $S$, and any real numbers $r, \xi > 0$, there exists $x_0, y_0 \in \mathbb{N}$ such that*

*(i) $C(x_0, y_0)$ holds,*

*(ii)* $|x_0/y_0 - r| < \xi$,

*(iii)* $f_i(x_0, y_0)$ *has no prime factors in* $\mathscr{P}_i$ *for all* $i \in \{1, \dots, n\}$.

*Then Conjecture 8.4.1 holds for this choice of* $k_1, \dots, k_n, L_1, \dots, L_n$ *and* $S_0$.

*Proof.* From [57, Remark 9.3 (iii)], we are free to adjoin to $S_0$ a finite number of places, and so we may assume that $S_0 = S \cup \{\infty\}$. We choose $t_0 = x_0/y_0$. Then property (1) of Conjecture 8.4.1 immediately follows from (i) and (ii) by appropriate choices of $C(x, y), r$ and $\xi$. Let $\mathfrak{p}$ be a place of $k_i$ above a prime $p \notin S$, satisfying $\mathrm{ord}_{\mathfrak{p}}(t_0 - a_i) > 0$. Then

$$f_i(x_0, y_0) = y_0^{\deg f_i} f_i(x_0/y_0, 1) = y_0^{\deg f_i} c_i N_{k_i/\mathbb{Q}}(t_0 - a_i).$$

Now $\mathrm{ord}_{\mathfrak{p}}(t_0 - a_i) > 0$ implies that $\mathrm{ord}_p(N_{k_i/\mathbb{Q}}(t_0 - a_i)) > 0$. Since $p \notin S$, we have $\mathrm{ord}_p(y_0 c_i) \geqslant 0$, and so $p \mid f_i(x_0, y_0)$. By (iii), we have $p \notin \mathscr{P}_i$, and so by construction of $\mathscr{P}_i$, we deduce that property (2) of Conjecture 8.4.1 holds. □

In view of Lemma 8.4.2, we let

$$\boldsymbol{\mathcal{P}} = (\mathscr{P}_1, \dots, \mathscr{P}_n),$$
$$\mathscr{R} = \{(x_0, y_0) \in [0, N]^2 : |x_0/y_0 - r| \leqslant \xi\},$$

and we aim to show that the sifting function

$$S(\mathscr{A}, \boldsymbol{\mathcal{P}}, x) = \#\{(x_0, y_0) \in \mathscr{R} \cap \mathbb{Z}^2 : C(x_0, y_0), \gcd(f_i(x_0, y_0), P_i(x)) = 1 \, \forall i\}$$

is positive for sufficiently large $N$. We do not attempt here to generalise Theorem 5.7.1 to deal with different sifting sets $\mathscr{P}_i$ for each $i$, but instead define $\mathscr{P} = \bigcup_{i=1}^n \mathscr{P}_i$ and replace each of the conditions $\gcd(f_i(x_0, y_0), P_i(x)) = 1$ with $\gcd(f_i(x_0, y_0), P(x)) = 1$. The resulting sifting function is precisely the function $S(\mathscr{A}, \mathscr{P}, x)$ from (8.2.1) with $f(x, y) = \prod_{i=1}^n f_i(x, y)$, which we can treat using Theorem 5.7.1 and Theorem 5.7.2. Below, we let $\alpha_i$ denote the density of $\mathscr{P}_i$, so that $\mathscr{P}$ has density $\alpha \leqslant \sum_{i=1}^n \alpha_i$.

*Proof of Theorem 8.1.4.* We recall that $L_i$ is the compositum $k_i M_i$, for a number field $M_i$ satisfying $k_i \cap M_i = \mathbb{Q}$. Consequently, $[L_i : k_i] = [M_i : \mathbb{Q}]$. Writing $M_i = \mathbb{Q}(\beta_i)$ using the primitive element theorem, we therefore have that the minimum polynomial of $\beta_i$ over $\mathbb{Q}$ and over $k_i$ coincide. We denote this minimum polynomial by $g_i$.

Let $\mathfrak{p}$ be a place of $k_i$. The inertia degrees of the places of $L_i$ above $\mathfrak{p}$ are the degrees of $g_i$ when factored modulo $\mathfrak{p}$. If $g_i$ has a root modulo $p$, then it has a root modulo every $\mathfrak{p} \mid p$, and so $p \notin \mathscr{P}_i$. Therefore, applying the Chebotarev

density theorem (Lemma 5.8.5), we have in the notation from (8.1.4) that $\alpha_i \leqslant T_i$.

We now bound the value of $\theta$ defined in (5.7.8). Here, we have already defined $f_i$ to be a binary form, and so no additional term $\theta_0$ coming from homogenisation is required. We apply the trivial estimate $\nu_i(p) \leqslant \deg f_i = [k_i : \mathbb{Q}]$ for all $p \notin S$. We conclude that $\theta \leqslant \sum_{i=1}^n [k_i : \mathbb{Q}] = d$. Combining Lemma 8.4.2 and Theorem 5.7.1 completes the proof of part (1) of Theorem 8.1.4.

We now turn to the cubic case. We recall from the discussion in Section 8.2.7 that in order to obtain good enough bounds on the sums $S_4^{(i)}$, we need $\mathscr{P} \subseteq \{p \notin S : p \equiv 1 \pmod q\}$ for a sufficiently large prime $q$. However, this does not hold for our current choice of $\mathscr{P}$; instead, we have the assumption in part (2) of Theorem 8.1.4 that $\mathscr{P}_i \subseteq \{p \notin S : p \equiv 1 \pmod{q_i}\}$ for each individual sifting set $\mathscr{P}_i$. In order to circumvent this, we observe that in the sieve decomposition in (8.2.3), we may replace the sum over $\mathscr{P}$ defining $S_4^{(i)}$ with a sum over $\mathscr{P}_i$. This reinserts the required congruence conditions $r \equiv r_0 \pmod{q_i}$ in the sums $S_4^{(i)}$. As in Section 8.2.7, we conclude that $S(\mathscr{A}, \boldsymbol{\mathcal{P}}, x) > 0$ for sufficiently large $N$, provided that $t < 0.28371...$, where $t = \deg f \sum_{i=1}^n 1/(q_i - 1)$. Rearranging, and recalling $\deg f = d$, we complete the proof of part (2) of Theorem 8.1.4. □

**Remark 8.4.3.** In contrast to Section 8.3, now $\mathrm{Gal}(\widehat{M_i}/\mathbb{Q}) = S_n$ is not a case we can handle, because there the proportion of fixed point free elements is $1 - 1/e$ as $n \to \infty$ (where $e = 2.718...$ is Euler's constant), which is much too large.

For a permutation group $G$ acting on $X = \{1, \dots, k\}$, we define $h(G)$ to be the proportion of elements of $G$ with no fixed point. The family of of groups $G$ for which $h(G)$ is smallest are the *Frobenius groups*. These are the groups where $G$ has a nontrivial element fixing one point of $X$, but no nontrivial elements fixing more than one point of $X$. We state two known results about Frobenius groups.

**Lemma 8.4.4** ([112, Theorem 1])**.** *Any Frobenius group can be realised as a Galois group over* $\mathbb{Q}$.

**Lemma 8.4.5** ([8, Theorem 3.1])**.** *Let $G$ be a transitive permutation group on $k$ letters.*

1. *We have $h(G) \geqslant 1/k$, with equality if and only if $G$ is a Frobenius group of order $k(k-1)$ and $k$ is a prime power.*
2. *In all other cases, $h(G) \geqslant 2/k$.*

*Proof of Corollary 8.1.5.* As computed in Example 8.3.5, we have that $G_i := \mathrm{Gal}(\widehat{M_i}/\mathbb{Q})$ is isomorphic to the group $\mathrm{AGL}(1, q_i)$ of affine linear transformations on $\mathbb{F}_{q_i}$. This is a Frobenius group of order $q_i(q_i - 1)$. By Lemma 8.4.5, we have $T_i = h(G_i) = 1/q_i$. (This also agrees with our computation in Example 8.3.5.) If $[k_i : \mathbb{Q}] \leqslant 2$ for all $i$, we can therefore apply part (1) of Theorem 8.1.4 provided that $\sum_{i=1}^{n} 1/q_i < 0.39006.../d$. Moreover, for all $i \in \{1, \dots, n\}$, the sifting sets $\mathscr{P}_i$ are contained in $\{p \notin S : p \equiv 1 \pmod{q_i}\}$. Indeed, it can be checked that the minimum polynomial $x^{q_i} - r_i$ has a root modulo $p$ for all but finitely many $p \not\equiv 1 \pmod{q_i}$, and these finitely many exceptional primes can be included in $S$. Therefore, we can apply part (2) of Theorem 8.1.4 provided that $\sum_{i=1}^{n} 1/(q_i - 1) < 0.28371.../d$. □

APPENDIX A

# The Brauer group for the equation $f(t) = \mathbf{N}(\mathbf{x}) \neq 0$

This appendix will be concerned with the Brauer group of a smooth projective model $X$ of the equation $f(t) = \mathbf{N}(\mathbf{x}) \neq 0$. In particular, we prove that in the setting of Corollary 8.1.3, we have $\mathrm{Br}\, X = \mathrm{Br}\, \mathbb{Q}$ whenever $n \geqslant 3$. We are grateful to Colliot-Thélène for providing the arguments presented in this appendix.

## A.1 Main results

**Theorem A.1.1.** *Let $k$ be a field of characteristic zero. Let $K/k$ be an extension of degree $n$, and let $L/k$ be the Galois closure. Suppose that $Gal(L/k) \cong S_n$. Let $f(t) \in k[t]$ be a squarefree polynomial. Let $Y/k$ be the affine variety given by the equation $\mathbf{N}(x_1, \ldots, x_n) = f(t) \neq 0$, and $Y \to \mathbb{A}^1_k$ its projection onto $t$. Let $\pi : X \to \mathbb{P}^1_k$ be a smooth projective birational model of $Y \to \mathbb{A}^1_k$. Suppose that $k[t]/(f(t))$ and $L$ are linearly disjoint over $k$. Then $\mathrm{Br}\, k = \mathrm{Br}\, X$.*

**Theorem A.1.2.** *Let $k$ be a field of characteristic zero. Let $K/k$ be a finite extension of degree $n \geqslant 3$, such that the Galois closure $L/k$ satisfies $Gal(L/k) = S_n$. Let $c \in k^\times$, and let $Z$ be a smooth projective model of $\mathbf{N}_{K/k}(x_1, \ldots, x_n) = c$. Then $\mathrm{Br}\, k \to \mathrm{Br}\, Z$ is surjective.*

## A.2 Proof of Theorem A.1.2

*Proof.* The key ideas of the proof are discussed in detail by Bayer-Fluckiger and Parimala [6], and so here we just give a sketch. We would like to show that

$\mathrm{Br}(Z)/\operatorname{Im}(\mathrm{Br}(k)) = 0$. We begin by reducing to the case $c = 1$. Suppose that $T$ is the norm one torus given by $\mathbf{N}_{K/k}(x_1, \ldots, x_n) = 1$, and let $T^c$ denote a smooth compactification of $T$. Let $k_s$ denote the separable closure of $k$, and let $\overline{Z} = Z \times_k k_s$, and $\overline{T} = T \times_k k_s$. By [36, Lemme 2.1], we have an isomorphism $H^1(k, \operatorname{Pic} \overline{Z}) \cong H^1(k, \operatorname{Pic} \overline{T^c})$. Combining this with [6, Theorem 2.4], we have

$$\mathrm{Br}(Z)/\operatorname{Im}(\mathrm{Br}(k)) \hookrightarrow H^1(k, \operatorname{Pic} \overline{Z}) \cong H^1(k, \operatorname{Pic} \overline{T^c}) \cong \mathrm{Br}(T^c)/\operatorname{Br}(k), \tag{A.2.1}$$

and hence it suffices to show that $\mathrm{Br}(T^c)/\operatorname{Br}(k) = 0$.

Let $G = \mathrm{Gal}(L/k)$. The character group $\widehat{T} = \operatorname{Hom}(T, \mathbb{G}_m)$ can be viewed as a $G$-lattice. By [34, Proposition 9.5 (ii)], we have an isomorphism

$$\mathrm{Br}(T^c)/\operatorname{Br}(k) \cong Ш^2_{\mathrm{cycl}}(G, \widehat{T}),$$

where

$$Ш^2_{\mathrm{cycl}}(G, \widehat{T}) = \ker\left[H^2(G, \widehat{T}) \to \prod_{g \in G} H^2(\langle g \rangle, \widehat{T})\right].$$

Let $M/k$ be a finite extension with $M$ linearly disjoint from $L$, and let $L' = LM, K' = KM, k' = kM$. Then the extension $K'/k'$ has degree $n$ and Galois closure $L'$, with $\mathrm{Gal}(L'/k') = G$. Moreover, by a construction of Frölich [53], we may choose $M$ in such a way that $L'/k'$ is unramified.

Using [6, Proposition 4.1], we have $Ш^2_{\mathrm{cycl}}(G, \widehat{T}) \cong Ш^2(k', \widehat{T})$, where $\widehat{T}$ is regarded as a $\mathrm{Gal}(k'_s/k')$-module via the surjection $\mathrm{Gal}(k'_s/k') \to G$. In turn, this is isomorphic to $Ш^1(k', T)^\vee$ by Poitou–Tate duality. To summarise, we have isomorphisms

$$\mathrm{Br}(T^c)/\operatorname{Br}(k) \cong Ш^2_{\mathrm{cycl}}(G, \widehat{T}) \cong Ш^2(k', \widehat{T}) \cong Ш^1(k', T)^\vee, \tag{A.2.2}$$

and so it suffices to show that $Ш^1(k', T) = 0$. However, $Ш^1(k', T)$ is isomorhpic to the knot group $\kappa(K'/k') = \frac{k'^\times \cap N_{K'/k'}(\mathbb{A}^\times_{K'})}{N_{K'/k'}(k'^\times)}$. Due to the assumption $\mathrm{Gal}(L'/k') = G = S_n$, we may apply the result of Kunyavskiĭ and Voskresenskiĭ [76] to deduce that the Hasse norm principle holds for the extension $K'/k'$, and hence $\kappa(K'/k') = 0$. □

## A.3 Proof of Theorem A.1.1

**Lemma A.3.1.** *The base change $X_K = X \times_k K$ is a $K$-rational variety.*

*Proof.* Since $X$ is a smooth projective model of $Y$, it suffices to show that $Y_K$ is $K$-rational. Let $K = k[x]/(p(x))$, where $p(x)$ is an irreducible polynomial over $k$. Let $a$ denote the class of $x$. Over $K$, the polynomial $p(x)$ factorises as

$p(x) = \prod_{i=0}^{r} q_i(x)$, where $q_0(x), \ldots, q_r(x) \in K[x]$ are distinct and irreducible, and $q_0(x) = x - a$. Let $K_i = K[x]/(q_i(x))$. We shall construct a birational map of the form

$$\begin{aligned} \varphi : Y_K &\to \mathbb{A}^1_K \times \prod_{i=1}^{r} R_{K_i/K}\mathbb{A}^1 \\ (t, x_0, \ldots, x_{n-1}) &\mapsto (t, z_1, \ldots, z_r), \end{aligned} \tag{A.3.1}$$

where $R_{K_i/K}$ denotes the Weil restriction. Since $R_{K_i/K}\mathbb{A}^1 \cong \mathbb{A}^{\deg q_i}_K$, the right hand side of (A.3.1) is isomorphic to $\mathbb{A}^n_K$, which is a Zariski open subset of $\mathbb{P}^n_K$. Therefore, $\varphi$ induces a birational map $Y_K \dashrightarrow \mathbb{P}^n_K$, as desired.

Let $\overline{k}$ denote an algebraic closure of $k$. We denote by $\mathrm{Emb}_k(K, \overline{k})$ the embeddings $K \hookrightarrow \overline{K}$ fixing $k$, or in other words, the conjugates of $K/k$ in $\overline{k}$. Over $\overline{k}$, the polynomials $p(t), q_0(t), \ldots, q_r(t)$ split as

$$p(t) = \prod_{\sigma \in \mathrm{Emb}_k(K,\overline{k})} (x - \sigma(a)), \qquad q_i(x) = \prod_{\substack{\sigma \in \mathrm{Emb}_k(K,\overline{k}) \\ q_i(\sigma(a))=0}} (x - \sigma(a)). \tag{A.3.2}$$

For each $i$, we fix an isomorphism $K_i \cong K(\sigma_i(a))$ for some $\sigma_i \in \mathrm{Emb}_k(K, \overline{k})$ satisfying $q_i(\sigma_i(a)) = 0$, and view $\sigma_i(a)$ as the class of $x$ in $K_i/K$. (The particular choice of representative $\sigma_i$ does not matter.) Since $q_i(x)$ is the minimum polynomial of $\sigma_i(a)$ over $K$, it splits over $\overline{k}$ as the product of the conjugates of $\sigma_i(a)$, and so

$$q_i(t) = \prod_{\sigma' \in \mathrm{Emb}_K(K_i,\overline{k})} (x - \sigma'\sigma_i(a)).$$

For $i \in \{0, \ldots, r\}$, we define $z_i \in R_{K_i/K}\mathbb{A}^1$ as

$$z_i = x_0 + \sigma_i(a)x_1 + \cdots + \sigma_i(a)^{n-1}x_{n-1}. \tag{A.3.3}$$

the polynomial $\sum_{j=0}^{\deg q_i - 1} z_i^{(j)} x^j$ representing $z_i$ is the reduction of $x_0 + x_1 x + \cdots + x_{n-1}x^{n-1}$ modulo $q_i$. By the Chinese remainder theorem, we have an isomorphism of $K$-algebras

$$K \otimes_k K \cong K[t]/(p(t)) \cong \prod_{i=0}^{r} K[t]/(q_i(t)) = \prod_{i=0}^{r} K_i,$$

and so $z_0, \ldots, z_r \in \prod_{i=0}^{r} R_{K_i/K}\mathbb{A}^1$ uniquely determine $x_0, \ldots, x_{n-1} \in \mathbb{A}^1_K$.

For any number field extension $E/M$, and any $y \in E$, we have

$$N_{E/M}(y) = \prod_{\sigma \in \mathrm{Emb}_M(E,\overline{M})} \sigma(y).$$

Therefore,

$$N_{K/k}(y) = \prod_{\sigma \in \mathrm{Emb}_k(K,\overline{k})} \sigma(y) = \prod_{i=0}^{r} \prod_{\sigma' \in \mathrm{Emb}_K(K_i,\overline{k})} \sigma'\sigma_i(y) = \prod_{i=0}^{r} N_{K_i/K}(\sigma_i(y)),$$

and so

$$\mathbf{N}_{K/k}(x_0, \ldots, x_{n-1}) = \prod_{i=0}^{r} N_{K_i/K}(z_i). \tag{A.3.4}$$

We deduce that the equations (A.3.3) define an isomorphism from $Y_K$ to the variety $V \subseteq \mathbb{A}^1_K \times \prod_{i=0}^r R_{K_i/K}\mathbb{A}^1$ given by $z_0 \prod_{i=1}^r N_{K_i/K}(z_i) = f(t) \neq 0$. For $t, z_1, \ldots, z_r$ satisfying the Zariski open condition $\prod_{i=1}^r N_{K_i/K}(z_i) \neq 0$, we have $z_0 = f(t)/\prod_{i=1}^n N_{K_i/K}(z_i)$. Therefore, the projection of $V$ onto $\mathbb{A}^1_K \times \prod_{i=1}^r R_{K_i/K}\mathbb{A}^1$ is birational. We conclude that the map $\varphi$ from (A.3.1) is birational. □

We now commence with the proof of Theorem A.1.1. Let $k$ be a field of characteristic zero. For a smooth irreducible variety $X/k$ with function field $\kappa(x)$, we recall that $\mathrm{Br}\, X$ consists of all elements of $\mathrm{Br}\, \kappa(X)$ which are unramified everywhere on $X$. Constant classes are unramified, and so we have $\mathrm{Br}\, k \subseteq \mathrm{Br}\, X \subseteq \mathrm{Br}\, \kappa(X)$. By the purity theorem [35, Theorem 3.7.1], the ramification locus of $\mathscr{A} \in \mathrm{Br}\, \kappa(X)$ is pure of codimension one. Consequently, to check $\mathscr{A} \in \mathrm{Br}\, X$, it suffices to check it is unramified at all codimension one points of $X$.

Let $C$ be a codimension one point. We recall from [35, Section 1.4.3] the *residue map*

$$\partial_C : \mathrm{Br}\, \kappa(X) \to H^1(\kappa(C), \mathbb{Q}/\mathbb{Z})$$

is such that $\mathscr{A}$ is unramified at $C$ if and only if $\partial_C(\mathscr{A})$ is trivial.

In our setting, codimension one points of $X$ come in two types:

1. Irreducible components of fibres $X_c = \pi^{-1}(c)$ above codimension one points $c$ of $\mathbb{P}^1_k$,

2. Codimension one points on the generic fibre $X_\eta$ of $\pi : X \to \mathbb{P}^1_k$.

We recall that $\kappa(X) = \kappa(X_\eta)$. The codimension one points of $X_\eta$ are a subset of the codimension one points of $X$, and so we have an inclusion $\mathrm{Br}\, X \hookrightarrow \mathrm{Br}\, X_\eta$. Since $X_\eta$ is a smooth projective model of $\mathbf{N}_{K(t)/k(t)}(x_1, \ldots, x_n) = f(t)$ over $k(t)$, it follows from Theorem A.1.2, applied to the extension $K(t)/k(t)$ and with $Z = X_\eta$, that $\mathrm{Br}\, k(t) \to \mathrm{Br}\, X_\eta$ is surjective. Putting everything together,

we obtain a commutative diagram

$$\begin{array}{ccccc} \operatorname{Br} X & \hookrightarrow & \operatorname{Br} X_\eta & \hookrightarrow & \operatorname{Br} \kappa(X_\eta) = \operatorname{Br} \kappa(X) \\ \uparrow & & \uparrow\!\!\uparrow & & \\ \operatorname{Br} k & \hookrightarrow & \operatorname{Br} k(t) & & \end{array}$$

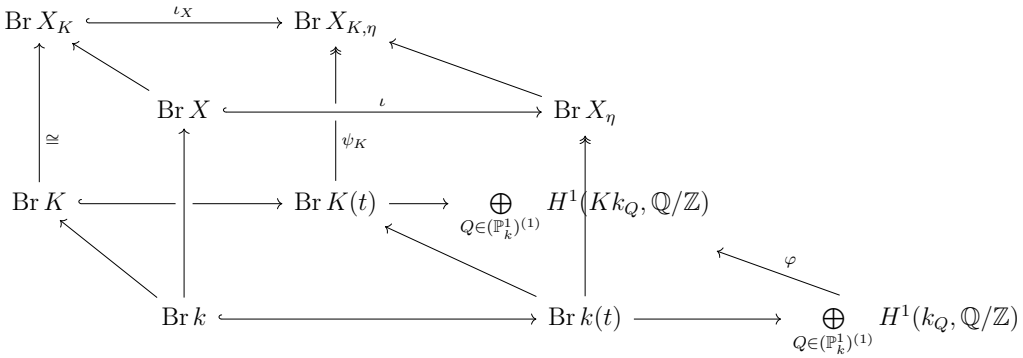
Let $\alpha \in \operatorname{Br} X$. By the above diagram, we can find $\beta \in \operatorname{Br} k(t)$ whose image in $\operatorname{Br} X_\eta$ is equal to the image of $\alpha$ in $\operatorname{Br} X_\eta$. We want to show that $\beta$ is the image of an element of $\operatorname{Br} k$, because then it follows from commutativity of the diagram that $\alpha$ is the image of an element of $\operatorname{Br} k$.

For any $n \geqslant 1$ and any field $k$, we have $\operatorname{Br} \mathbb{P}^n_k = \operatorname{Br} k$ [35, Theorem 6.1.3]. In particular, we have $\operatorname{Br} k = \operatorname{Br} \mathbb{P}^1_k$. Also, $k(t) = \kappa(\mathbb{P}^1_k)$, so $\operatorname{Br} k(t) = \operatorname{Br} \kappa(\mathbb{P}^1_k)$. Therefore, as discussed above, to prove that $\beta$ is in the image of $\operatorname{Br} k$, it suffices to show $\beta$ is unramified at every codimension one point of $\mathbb{P}^1_k$. This is formalised by the *Faddeev exact sequence* [35, Theorem 1.5.2], which is the exact sequence

$$0 \to \operatorname{Br}(k) \hookrightarrow \operatorname{Br} k(t) \to \bigoplus_{Q \in (\mathbb{P}^1_k)^{(1)}} H^1(k_Q, \mathbb{Q}/\mathbb{Z}) \twoheadrightarrow H^1(k, \mathbb{Q}/\mathbb{Z}) \to 0, \tag{A.3.5}$$

where $(\mathbb{P}^1_k)^{(1)}$ denotes the codimension one points of $\mathbb{P}^1_k$ and the third map is the direct sum of the residue maps $\partial_Q$. In other words, to show that $\beta \in \operatorname{Br} k(t)$ is actually in $\operatorname{Br} k$, it suffices to show that $\partial_Q(\beta) = 0$ for all $Q \in (\mathbb{P}^1_k)^{(1)}$. We have $\partial_Q(\beta) = 0$ unless $Q$ is an irreducible factor of $f(t)$ by [35, Proposition 11.1.5], so we suppose from now on that $Q$ is an irreducible factor of $f(t)$.

The base change $X_K = X \times_k K$ is a $K$-rational variety, i.e., it is birational to $\mathbb{P}^n_K$. Since the Brauer group is a birational invariant on smooth projective varieties [35, Corollary 6.2.11], it follows that $\operatorname{Br} X_K = \operatorname{Br} \mathbb{P}^n_K = \operatorname{Br} K$. Therefore, we obtain the following commutative diagram:




**Lemma A.3.2.** *We have $\partial_Q(\beta) \in \ker \varphi$, where $\varphi$ is as given in the above commutative diagram.*

*Proof.* Let $\beta_K$ denote the image of $\beta$ in $\operatorname{Br} K(t)$, and $\partial_{K,Q}$ the residue map at $Q$ on $\operatorname{Br} K(t)$. We want to show that $\partial_{K,Q}(\beta_K) = 0$. By exactness of the Faddeev exact sequence over $K$, for this it suffices to show $\beta_K$ is in the image $\operatorname{Br} K \to \operatorname{Br} K(t)$. We know that $\psi(\beta) = \iota(\alpha)$. Applying a base change to $K$, we see that $\psi_K(\beta_K) = \iota_K(\alpha_K)$, where $\alpha_K, \beta_K$ are the images of $\alpha, \beta$ under base change. Since $\operatorname{Br} K \cong \operatorname{Br} X_K$, we have that $\alpha_K$ is in the image of $\operatorname{Br} K \to \operatorname{Br} X_K$, and hence by commutativity of the diagram, $\beta_K$ is in the image of $\operatorname{Br} K \to \operatorname{Br} K(t)$, as required. □

Let $M$ be a number field, and let $G_M = \mathrm{G}al(\overline{M}/M)$. For a finite Galois extension $M'/M$, we consider $\mathrm{G}al(M'/M)$ as a topological space with the discrete toplology. We can then put the profinite topology on $G_M$, which is defined as the inverse limit

$$G_M = \varprojlim_{M'/M \text{ Galois}} \mathrm{G}al(M'/M).$$

We recall that $H^1(M, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}_{\text{cont}}(G_M, \mathbb{Q}/\mathbb{Z})$, the continuous group homomorphisms $G_M \to \mathbb{Q}/\mathbb{Z}$ [35, pp.16]. Suppose that $\theta \in \operatorname{Hom}_{\text{cont}}(G_M, \mathbb{Q}/\mathbb{Z})$. Then $\ker\theta$ is an open subgroup of $G_M$. Since $G_M$ is a profinite group, this implies that $\ker\theta$ has finite index in $G_M$. By the fundamental theorem of Galois theory, $\operatorname{im}\theta \cong G_M/\ker\theta \cong \mathrm{G}al(M'/M)$, for some finite Galois extension $M'/M$. Moreover, $\operatorname{im}\theta$ is a finite subgroup of $\mathbb{Q}/\mathbb{Z}$. All finite subgroups of $\mathbb{Q}/\mathbb{Z}$ are cyclic groups of the form $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ for some positive integer $n$. Consequently, $\ker\theta = \mathrm{G}al(M'/M)$ for a cyclic extension $M'/M$. To summarise, we have the identification

$$H^1(M, \mathbb{Q}/\mathbb{Z}) = \{M'/M \text{ cyclic, with a given map } \psi : \mathrm{G}al(M'/M) \hookrightarrow \mathbb{Q}/\mathbb{Z}\}.$$

Returning to our setup, we now define $\varphi : H^1(k_Q, \mathbb{Q}/\mathbb{Z}) \to H^1(Kk_Q, \mathbb{Q}/\mathbb{Z})$ explicitly. Using the above identification, we view an element $\theta \in H^1(k_Q, \mathbb{Q}/\mathbb{Z})$ as a pair $(M'/k_Q, \psi)$. The map $\varphi$ is given by taking the compositum with $K$. More precisely, it sends the above pair to $(KM'/Kk_Q, \psi)$, where now $\psi$ is viewed as a map $\mathrm{G}al(KM'/KK_Q) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ via the natural identification of $\mathrm{G}al(KM'/Kk_Q)$ as a subgroup of $\mathrm{G}al(M'/k_Q)$. Therefore, $(M'/k_Q, \psi) \in \ker\varphi$ if and only if $M'/k_Q$ is a cyclic subextension of $Kk_Q/k_Q$.

Due to the assumption that $k_Q$ and $L$ are linearly disjoint over $k$, we have $\mathrm{G}al(Kk_Q/k_Q) \cong \mathrm{G}al(K/k) \cong S_n$. We now complete the proof of Theorem A.1.1 with the following elementary group theory fact.

**Lemma A.3.3.** *Suppose that $K/k$ is a finite extension of degree $n \geqslant 3$, and the Galois group of the Galois closure $Gal(L/k)$ is isomorphic to $S_n$. Then there are no nontrivial cyclic extensions $M/k$ with $M \subseteq K$.*

*Proof.* By the fundamental theorem of Galois theory, if $M/k$ is a subextension of $K/k$, then $\mathrm{G}al(L/K) \leqslant \mathrm{G}al(L/M) \leqslant \mathrm{G}al(L/k) = S_n$. However, $\mathrm{G}al(L/K) \cong S_{n-1}$. (More explicitly, if $K = k(\alpha_1)$ and $\alpha_1, \ldots, \alpha_n$ are the roots of the minimum polynomial of $\alpha_1$ over $k$, then $\mathrm{G}al(L/K)$ consists of all permutations of $\{\alpha_1, \ldots, \alpha_n\}$ which fix $\alpha_1$.) However, $S_{n-1}$ is a maximal subgroup of $S_n$, and so $M = k$ or $M = K$. Since $n \geqslant 3$, the extension $K/k$ is not cyclic. Therefore, $M = k$. □

In conclusion, the map $\varphi : H^1(k_Q, \mathbb{Q}/\mathbb{Z}) \to H^1(Kk_Q, \mathbb{Q}/\mathbb{Z})$ is injective by Lemma A.3.3, and $\partial_Q(\beta) \in \ker \varphi$ by Lemma A.3.2, and hence $\partial_Q(\beta) = 0$. This means that all the residue maps of $\beta$ are trivial, so $\beta$ is in the image of $\mathrm{Br}\, k \to \mathrm{Br}\, k(t)$. Hence $\alpha$ is in the image of $\mathrm{Br}\, k \to \mathrm{Br}\, X$, and so $\mathrm{Br}\, X = \mathrm{Br}\, k$. This completes the proof of Theorem A.1.1.

# Bibliography


[1] Abramovich D. Birational geometry for number theorists. *Arithmetic geometry, Clay Mathematics Proceedings*, 8:335–373, 2009.

[2] Bartels H.-J. Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen. *Journal of Algebra*, 70:179–199, 1981.

[3] Bateman P., and Grosswald E. On a theorem of Erdös and Szekeres. *Illinois Journal of Mathematics*, 2:88–98, 1958.

[4] Batyrev V., and Tschinkel Y. Rational points on some Fano cubic bundles. *Comptes Rendus de l'Académie des Sciences Series I-Mathematics*, 323:41–46, 1996.

[5] Batyrev V., and Tschinkel Y. Manin's conjecture for toric varieties. *Journal of Algebraic Geometry*, 7:15–53, 1998.

[6] Bayer-Fluckiger E., and Parimala R. On unramified Brauer groups of torsors over tori. *Documenta mathematica*, 25, 2020.

[7] Birch J. Forms in many variables. *Proceedings of the Royal Society of London. Series A. Mathematical and Physical Sciences*, 265:245–263, 1962.

[8] Boston N., Dabrowski W., Foguel T., Gies P., Jackson D., Ose D., and Walker J. The proportion of fixed-point-free elements of a transitive permutation group. *Communications in Algebra*, 21:3259–3275, 1993.

[9] Browning T. An overview of Manin's conjecture for del Pezzo surfaces. *Analytic number theory*, 7:39–55, 2007.

[10] Browning T. Density of integer solutions to diagonal quadratic forms. *Monatshefte für Mathematik*, 152(1):13–38, 2007.

[11] Browning T. *Quantitative Arithmetic of Projective Varieties*. Progress in Mathematics. Springer, 2009.

[12] Browning T. *Cubic Forms and the Circle Method*. Birkhäuser, Cambridge, MA, 2022.

[13] Browning T., and Gorodnik A. Power-free values of polynomials on symmetric varieties. *Proceedings of the London Mathematical Society*, 114:1044–1080, 2017.

[14] Browning T., and Heath-Brown D.R. Quadratic polynomials represented by norm forms. *Geometric and Functional Analysis*, 22(5):1124–1190, 2012.

[15] Browning T., and Heath-Brown D.R. Forms in many variables and differing degrees. *Journal of the European Mathematical Society*, 19:357–394, 2017.

[16] Browning T., and Heath-Brown D.R. Counting rational points on quadric surfaces. *Discrete Analysis*, 15, 2018.

[17] Browning T., and Heath-Brown D.R. Density of rational points on a quadric bundle in $\mathbb{P}^3 \times \mathbb{P}^3$. *Duke Mathematical Journal*, 169:3099–3165, 2020.

[18] Browning T., and Hu L. Counting rational points on biquadratic hypersurfaces. *Advances in Mathematics*, 349:920–940, 2019.

[19] Browning T., and Matthiesen L. Norm forms for arbitrary number fields as products of linear polynomials. *Annales Scientifiques de l'École Normale Supérieure*, 50:1383–1446, 2017.

[20] Browning T., and Prendiville S. Improvements in Birch's theorem on forms in many variables. *Journal für die Reine und Angewandte Mathematik*, pages 203–234, 2017.

[21] Browning T., and Schindler D. Strong approximation and a conjecture of Harpaz and Wittenberg. *International Mathematics Research Notices*, pages 4340–4369, 2019.

[22] Browning T., and Van Valckenborgh K. Sums of three squareful numbers. *Experimental Mathematics*, 21:204–211, 2012.

[23] Browning T., and Yamagishi S. Arithmetic of higher-dimensional orbifolds and a mixed Waring problem. *Mathematische Zeitschrift*, 299:1071–1101, 2021.

[24] Brun V. Über das Goldbachsche Gesetz und die Anzahl der Primzahllpaare. *Archiv for Mathematik og Naturvidenskab*, 1915.

[25] Campana F. Orbifolds, special varieties and classification theory. *Annales de l'institut Fourier*, 54:499–630, 2004.

[26] Campana F. Orbifoldes géométriques spéciales et classification biméromorphe des variétés Kählériennes compactes. *Journal of the Institute of Mathematics of Jussieu*, 10:809–934, 2011.

[27] Cassels J. Bounds for the least solutions of homogeneous quadratic equations. *Mathematical Proceedings of the Cambridge Philosophical Society*, 51:262–264, 1955.

[28] Chambert-Loir A., and Tschinkel Y. On the distribution of points of bounded height on equivariant compactifications of vector groups. *Inventiones Mathematicae*, 148:421–452, 2002.

[29] Chambert-Loir A., and Tschinkel Y. Integral points of bounded height on partial equivariant compactifications of vector groups. *Duke Mathematical Journal*, 161:2799–2836, 2012.

[30] Chen R. On the representation of a larger even integer as the sum of a prime and the product of at most two primes. *Scientia Sinica*, 16:157–176, 1973.

[31] Colliot-Thélène J.-L. Points rationnels sur les fibrations. In *Higher dimensional varieties and rational points*, pages 171–221. Springer, 2003.

[32] Colliot-Thélène J.-L., and Salberger P. Arithmetic on some singular cubic hypersurfaces. *Proceedings of the London Mathematical Society*, 3:519–549, 1989.

[33] Colliot-Thélène J.-L., and Sansuc J.-J. La $R$-équivalence sur les tores. In *Annales scientifiques de l'École Normale Supérieure*, volume 10, pages 175–229, 1977.

[34] Colliot-Thélène J.-L., and Sansuc J.-J. Principal homogeneous spaces under flasque tori: Applications. *Journal of Algebra*, 106:148–205, 1987.

[35] Colliot-Thélène J.-L., and Skorobogatov A. *The Brauer–Grothendieck group*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics. Springer Nature, Cham, Switzerland, 2021.

[36] Colliot-Thélène J.-L., Harari D., and Skorobogatov A. Valeurs d'un polynôme à une variable représentées par une norme. *London Mathematical Society lecture note series*, pages 69–90, 2003.

[37] Colliot-Thélène J.-L., Sansuc J.-J., and Swinnerton-Dyer P. Intersections of two quadrics and Châtelet surfaces. I. *Journal für die Reine und Angewandte Mathematik*, 373:37–107, 1987.

[38] Colliot-Thélène J.-L., and Swinnerton-Dyer P. Hasse principle and weak approximation for pencils of Severi–Brauer and similar varieties. *Journal für die Reine und Angewandte Mathematik*, 1994:49–112, 1994.

[39] Comtat F. A uniform estimate for the density of rational points on quadrics. *Journal de Théorie des Nombres de Bordeaux*, 31:243–253, 2019.

[40] Daniel S. On the divisor-sum problem for binary forms. *Journal für die Reine und Angewandte Mathematik*, 507:107–129, 1999.

[41] Davenport H. Cubic forms in thirty-two variables. *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 251:193–232, 1959.

[42] de la Bretèche R. Nombre de points de hauteur bornée sur les surfaces de del Pezzo de degré 5. *Duke Mathematical Journal*, 113:421–464, 2002.

[43] de la Bretèche R., and Browning T. Manin's conjecture for quartic del Pezzo surfaces with a conic fibration. *Duke Mathematical Journal*, 160:1–69, 2011.

[44] Derenthal U., Smeets A., and Wei D. Universal torsors and values of quadratic polynomials represented by norms. *Mathematische Annalen*, 361:1021–1042, 2015.

[45] Dietmann R. Small solutions of quadratic Diophantine equations. *Proceedings of the London Mathematical Society*, 86:545–582, 2003.

[46] Duke W., Friedlander J., and Iwaniec H. Bounds for automorphic L-functions. *Inventiones Mathematicae*, 112:1–8, 1993.

[47] Erdös P., and Szekeres G. Über die Anzahl der abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem. *Acta Scientiarum Mathematicarum*, 7:95–102, 1934.

[48] Faltings G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones Mathematicae*, 73:349–366, 1983.

[49] Flajolet P., and Sedgewick R. *Analytic combinatorics*. Cambridge University Press, 2009.

[50] Franke J., Manin Y., and Tschinkel Y. Rational points of bounded height on Fano varieties. *Inventiones Mathematicae*, 95:421–435, 1989.

[51] Friedlander J., and Iwaniec H. The polynomial $x^2 + y^4$ captures its primes. *Annals of Mathematics*, pages 945–1040, 1998.

[52] Friedlander J., and Iwaniec H. *Opera de Cribro*, volume 57. American Mathematical Society, 2010.

[53] Fröhlich A. On non-ramified extensions with prescribed Galois group. *Mathematika*, 9:133–134, 1962.

[54] Green B., and Tao T. Linear equations in primes. *Annals of Mathematics*, pages 1753–1850, 2010.

[55] Green B., Tao T., and Ziegler T. An inverse theorem for the Gowers $U^{s+1}[N]$-norm. *Annals of Mathematics*, pages 1231–1372, 2012.

[56] Hardy G., and Wright E. *An Introduction to the Theory of Numbers*. Oxford University Press, 6th edition, 2008.

[57] Harpaz Y., and Wittenberg O. On the fibration method for zero-cycles and rational points. *Annals of Mathematics*, pages 229–295, 2016.

[58] Harpaz Y., Wei D., and Wittenberg O. Rational points on fibrations with few non-split fibres. *arXiv:2109.03547*, 2021.

[59] Hartshorne R. *Algebraic Geometry*. Graduate Texts in Mathematics, Vol. 52. Springer-Verlag, 1977.

[60] Heath-Brown D.R. Cubic forms in $10$ variables. In *Number Theory Noordwijkerhout 1983*, pages 104–108. Springer, 1984.

[61] Heath-Brown D.R. A new form of the circle method, and its application to quadratic forms. *Journal für die Reine und Angewandte Mathematik*, 481:149–206, 1996.

[62] Heath-Brown D.R. The density of rational points on curves and surfaces. *Annals of Mathematics*, 155:553–598, 2002.

[63] Heath-Brown D.R., and Moroz B. Primes represented by binary cubic forms. *Proceedings of the London Mathematical Society*, 84:257–288, 2002.

[64] Heath-Brown D.R., and Pierce L. Simultaneous integer values of pairs of quadratic forms. *Journal für die Reine und Angewandte Mathematik*, 727:85–143, 2017.

[65] Heath-Brown D.R., and Skorobogatov A. Rational solutions of certain equations involving norms. *Acta Mathematica*, 189:161–177, 2002.

[66] Hindry M., and Silverman J. *Diophantine Geometry: An Introduction*, volume 201. Springer Science & Business Media, 2013.

[67] Hooley C. On Waring's problem. *Acta Mathematica*, 157:49–97, 1986.

[68] Hosgood T. An introduction to varieties in weighted projective space. *arXiv:1604.02441*, 2016.

[69] Irving A. Cubic polynomials represented by norm forms. *Journal für die Reine und Angewandte Mathematik*, 2017:217–250, 2017.

[70] Iskovskikh V. A counterexample to the Hasse principle for a system of two quadratic forms in five variables. *Matematicheskie Zametki*, 10:253–257, 1971.

[71] Iwaniec H., and Kowalski E. *Analytic Number Theory*, volume 53. American Mathematical Society, 2004.

[72] Jahnel J. *Brauer Groups, Tamagawa Measures, and Rational Points on Algebraic Varieties.* American Mathematical Society, Vol. 198, 2014.

[73] Janusz J. *Algebraic Number Fields*, volume 7. American Mathematical Society, 1996.

[74] Karpilovsky G. *Topics in Field Theory*. North-Holland Mathematics Studies. Elsevier, 1989.

[75] Kloosterman H.D. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Mathematica*, 49:407–464, 1926.

[76] Kunyavskiĭ B., and Voskresenskiĭ V. Maximal tori in semisimple algebraic groups. *Manuscript deposited at VINITI*, 15:1269–84, 1984.

[77] Lagarias J., and Odlyzko A. Effective versions of the Chebotarev density theorem. *Algebraic Number Fields*, (A. Frölich edit.):409–464, 1977.

[78] Lang S. *Algebra (Revised Third Edition)*. Graduate Texts in Mathematics. Springer, 2002.

[79] Lazarsfeld R. *Positivity in Algebraic Geometry I: Classical Setting: Line Bundles and Linear Series*, volume 48. Springer, 2017.

[80] Lee A. Birch's theorem in function fields. *arXiv:1109.4953*, 2011.

[81] Lehmann B., Sengupta A., and Tanimoto S. Geometric consistency of Manin's conjecture. *arXiv:1805.10580*, 2018.

[82] Loughran D. Rational points of bounded height and the Weil restriction. *Israel Journal of Mathematics*, 210:47–79, 2015.

[83] Macedo A. The Hasse norm principle for $A_n$-extensions. *Journal of Number Theory*, 211:500–512, 2020.

[84] Marmon O., and Vishe P. On the Hasse principle for quartic hypersurfaces. *Duke Mathematical Journal*, 168:2727–2799, 2019.

[85] Matthiesen L. On the square-free representation function of a norm form and nilsequences. *Journal of the Institute of Mathematics of Jussieu*, 17:107–135, 2018.

[86] Maynard J. Small gaps between primes. *Annals of Mathematics*, pages 383–413, 2015.

[87] Maynard J. Primes with restricted digits. *Inventiones Mathematicae*, 217:127–218, 2019.

[88] Mitsui T. on the prime ideal theorem, dedicated to Professor S. Iyanaga on his 60th birthday. *Journal of the Mathematical Society of Japan*, 20:233–247, 1968.

[89] Munshi R. Pairs of quadrics in 11 variables. *Compositio Mathematica*, 151:1189–1214, 2015.

[90] Nakahara M., and Streeter S. Weak approximation and the Hilbert property for Campana points. *arXiv:2010.12555*, 2020.

[91] Peyre E. Hauteurs et mesures de Tamagawa sur les variétés de Fano. *Duke Mathematical Journal*, 79:101–218, 1995.

[92] Peyre E. Points de hauteur bornée, topologie adélique et mesures de Tamagawa. *Journal de Théorie des Nombres de Bordeaux*, 15:319–349, 2003.

[93] Peyre, E. Liberté et accumulation. *Documenta Mathematica*, 22:1615–1659, 2017.

[94] Peyre E. Beyond heights: Slopes and distribution of rational points. In *Arakelov Geometry and Diophantine Applications*, pages 215–279. Springer, 2021.

[95] Pieropan M., and Schindler D. Hyperbola method on toric varieties. *arXiv:2001.09815*, 2020.

[96] Pieropan M., Smeets A., Tanimoto S., and Várilly-Alvarado A. Campana points of bounded height on vector group compactifications. *Proceedings of the London Mathematical Society*, 2020.

[97] Polymath DHJ. Variants of the Selberg sieve, and bounded intervals containing many primes. *Research in the Mathematical Sciences*, 1:1–83, 2014.

[98] Poonen B. The projective line minus three fractional points. http://www-math.mit.edu/poonen/slides/campana_s.pdf, 2006.

[99] Rydin Myerson S. Quadratic forms and systems of forms in many variables. *Inventiones Mathematicae*, 213:205–235, 2018.

[100] Sawin W. Freeness alone is insufficient for Manin–Peyre. *arXiv:2001.06078*, 2020.

[101] Schindler D. Bihomogeneous forms in many variables. *Journal de Théorie des Nombres de Bordeaux*, 26:483–506, 2014.

[102] Schindler D., and Skorobogatov A. Norms as products of linear polynomials. *Journal of the London Mathematical Society*, 89:559–580, 2014.

[103] Selmer S. The Diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Mathematica*, 85:203–362, 1951.

[104] Serre J.-P. *Lectures on the Mordell–Weil Theorem, 3rd Edition*. Aspects of Mathematics. Vieweg $\&$ Teubner Verlag, Wiesbaden, 1997.

[105] Serre J.-P. *Topics in Galois Theory, 2nd Edition*. Research Notes in Mathematics, Vol. 1. A K Peters, Ltd., Wellesley, MA, 2008. With notes by Henri Darmon.

[106] Serre J.-P. *A Course in Arithmetic*, volume 7. Springer Science & Business Media, 2012.

[107] Shute A. Sums of four squareful numbers. *arXiv:2104.06966*, 2021.

[108] Shute A. On the leading constant in the Manin-type conjecture for Campana points. *arXiv:2104.14946v2*, 2022.

[109] Skinner M. Forms over number fields and weak approximation. *Compositio Mathematica*, 106:11–29, 1997.

[110] Skorobogatov A., and Sofos E. Schinzel hypothesis with probability 1 and rational points. *arXiv:2005.02998*, 2020.

[111] Sofos E. Uniformly counting rational points on conics. *Acta Arithmetica*, 166:1–13, 2014.

[112] Sonn J. $\mathrm{SL}(2,5)$ and Frobenius Galois groups over $\mathbb{Q}$. *Canadian Journal of Mathematics*, 32:281–293, 1980.

[113] Stein E., and Shakarchi R. *Functional Analysis*. Princeton Lectures in Analysis. Princeton University Press, 2011.

[114] Stein E., and Weiss G. *Introduction to Fourier Analysis on Euclidean Spaces*, volume 32 of *Princeton Mathematical*. Princeton University Press, 2016.

[115] Streeter S. Campana points and powerful values of norm forms. *Mathematische Zeitschrift*, 2021.

[116] Tao T. 254A, Notes 4: Some sieve theory. http://terrytao.wordpress.com/2015/01/21/254a-notes-4-some-sieve-theory/pas, 2015.

[117] Van Valckenborgh K. Squareful numbers in hyperplanes. *Algebra & Number Theory*, 6:1019–1041, 2012.

[118] Wang D. On the distribution of square-full integers. *Indian Journal of Pure and Applied Mathematics*, pages 1–8, 2021.

[119] Xiao H. Campana points on biequivariant compactifications of the Heisenberg group. *European Journal of Mathematics*, 8:205–246, 2022.

[120] Zhang Y. Bounded gaps between primes. *Annals of Mathematics*, pages 1121–1174, 2014.