Counting points on K3 surfaces and other arithmetic-geometric objects

Visse, H.D.

Counting points on K3 surfaces and other arithmetic-geometric objects

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof.mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op dinsdag 18 december 2018
klokke 10 uur

door

Hendrik Dick Visse

geboren te Zoetermeer

in 1989

promotor: dr. Ronald van Luijk
promotor: prof.dr. Peter Stevenhagen

Samenstelling van de promotiecommissie:

prof.dr. Aad van der Vaart (voorzitter; Universiteit Leiden)
prof.dr. Bart de Smit (secretaris; Universiteit Leiden)
prof.dr. Tim Browning (IST Austria / University of Bristol)
dr. Damaris Schindler (Universiteit Utrecht)
dr. Arne Smeets (Radboud Universiteit Nijmegen)

ISBN: 978-94-6323-412-2

Nothing will come of nothing

Lear, KING LEAR, Scene 1.1, line 82

Note about the epigraphs: the spelling of names, quoted line numbers, line breaks, interpunction, and exact wording are taken from [Sha08].

Contents

Introduction

O, for a muse of fire, that would ascend
The brightest heaven of invention

Chorus, Henry V, Prologue, lines 1-2

This thesis deals with three questions from arithmetic geometry. Even though it seems difficult to indicate one overarching topic, there do exist links between every pair of questions. Chapters 2 and 3 both deal with counting rational points, Chapters 2 and 4 are about K3 surfaces, and Chapters 3 and 4 both involve the concept of local solubility and obstructions to global solubility.

In Chapter 1 we give some necessary background from geometry and number theory that will allow us to study the topics in the later chapters. In particular, we give a quick treatment of the circle method, which is commonly used to address counting questions from geometry. When studying a polynomial $F \in \mathbb{Z}[X_1, \ldots, X_n]$, then the integral

$$\int_0^1 \exp(2\pi i \alpha F(\mathbf{x}))\mathrm{d}\alpha$$

tests if F has a zero at some point $\mathbf{x} \in \mathbb{Z}^n$. Indeed, since $F(\mathbf{x})$ is an integer, the integral evaluates to 0 unless $F(\mathbf{x}) = 0$ holds, in which case the integral equals 1. When for some bound B, we sum such integrals over all $\mathbf{x} \in (\mathbb{Z} \cap [-B, B])^n$, we may switch the order of the sum and the integral. The circle method describes a quite general way in which this integral can be approximated well enough so that we get valuable information out of it for large B. Moreover, this process generalizes to multiple polynomials. For now, it suffices to know that the main term will be a product of an integral (which should be easier to compute) and a series.

Chapter 2 is devoted to producing evidence towards a precise Manin type conjecture for K3 surfaces, predicting the number of rational points up

to bounded height. If $\mathbf{x} = (x_0 : \ldots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ is any point, we may arrange its coefficients so that each of the x_i is an integer, and the $(n+1)$-tuple has trivial greatest common divisor. If we do that, then we call $H(\mathbf{x}) = \max_i |x_i|$ the height of the point $\mathbf{x}$. A useful property is that for any given bound B, there are only finitely many points in $\mathbb{P}^n(\mathbb{Q})$ that have height at most B. The same is true for any subvariety of $\mathbb{P}^n_{\mathbb{Q}}$. Hence, for any given subvariety, we may count this number $N(B)$ of points for varying B. In the case of Fano varieties, Manin stated a rather general conjecture for the shape of $N(B)$, involving some geometric invariants. In particular, Manin's conjecture asks us to restrict ourselves to open subsets since there might exist so-called accumulating subvarieties. These may contain 'too many' rational points and we should ignore those. Many examples of Fano varieties have been studied in the literature, and at least for surfaces there are many examples where $N(B)$ involves a power of B and a power of $\log(B)$. The exponent of the logarithm is $\rho - 1$, where ρ is the rank of the Picard group of the variety.

Leaving the world of Fano varieties, we study diagonal quartic surfaces, which are examples of K3 surfaces, and we employ the circle method to count zeroes of the defining equation. Experts will immediately recognize that in this case the emergent error terms will exceed the desired main term. We focus on the main term and we speculate that there should be a connection between the error terms and accumulating subvarieties on the surface. Such behaviour has been observed in the literature for other types of varieties, but a detailed treatment supporting such speculation seems out of reach of our methods. The main result of this chapter gives heuristic support for hitherto unexplained data obtained in computer experiments by van Luijk some years ago. In particular we find that no power of B occurs and in contrast to the Fano varieties discussed above, that the power of $\log(B)$ ought to be ρ instead. Apart from this result, the approach to obtain these heuristics could be viewed as the main contribution of this chapter: we use averaging results of multiplicative functions to study the series coming out of the circle method, and we exploit the Tate conjecture to determine the exponent of the logarithm via the L-function of the surface. This gives $\rho - 1$ factors of $\log(B)$, while the last logarithm is obtained from the remaining factor that comes in the form of an integral.

Chapter 3 is joint work with Efthymios Sofos and concerns Serre's problem about fibrations. In the 1990s, Serre studied examples of conic bundles, where he looked at the number of fibres containing a rational point. More

precisely, he studied the number of rational points in the base up to a bounded height, say B, such that the fibres over these points contain a rational point themselves. Serre was only able to prove upper bounds, but for his specific examples it has since been shown that these upper bounds are in fact asymptotically correct. In recent years more examples of fibrations, not necessarily conic bundles, have been studied. Most notably, Loughran and Smeets have provided a framework into which results in this area should fit. Complete examples in the literature are rare, and our contribution lies in giving a wide class of conic bundles for which we can not only prove asymptotic results, but where we are also able to study the leading constant of such asymptotics. In particular, we look at bundles that can locally be described as follows. We take two polynomials f_1 and f_2 in n variables and of even degree d, subject to some more conditions that are outlined in Chapter 3. Now consider the variety $\mathcal{B}$ defined by $f_2(t_1, \dots, t_n) = 0$ as a subvariety of $\mathbb{P}^{n-1}_{\mathbb{Q}}$. Over the affine patch where we take $t_i = 1$, we define a conic bundle

$$\begin{aligned} x^2 + y^2 =& f_1(t_1, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_n) z^2, \\ & f_2(t_1, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_n) = 0. \end{aligned}$$

These bundles glue together into a conic bundle $\phi : X \to \mathcal{B}$. Now let $N(B)$ be the number of rational points of $\mathcal{B}$ up to height B, the fibre over which has a rational point itself. Then we prove that there is a constant c_ϕ such that we have

$$N(B) = c_\phi \frac{B^{n-d}}{(\log B)^{1/2}}$$

up to an error term with a logarithmic exponent slightly bigger than $1/2$. Moreover, our methods allow us to prove a Hasse principle on smooth fibres. To obtain our results, we use the circle method together with sieving techniques to study the series that appears. The conditions on the fibre in order for it to contain rational points appear through an indicator function detecting everywhere local solubility. Since our fibres are conics and therefore themselves satisfy the Hasse principle, this guarantees global solubility. Considerable effort goes into writing the leading constant c_ϕ as a product of recognizable factors, and we indicate how this fits conjectural expectations first described by Loughran.

It is known that the Hasse principle does not hold for K3 surfaces, and it has been conjectured that the Brauer–Manin obstruction has enough strength to explain this fact. In Chapter 4, which is written together with

Victoria Cantoral-Farfán, Yunqing Tang, and Sho Tanimoto, we study Brauer groups of Kummer surfaces. In particular, by a celebrated result of Skorobogatov and Zarhin we know that for any K3 surface over the field of rational numbers, its Brauer group (modulo constants) is finite. Our work gives explicit upper bounds for the size that this group may attain, at least when dealing with Kummer surfaces. For an abelian surface A over a number field k, with Kummer surface X, it is known that $\mathrm{Br}(\overline{A})$ and $\mathrm{Br}(\overline{X})$ are isomorphic as Galois modules, and we will bound the transcendental Brauer group $\mathrm{Br}(X)/\mathrm{Br}_1(X)$ as a subgroup of $\mathrm{Br}(\overline{X})^\Gamma$, where Γ denotes the absolute Galois group of k.

The proof of Skorobogatov and Zarhin's result relies on an exact sequence of cohomology groups, namely

$$\begin{aligned} 0 \to \left(\mathrm{NS}(\overline{A})/\ell^n\right)^\Gamma \xrightarrow{f_n} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma \to \mathrm{Br}(\overline{A})^\Gamma_{\ell^n} \to \\ \to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \xrightarrow{g_n} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})), \end{aligned}$$

where A is an abelian surface over a number field k, ℓ is a prime number, and the subscript ℓ^n indicates ℓ^n-torsion. We use this exact sequence and we study the cokernel of f_n and the kernel of g_n. Bounds on their sizes imply bounds on the size of $\mathrm{Br}(\overline{X})^\Gamma_{\ell^n}$, and we provide bounds independent of n. There are only finitely many ℓ for which such bounds are non-trivial, so we should also bound the size of such ℓ. This last point in particular relies on effective versions of Faltings' finiteness theorem for abelian varieties.

Although the existence of upper bounds like ours is not new, our methods have the advantage of being more explicit than those that were already known, especially for Kummer surfaces of minimal Picard rank. In particular, if one is given a curve C of genus 2 over a number field k, for which the Jacobian $\mathrm{Jac}(C)$ has Picard rank 1 and Faltings height h, let δ denote the discriminant of $\mathrm{NS}(X)$, where X is the Kummer surface of $\mathrm{Jac}(C)$. In order to obtain an upper bound for the transcendental part $\#\,\mathrm{Br}(X)/\mathrm{Br}_1(X)$, one needs only apply our formula with inputs $[k:\mathbb{Q}]$, h, and δ. Moreover, we prove that the algebraic part $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ has order at most 2. Although our bounds are explicit, they are unlikely to be sharp. We compute the example of the curve C given by

$$y^2 = x^6 + x^3 + x + 1.$$

The Brauer group of its associated Kummer surface turns out to have an order at most $2^{10} \cdot 10^{805050}$.

Chapter 1

Background

Though this be madness, yet there is a method in't

Polonius, HAMLET, Scene 2.2, line 207

1.1 Notation

Throughout this thesis, we will often use the font $\mathbf{x}$ as short-hand for either a tuple $(x_1, \ldots, x_n)$ or a collection of variables x_i where the range of i is to be understood.

For functions $f, g : \mathbb{R} \to \mathbb{R}$ we write

- $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$;
- $f(x) \sim g(x)$ if either $f(x) = g(x) = 0$ holds for all sufficiently large x, or $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$;

Somewhat differently, given a subset $R \subset \mathbb{R}^{m+n}$ and a function $f : R \to \mathbb{R}$, we write

$$f(s_1, \ldots, s_m, x_1, \ldots, x_n) = O_{s_1,\ldots,s_m}(g(s_1, \ldots, s_m, x_1, \ldots, x_n))$$

for some function $g : R \to \mathbb{R}_{\geq 0}$, or equivalently

$$f(x_1, \ldots, x_n) \ll_{s_1,\ldots,s_m} g(s_1, \ldots, s_m, x_1, \ldots, x_n),$$

if there exists a non-negative valued function C whose domain is the projection of R onto $\mathbb{R}^m$ given by its first m coordinates, such that for all $(s_1, \ldots, s_m, x_1, \ldots, x_n) \in R$ we have

$$|f(s_1, \ldots, s_m, x_1, \ldots, x_n)| \leq C(s_1, \ldots, s_m) g(s_1, \ldots, s_m, x_1, \ldots, x_n).$$

We will often think about $s_1, \dots, s_m$ as parameters and $x_1, \dots, x_n$ as variables. Hence by a slight abuse of language, any such C is called an implied constant.

When we write $f(\mathbf{s}, \mathbf{x}) = h(\mathbf{s}, \mathbf{x}) + O_{\mathbf{s}}(g(\mathbf{s}, \mathbf{x}))$, then this should be interpreted to mean $f(\mathbf{s}, \mathbf{x}) - h(\mathbf{s}, \mathbf{x}) = O_{\mathbf{s}}(g(\mathbf{s}, \mathbf{x}))$.

Furthermore, we will write $f(\mathbf{s}, \mathbf{x}) = \Theta_{\mathbf{s}}(g(\mathbf{s}, \mathbf{x}))$ or $f(\mathbf{s}, \mathbf{x}) \asymp_{\mathbf{s}} g(\mathbf{s}, \mathbf{x})$ if both $f(\mathbf{s}, \mathbf{x}) = O_{\mathbf{s}}(g(\mathbf{s}, \mathbf{x}))$ and $g(\mathbf{s}, \mathbf{x}) = O_{\mathbf{s}}(f(\mathbf{s}, \mathbf{x}))$ hold, possibly with different implied constants.

One should note that this notation $O(\ )$ differs in use from that of Landau or Bourbaki, but it is in line with the use in standard references like [IK04] or [MV07] and many papers in analytic number theory.

The notation $\mathbf{1}_A$ for some condition A will be used for the indicator symbol, that is $\mathbf{1}_A = 1$ if and only if the condition A holds, and $\mathbf{1}_A = 0$ otherwise.

1.2 Geometry and rational points

Since this thesis deals with number theory in a geometric context, we will need to recall a few concepts from geometry.

Definition 1.2.1. A *variety* is a separable scheme of finite type over a field. We call a variety *nice* if it is smooth, projective, and geometrically integral over its base field.

Definition 1.2.2. A *curve* is a variety of pure dimension 1. A *surface* is a variety of pure dimension 2.

Definition 1.2.3. If X is a nice variety and D and D' are two effective divisors, then we say that D and D' are linearly equivalent if there is an element f of the function field satisfying $\operatorname{div} f = D - D'$. The *Picard group* $\operatorname{Pic} X$ is the free abelian group of divisors on X divided out by linear equivalence.

In the definition above, the element f may be viewed as a rational map $X \to \mathbb{P}^1$, which will make D and D' fibres over two closed points (namely 0 and ∞). By applying an automorphism of $\mathbb{P}^1$, we may move 0 and ∞ to any other two different points. Hence we may generalize linear equivalence to what we call algebraic equivalence.

DEFINITION 1.2.4. Let X be a nice variety with two effective divisors D and D'. We call D and D' pre-algebraically equivalent if there exists a smooth curve C, two points x and x' on C, an effective divisor $\mathcal{D}$ on $X \times C$ with a flat morphism $f : \mathcal{D} \to C$ such that we have $D = f^{-1}(x)$ and $D' = f^{-1}(x')$. The equivalence relation generated by pre-algebraic equivalence is called *algebraic equivalence*. The group of divisors divided out by algebraic equivalence is the *Néron-Severi group* of X, denoted $\mathrm{NS}\, X$.

REMARK 1.2.5. Both $\mathrm{Pic}\, X$ and $\mathrm{NS}\, X$ are abelian groups by construction.

If X is a nice surface, then one can define a symmetric bilinear intersection pairing $(\ \cdot\ ) : \mathrm{Pic}\, X \times \mathrm{Pic}\, X \to \mathbb{Z}$ which further induces a pairing on $\mathrm{NS}\, X$. The Néron-Severi group of a nice surface is finitely generated and consequently has finite rank. Thus the pairing turns $\mathrm{NS}\, X$ into a lattice.

If X is a nice surface over $\mathbb{C}$, the Néron-Severi lattice $\mathrm{NS}\, X$ injects canonically into $\mathrm{H}^2(X, \mathbb{Z})$, which is a lattice by the cup product pairing. The lattice structures are compatible.

DEFINITION 1.2.6. For a nice surface X over $\mathbb{C}$, we call the orthogonal complement of $\mathrm{NS}\, X$ in $\mathrm{H}^2(X, \mathbb{Z})$ the *transcendental lattice* of X, denoted $T(X)$.

DEFINITION 1.2.7. For a nice surface X, we call the rank of its Néron-Severi lattice its *Picard rank* or sometimes *Néron–Severi rank*. We often denote this number by $\rho(X)$ or just ρ.

For a nice surface X, one may take a further quotient of $\mathrm{Pic}\, X$ by numerical equivalence, defined as follows.

DEFINITION 1.2.8. For a nice surface X, two line bundles $L, L' \in \mathrm{Pic}\, X$ are called *numerically equivalent* if for every line bundle L'' we have the equality $(L \cdot L'') = (L' \cdot L'')$. The quotient of $\mathrm{Pic}\, X$ by numerical equivalence is denoted $\mathrm{Num}\, X$.

Linear equivalence implies algebraic equivalence, which in its turn implies numerical equivalence, so by taking repeated quotients there are natural surjections

$$\mathrm{Pic}\, X \to \mathrm{NS}\, X \to \mathrm{Num}\, X.$$

1.2.1 K3 surfaces

Definition 1.2.9. A *K3 surface* is a nice surface X satisfying the following two properties:

- The canonical bundle ω_X is isomorphic to $\mathcal{O}_X$.
- The cohomology group $\mathrm{H}^1(X, \mathcal{O}_X)$ is trivial.

Example 1.2.10. We list a few basic examples of K3 surfaces:

- quartic surfaces in $\mathbb{P}^3$,
- double covers of $\mathbb{P}^2$ branched along a smooth sextic curve,
- the minimal resolution of the quotient of an abelian surface by the action of -1; these are called *Kummer surfaces*.

Proposition 1.2.11. *If X is a K3 surface, then the maps* $\operatorname{Pic} X \to \operatorname{NS} X$ *and* $\operatorname{NS} X \to \operatorname{Num} X$ *are isomorphisms and the intersection pairing on* $\operatorname{Pic} X$ *is even and non-degenerate and has signature* $(1, \rho(X) - 1)$.

Proof. This is [Huy16, Prop 1.2.4]. The proof almost entirely relies on the Riemann–Roch formula for surfaces and the Hodge index theorem. □

For a K3 surface X over $\mathbb{C}$, the cohomology group $\mathrm{H}^2(X, \mathbb{Z})$ has a Hodge structure as $\mathrm{H}^2(X, \mathbb{C}) \cong \mathrm{H}^{2,0} \oplus \mathrm{H}^{1,1} \oplus \mathrm{H}^{0,2}$, where we have written $\mathrm{H}^{p,q}$ for $\mathrm{H}^q(X, \Omega^p_{X/\mathbb{C}})$ and $\Omega_{X/\mathbb{C}}$ is the sheaf of Kähler differentials on X. These summands have dimensions 1, 20, and 1 respectively. The Lefschetz $(1,1)$-theorem assures that under the canonical embedding $\operatorname{NS} X$ lands in $\mathrm{H}^{1,1} \cap \mathrm{H}^2(X, \mathbb{Z})$. Thus the Picard rank of a K3 surface over a field of characteristic zero satisfies $1 \leq \rho(X) \leq 20$. In positive characteristic higher Picard ranks may be achieved, however still no higher than 22.

1.2.2 Manin's conjecture

Definition 1.2.12. Let $x = (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ be any point and for all coordinates assume $x_i \in \mathbb{Z}$ without loss of generality and further assume $\gcd(x_0, \ldots, x_n) = 1$. Then the *height* of x is $H(x) = \max_i |x_i|$.

Given a projective variety X over $\mathbb{Q}$ and a very ample divisor D on X we can embed X into some $\mathbb{P}^n_{\mathbb{Q}}$ using D. This induces a height function as in Definition 1.2.12 on the rational points of X, which depends on D and on

the specific set of global sections chosen to give the embedding. We write H_D for this height function.

DEFINITION 1.2.13. Let $U \subset X$ be an open subvariety of a variety X embedded in $\mathbb{P}^n_{\mathbb{Q}}$ via a very ample divisor D. We write

$$N_{U,D}(B) = \#\{x \in U(\mathbb{Q}) \mid H_D(x) \leq B\}.$$

REMARK 1.2.14. The number $N_{U,D}(B)$ is always finite. This is known as the Northcott property of the height H_D.

In the late 1980's, Manin stated a conjecture, first recorded in [FMT89], concerning the heights of rational points of Fano varieties. It was later extended most notably by Batyrev and Manin [BM90] and Peyre [Pey95].

Manin's original formulation is for Fano varieties. A smooth variety X is called Fano if its anticanonical divisor $-K_X$ is ample.

CONJECTURE 1.2.15 (Manin). *For any Fano variety X over $\mathbb{Q}$ of Picard rank ρ and with very ample anticanonical divisor $-K_X$, there exists an open subvariety $U \subset X$ and a non-negative constant c_X such that as $B \to \infty$ the following holds:*

$$N_{U,-K_X}(B) \sim c_X B \log(B)^{\rho-1}.$$

Refinements of this conjecture allow one to go beyond the case of Fano varieties, at the cost of some precision. For example, we have the following conjecture from [BM90].

CONJECTURE 1.2.16 (Batyrev–Manin). *For a K3 surface X over $\mathbb{Q}$, take $\varepsilon \in \mathbb{R}_{>0}$ and let D be a very ample divisor on X. Then there exists a non-empty Zariski open subvariety $U(\varepsilon) \subset X$ such that for $B \geq 1$ we have*

$$N_{U(\varepsilon),D}(B) = O_\varepsilon(B^\varepsilon).$$

McKinnon proved in [McK11] that Conjecture 1.2.16 follows from a powerful conjecture by Vojta. However, Conjecture 1.2.16 can be sharpened still. In Chapter 2 we will see heuristics for such a sharpening. In particular we will display evidence that for K3 surfaces the power of $\log B$ ought to be $\rho(X)$, in contrast to the case of Fano varieties. Here it must be noted that the evidence displayed in Chapter 2 matches well with computational data produced by van Luijk which can be found on his website [Lui].

In all of these conjectures, one is forced to take an open $U \subset X$ rather than state the conjecture just for X itself since X may contain so-called accumulating subvarieties. These are subvarieties of X that upon counting their rational points up to height B would give an asymptotic that dominates the expected main term in the Manin conjectures. It can be shown that embedded rational curves of degree d asymptotically contribute a constant multiple of $B^{2/d}$ to the counting, so for Fano varieties it is necessary to exclude embedded lines, by which we merely mean the cases $d = 1$. However, there are examples where leaving out a finite number of accumulating subvarieties is not enough, see for example the counterexample by Batyrev and Tschinkel in [BT96], where infinitely many subvarieties give the 'correct' exponent of B, but an exponent of $\log B$ that is too high. It is a topic of active research to find the correct modification of the conjectures to accommodate for these defects, see for example [Rud14], [Pey17], [Pey18], [LST18], or the overview article [LT18].

In the case of K3 surfaces, where the expected exponent of B is 0, the problems are even worse. Not only do embedded rational curves of any degree provide problems, so may embedded elliptic curves. For an elliptic curve E of Mordell–Weil rank r_E, it is a classical result by Néron that there is a contant c validating

$$N_E(B) \sim c(\log B)^{r_E/2},$$

see for example [Ser97, §4.5] where the constant c is also given. Hence if our heuristic is correct, every elliptic curve satisfying $r_E > 2\rho$ will need to be removed before counting rational points on the remainder. Here one quickly encounters an active research problem of an entirely different nature: since any elliptic curve on a K3 surface provides an elliptic fibration (this may be proven using the Riemann–Roch formula for surfaces), one is directed to the question how Mordell–Weil ranks vary in families of elliptic curves. However interesting these problems may be, we will not consider them in this thesis, and we leave the discussion here only for the sake of the interested reader.

One cannot discuss Conjecture 1.2.15 without mentioning the conjectural refinement obtained by Peyre [Pey95], with a small modification by Batyrev and Tschinkel [BT95]. In these papers, a geometric interpretation is given to the constant c_X: one should expect this constant to have the shape

$$c_X = \alpha(X)\beta(X) \lim_{s\to 1}(s-1)^\rho L(s) \prod_v \frac{\tau_v}{L_v(1)},$$

where $\alpha(X)$ measures the volume of some region in the cone spanned by effective divisors in the real vector space $\mathrm{NS}(X) \otimes \mathbb{R}$; the factor $\beta(X)$ equals the order of the finite group $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}\,\overline{X})$; for each place v of $\mathbb{Q}$ the τ_v are Tamagawa numbers, or otherwise put they are v-adic measures of the adèlic points of X; the numbers $L_v(1)$ are factors making the infinite product converge; and the limit balances out these convergence factors.

We will not include a detailed treatment of this conjectural constant, but while we were thinking about possible adaptations to the case of K3 surfaces, a point of confusion came up in several conversations with other researchers. We do want to address this quickly. The cohomology group $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}\,\overline{X})$ may be recognized as the algebraic Brauer group $\mathrm{Br}_1(X)/\mathrm{Br}(\mathbb{Q})$. For Fano varieties the algebraic part forms the entire Brauer group: there are no transcendental elements. Passing to K3 surfaces, transcendental elements may in fact exist, but it is known that the Brauer group is still finite. This was first proven in [SZ08], and it forms the basis for the work in Chapter 4. Based purely on this recognition one could guess that it is in fact $\#\,\mathrm{Br}(X)$ that should replace $\beta(X)$ in general. However, if one looks more closely at the available literature (for example in the very detailed paper by Salberger [Sal98]), one finds that $\mathrm{H}^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mathrm{Pic}\,\overline{X})$ also parametrizes so-called *universal torsors* over X, which may be applied when counting rational points on X. The connection to the (algebraic) Brauer group seems to be merely coincidental. Based on conjectures about Brauer–Manin obstructions to weak approximation on Fano varieties, some researchers seem to believe that the factor $\beta(X)$ should somehow measure the failure of weak approximation. Because the recognition of $\#\,\mathrm{Br}_1(X)/\mathrm{Br}(\mathbb{Q})$ in $\beta(X)$ seems coincidental to us, we believe that such an interpretation falls in the realm of wishful thinking. One should however note that in uncharted terrain, wishful thinking may be a guiding principle, and one should try and avoid negativity.

In light of Chapter 3, it is in order to make one final remark about Peyre's conjectural constant. In said chapter, we count points up to bounded height B in the base of a family of conics whose fibres have a rational point. Much of the work there involves studying the leading constant. As in Manin's conjectures, the asymptotic formula that we obtain contains a power of B and a power of $\log B$, albeit that the latter turns out to be fractional. It was first noticed by Loughran in [Lou13] that both asymptotic formulas look remarkably similar, up to and including the shape of

the leading constant. Loughran discusses a theoretical framework in which one should place the leading constant for this problem, and we compare our findings to his framework in §3.5.4.

1.2.3 L-functions of varieties

We will first define the zeta function of varieties over finite fields, before moving on to characteristic zero.

DEFINITION 1.2.17. Let X_p be a nice variety defined over $\mathbb{F}_p$. One defines the *zeta function* of X_p as

$$\zeta(X_p, T) = \exp\left(\sum_{m=1}^{\infty} \frac{\#X_p(\mathbb{F}_{p^m})}{m} T^m\right).$$

If X is a nice variety defined over $\mathbb{Q}$ such that X has a finite presentation model $\mathcal{X}$ over $\mathbb{Z}$, we write X_p for $\mathcal{X} \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}\mathbb{F}_p$. The further base change to $\mathbb{F}_q$ is denoted X_q and we write $\overline{X_p}$ for the base change to $\overline{\mathbb{F}_p}$. As per usual we write S for the (finite) set of primes p where X_p is not smooth.

There is a well-known connection between zeta functions of varieties and traces of Frobenius via the Lefschetz trace formula. For q a power of p, we write $\tau_{q,i,\ell}$ for $\operatorname{tr}\left(\operatorname{Frob}_q \mid \mathrm{H}^i_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)\right)$, $(\ell \neq p)$. The $\mathbb{F}_q$-rational points of X_p are the closed fixed points of $\operatorname{Frob}_q : \overline{X_p} \to \overline{X_p}$, and the Lefschetz trace formula gives

$$\#X_p(\mathbb{F}_q) = \sum_{i=0}^{2\dim X} (-1)^i \tau_{q,i,\ell}.$$

and this equality is independent of ℓ.

If we denote the eigenvalues of Frob_p on $\mathrm{H}^i_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)$ by α_{ij}, and write b_i for the dimension of $\mathrm{H}^i_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)$, then by the Lefschetz trace formula we have

$$\begin{aligned}\zeta(X_p, T) &= \prod_{i=0}^{2\dim X} \prod_{j=1}^{b_i} \exp\left((-1)^i \sum_{m=1}^{\infty} \frac{\alpha_{ij}^m T^m}{m}\right) \\ &= \prod_{i=0}^{2\dim X} \prod_{j=1}^{b_i} \exp\left((-1)^{i+1} \log(1-\alpha_{ij}T)\right) \\ &= \prod_{i=0}^{2\dim X} \prod_{j=1}^{b_i} (1-\alpha_{ij}T)^{(-1)^{i+1}}\end{aligned}$$

and hence

$$\zeta(X_p, T) = \prod_{i=0}^{2\dim X_p} \det\left(1 - \mathrm{Frob}_p T \mid \mathrm{H}^i_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}}. \tag{1.1}$$

So far, we have used the terminology of zeta functions, but from now on we want to switch over to the terminology of L-functions. In some sense there is no difference: the *L-function* of a variety in characteristic p is just its zeta function, but with the variable T replaced by p^{-s}. For varieties over $\mathbb{Q}$ as above we do this at every p-adic factor.

Definition 1.2.18. The *L-function* of X is defined via $\zeta(X_p, T)$ as

$$L(X, s) = \prod_{p \notin S} \zeta(X_p, p^{-s}),$$

where S is the set of bad primes.

Some authors prefer to extend the definition of $L(X, s)$ to include factors for every prime p, rather than only those not in S. In that case one refers to (1.1) but instead lets $1 - \mathrm{Frob}_p T$ act on the part of $\mathrm{H}^i_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)$ that is fixed by the inertia group at p. For $p \notin S$, this interia group acts trivially so there is no modification.

As for the zeta functions in (1.1), these L-functions break apart into factors, one for each i in the range $0 \le i \le 2\dim X$.

Definition 1.2.19. We will also write

$$L(\mathrm{H}^i(X), s) = \prod_{p \notin S} \det\left(1 - \mathrm{Frob}_p\, p^{-s} \mid \mathrm{H}^i_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}}$$

for the individual factors that make up $L(X, s)$, $i = 0, \ldots, 2\dim X$.

L-functions for K3 surfaces

If X is a K3 surface, the only non-trivial ℓ-adic étale cohomology occurs at $i = 0$, $i = 2$, and $i = 4$. The factor $L(\mathrm{H}^2(X), s)$ will be of importance in Chapter 2.

For K3 surfaces, we study the $L(\mathrm{H}^2(X), s)$ somewhat further. In [PSD91], it is explained that $L(\mathrm{H}^2(X), s)$ breaks apart into two multiplicative parts: one part $L'(\mathrm{H}^2(X), s)$ coming from the Néron-Severi lattice (over the algebraic closure), and the other $L''(\mathrm{H}^2(X), s)$ coming from the transcendental lattice. The first part itself breaks down as a product of shifted Riemann zeta functions $\zeta(s-1)$ and other similarly shifted Dirichlet L-series, coming from the Galois representation on the Néron-Severi lattice. The multiplicity of $\zeta(s-1)$ that occurs is equal to the rank of $\mathrm{NS}\, X$.

In the number theory part of this chapter we will mention a well-known and important property of Dirichlet L-series, namely Theorem 1.3.39. In the currect context, this theorem shows that only the factors $\zeta(s-1)$ contribute to the pole at $s = 2$ and consequently that the rank of $\mathrm{NS}\, X$ is equal to the order of the pole of $L'(\mathrm{H}^2(X), s)$ at $s = 2$. The same holds for the full $L(\mathrm{H}^2(X), s)$, provided that the factor $L''(\mathrm{H}^2(X), s)$ is analytic at $s = 2$. For diagonal quartic surfaces in particular, this was already studied, yet not fully proven, in [PSD91]. Their results are a special case of the following general principle of modularity, which we will not define, but whose consequence will be useful.

Over some extension of the base field, every diagonal quartic surface is isomorphic to the Fermat quartic $x_1^4 + x_2^4 + x_3^4 + x_4^4 = 0$. This surface is known to have maximal Picard rank 20 over $\overline{\mathbb{Q}}$. K3 surfaces with geometric Picard rank 20 are called *singular K3 surfaces* where the word singular is not to be confused with the negation of non-singular or smooth. Livné proved the following important theorem.

THEOREM 1.2.20 (Livné). *Every singular K3 surfaces X over $\mathbb{Q}$ is modular. The 2-dimensional Galois representation defined by the transcendental lattice $T(X)$ has an associated modular form that is a Hecke eigenform of weight 3 with complex multiplication by $\mathbb{Q}(\sqrt{-\operatorname{disc}(\mathrm{NS}\, X)})$.*

Proof. This is proven in [Liv95]. □

Hecke eigenforms with complex multiplication are in particular holomorphic cusp forms and Hecke proved that L-functions of modular forms are

well-behaved in many regards. In particular we have the following theorem.

THEOREM 1.2.21 (Hecke). *The L-function $L(f,s)$ of a modular form f of weight k has a meromorphic continuation to the whole complex plane and satisfies a functional equation. Moreover, $L(f,s)$ is entire if f is a holomorphic cusp form, and otherwise it has only a simple pole at $s=k$.*

Proof. This is [IK04, Theorem 14.7]. □

REMARK 1.2.22. None of this should come as a surprise. In his excellently written [Tat65], Tate repeats his conjecture that relates the Picard rank of a variety to the order of the accociated pole of $L(\mathrm{H}^2(X),s)$. For K3 surfaces, the full Tate conjectures are now known through work of André [And96] and Tankeev [Tan88] in characteristic zero, in odd characteristic by work of many people, among them Nygaard and Ogus [NO85], Maulik [Mau14], Charles [Cha13], and Madapusi Pera [MP15], and finally in characteristic 2 by Kim and Madapusi Pera [KMP16].

In preparation of this thesis, a point of confusion came up relating to this. It may be useful to spend a few words in order to make sure that the reader does not fall victim to the same fate.

If X_p is a nice surface over $\mathbb{F}_p$, then the Tate conjecture says that for $L(\mathrm{H}^2(X_p),s)$ the order of the pole at $s=1$ equals the Picard rank of X_p. Indeed, if the rank is ρ, then there will be at least ρ eigenvalues among the α_{2j} that are exactly p. These correspond to the eigenvalues 1 on the twisted cohomology group $\mathrm{H}^2_{\text{ét}}(\overline{X_p},\mathbb{Q}_\ell(1))$. Conjecturally these are all of them.

Now let X be a nice surface over $\mathbb{Q}$ with good reduction X_p at p. Then the p-adic factor of $L(\mathrm{H}^2(X),s)$ should have a pole of order $\rho(X_p)$ at $s=1$. And this should be true for every other prime of good reduction as well. Are we multiplying infinitely many poles? But that would not give a meromorphic function! This is where one may get confused, so let us review the argument closely. The Tate conjecture in characteristic 0 says that $L(\mathrm{H}^2(X),s)$ has a pole at $s=2$, since every nice surface has positive Picard rank. Around $s=1$ the L-function $L(\mathrm{H}^2(X),s)$ is defined, but only through some abstract analytic continuation. The point here is that in this region the function is no longer defined by a product over all good primes as in Definition 1.2.18; we are not multiplying together infinitely many poles.

Let us consider an easy example: $X = \mathbb{P}^n_{\mathbb{Q}}$. We have $\operatorname{Pic} X \cong \mathbb{Z}$. It is not difficult to derive $L(\mathrm{H}^2(X), s) = \zeta(s-1)$, where ζ denotes the Riemann zeta function. Indeed this function has a pole of order 1 at $s = 2$, and value $-\frac{1}{2}$ at $s = 1$.

1.3 Number theory and solving equations

In this section we will collect some results from number theory, in particular we will mostly discuss the circle method, which is to be used to count rational or integral solutions to polynomial equations. Before we set off, we will mention a few results which will come up several times.

THEOREM 1.3.1 (Abel's summation formula). *Let $(a_n)_n$ be a sequence of complex numbers and let $\phi : \mathbb{R}_{>0} \to \mathbb{R}$ be differentiable with continuous derivative. For any $x \in \mathbb{R}_{\geq 1}$, write $A(x) = \sum_{1 \leq n \leq x} a_n$. Then for all $1 \leq y < x$ the following equation holds:*

$$\sum_{y < n \leq x} a_n \phi(n) = A(x)\phi(x) - A(y)\phi(y) - \int_y^x A(t)\phi'(t)\mathrm{d}t.$$

Proof. This is [Apo76, Theorem 4.2]. □

We also record the famous Prime Number Theorem here, mostly because a high brow proof of it will be a guide for the methods in §2.2, but secondarily also since its statement will briely occur in combination with Abel's summation formula in that same section.

THEOREM 1.3.2 (Prime Number Theorem). *Let $\pi(x)$ denote the number of primes up to x. The function $\pi(x)$ satisfies*

$$\pi(x) \sim \frac{x}{\log x}.$$

Proof. This well-celebrated theorem can be found in almost any book on analytic number theory. For example see [IK04, Chapter 2] or [MV07, Chapter 6]. □

1.3.1 The circle method

In this subsection we give a treatment of the basics of the circle method. The reader wishing to learn more is adviced to read for example [Bro09], [Dav05], or [IK04]. The circle method was first developed by Hardy and Ramanujan to study partitions of numbers, and later adapted to study zeroes of polynomials over $\mathbb{Z}$.

Let $F(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ be a homogeneous polynomial of degree d in n variables. The goal for which the circle method is commonly applied is to count integral zeroes of F in some bounded box $\mathcal{B} = [-B, B]^n$.

The starting point of the method is the following indicator integral, where $\mathbf{x}$ is an integer vector:

$$\int_0^1 e\left(\alpha F(\mathbf{x})\right) \mathrm{d}\alpha = \begin{cases} 1 \text{ if } F(\mathbf{x}) = 0, \\ 0 \text{ otherwise,} \end{cases}$$

where we have written $e(z)$, and will continue to do so, when we mean $\exp(2\pi i z)$.

Definition 1.3.3. We write $N_F(B)$ for the number of integral zeroes of F in the region $\mathcal{B}$.

By applying the above indicator integral, we have

$$\begin{aligned} N_F(B) &= \sum_{\mathbf{x} \in \mathbb{Z}^n \cap \mathcal{B}} \int_0^1 e\left(\alpha F(\mathbf{x})\right) \mathrm{d}\alpha \\ &= \int_0^1 \sum_{\mathbf{x} \in \mathbb{Z}^n \cap \mathcal{B}} e\left(\alpha F(\mathbf{x})\right) \mathrm{d}\alpha. \end{aligned}$$

Notice that switching the sum and the integral is allowed because the sum is over a finite set.

Without applying any machinery to study this integral expression, one may very intuitively guess that the number $N_F(B)$ should behave as $O\left(B^{n-d}\right)$ because of the following argument. When we vary $\mathbf{x}$ over $\mathbb{Z}^n \cap \mathcal{B}$, the function $F(\mathbf{x})$ takes values in an interval of length $\ell = \Theta(B^d)$ with implied constants depending on n and the coefficients of F. One might guess that each integer value in the range is reached approximately equally often, in particular the occurrence $F(\mathbf{x}) = 0$ happens at a fraction ℓ^{-1} among all $O(B^n)$ possible instances. We will see that the circle method, when it

applies, will indeed provide this exponent $n-d$ of B, combined with more detailed information, such as additional logarithmic factors.

The method assumes that the main contributions to the integral occur around numbers α that are well approximated by rational numbers with small denominator, and according to this philosophy divides the range of integration up into segments centred around these well-approximable numbers. Figure 1.1 shows a sketch of the modulus of $\sum_{x\in\mathbb{Z}\cap[-10,10]} e(\alpha F(x))$ for a simple polynomial $F(x) = x^4$. Although the plot does not indicate whether this philosophy makes sense, at least it is clear that the value of the function shows quite erratic behaviour.

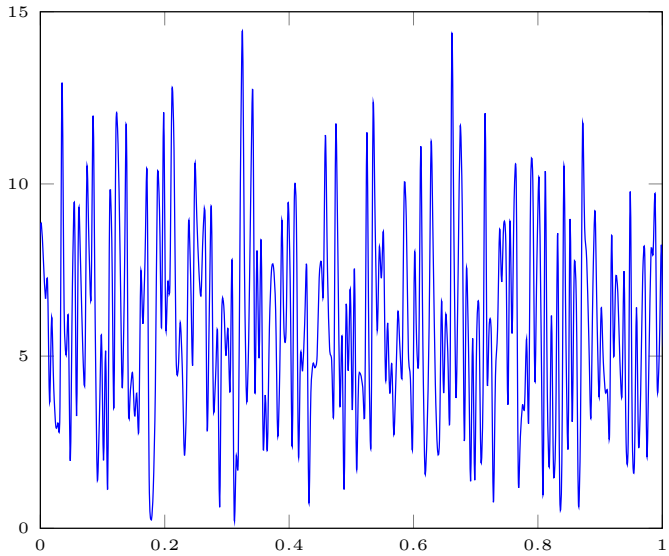

Figure 1.1: Plot of the modulus $\left|\sum_{x\in\mathbb{Z}\cap[-10,10]} e(\alpha x^4)\right|$ for $\alpha \in [0,1]$.

We let δ be a small parameter which will stay free to be chosen later and write $Q = B^\delta$.

Definition 1.3.4. For $a, q \in \mathbb{Z}$ coprime satisfying $1 \le a \le q \le Q$, we call the interval $\mathfrak{M}_{q,a}(\delta) = \left[\frac{a}{q} - B^{-d+\delta}, \frac{a}{q} + B^{-d+\delta}\right]$ the *major arc centred at* $\frac{a}{q}$. We write $\mathfrak{M}(\delta)$ for the union of major arcs and $\mathfrak{m}(\delta) = [0,1] \setminus \mathfrak{M}(\delta)$ for its complement, called the *minor arc*.

LEMMA 1.3.5. *For $\delta < \frac{d}{3}$ and $B > 2^{\frac{1}{d-3\delta}}$ different major arcs do not overlap.*

Proof. This is [Bro09, Lemma 8.3] We take two centres $\frac{a}{q}$ and $\frac{a'}{q'}$ of different major arcs and consider the difference $D := |\frac{a}{q} - \frac{a'}{q'}|$. Using $\frac{a}{q} \neq \frac{a'}{q'}$ in the shape $|aq' - a'q| \geq 1$, we find $D \geq \frac{1}{B^{2\delta}}$. On the other hand, the triangle inequality with a supposed midpoint in the intersection of these two major arcs shows $D \leq 2B^{-d+\delta}$. This is in contradiction with the quoted values for δ and B. □

We now want to study the behaviour of the integrand $\sum_{\mathbf{x}\in\mathbb{Z}^n\cap\mathcal{B}} e(\alpha F(\mathbf{x}))$ in a certain major arc $\mathfrak{M}_{q,a}$. We write $\alpha = \frac{a}{q} + \theta$ and we split the exponential. Realizing that $e\left(\frac{a}{q}F(\mathbf{x})\right)$ as a function of $\mathbf{x}$ is periodic modulo q, we find

$$\sum_{\mathbf{x}\in\mathbb{Z}^n\cap\mathcal{B}} e(\alpha F(\mathbf{x})) = \sum_{\mathbf{u}\in(\mathbb{Z}/q\mathbb{Z})^n} \left(e\left(\tfrac{a}{q}F(\mathbf{u})\right) \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\cap\mathcal{B} \\ \mathbf{x}\equiv\mathbf{u}(\mathrm{mod}\ q)}} e(\theta F(\mathbf{x})) \right). \quad (1.2)$$

DEFINITION 1.3.6. We write

$$I(t) = \int_{[-1,1]^n} e(tF(\mathbf{x}))\mathrm{d}\mathbf{x}.$$

Notice that the integral $I(\theta)$ only depends on F.

LEMMA 1.3.7. *For $1 \leq a \leq q \leq B$ with $\gcd(a,q) = 1$, and $\alpha = \frac{a}{q} + \theta$ we have*

$$\sum_{\mathbf{x}\in\mathbb{Z}^n\cap\mathcal{B}} e\left(\alpha F(\mathbf{x})\right) = \left(\tfrac{B}{q}\right)^n \left(\sum_{\mathbf{u}\in(\mathbb{Z}/q\mathbb{Z})^n} e\left(\tfrac{a}{q}F(\mathbf{u})\right) \right) \cdot I(\theta B^d) + O\left(qB^{n-1}(1+|\theta|B^d)\right).$$

Proof. This is [Bro09, Lemma 8.2]. Its proof relies on showing that the expression $\sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\cap\mathcal{B} \\ \mathbf{x}\equiv\mathbf{u}(\mathrm{mod}\ q)}} e(\theta F(\mathbf{x}))$ that appears in (1.2) is in fact independent of $\mathbf{u}$ and can be approximated by the quoted integral. □

This process can be applied for every major arc, or in other words for every $1 \leq q \leq Q$ and every $a \in (\mathbb{Z}/q\mathbb{Z})^\times$, provided $Q \leq B$ or equivalently $\delta \leq 1$ hold. Changing variables within the integral over any major arc

$$\int_{-B^{-d+\delta}}^{B^{-d+\delta}} I(\theta B^d)\mathrm{d}\theta = B^{-d}\int_{-B^\delta}^{B^\delta} I(\theta')\mathrm{d}\theta',$$

for sufficently small δ and large B, that is as in Lemma 1.3.5, we finally arrive at

$$\begin{aligned} N_F(B) = B^{n-d}\mathfrak{J}(Q)\sum_{q=1}^{Q}\frac{1}{q^n}\sum_{a\in(\mathbb{Z}/q\mathbb{Z})^\times}\sum_{\mathbf{u}\in(\mathbb{Z}/q\mathbb{Z})^n} e\left(\tfrac{a}{q}F(\mathbf{u})\right) \\ + \int_{\mathfrak{m}}\sum_{\mathbf{x}\in\mathbb{Z}^n\cap\mathcal{B}} e\left(\alpha F(\mathbf{x})\right)\mathrm{d}\alpha + E \end{aligned} \tag{1.3}$$

with

$$\mathfrak{J}(R) = \int_{-R}^{R} I(\theta)\mathrm{d}\theta = \int_{-R}^{R}\int_{[-1,1]^n} e(\theta F(\mathbf{x}))\mathrm{d}\mathbf{x}\mathrm{d}\theta,$$

and where the error E comes from integrating the error term in Lemma 1.3.7 over the range $\theta \in (-B^{-d+\delta}, B^{-d+\delta})$ and afterwards summing over $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ and $1 \leq q \leq Q = B^\delta$. It satisfies

$$E = O\left(B^{n-1-d+5\delta}\right).$$

Remark 1.3.8. In order to avoid the possibility of the error term E dominating, one should pick δ to satisfy $\delta < \frac{1}{5}$, rather than merely $\delta < \frac{d}{3}$ as suggested by Lemma 1.3.5. From now on, we will always assume that the error E is asymptotically small.

Definition 1.3.9. It is convenient to name some parts of the expression (1.3). We introduce the following notation:

- $S_{q,a} = \sum_{\mathbf{u}\in(\mathbb{Z}/q\mathbb{Z})^n} e\left(\frac{a}{q}F(\mathbf{u})\right)$,
- $S_q = \sum_{a\in(\mathbb{Z}/q\mathbb{Z})^\times} S_{q,a}$,
- $\mathfrak{S}(Q) = \sum_{q=1}^{Q}\frac{1}{q^n}S_q$.

We call the expression $B^{n-d}\mathfrak{J}(Q)\mathfrak{S}(Q)$ the *contribution from the major arcs*. The integral $\mathfrak{J}(Q)$ is called *the singular integral*, and the sum $\mathfrak{S}(Q)$ is named *the singular series*.

In many applications the singular integral converges for $R \to \infty$, and therefore is approximated by the same integral but with the range of integration stretched out to the whole real line.

REMARK 1.3.10. In the application of Chapter 2, the singular integral actually does not converge.

People say that "the circle method works" when one can prove that the major arcs give the main contribution to $N_F(B)$ and the minor arcs give an error term which is smaller, at least asymptotically. This usually needs n to be rather big compared to d. A naive probabilistic reasoning indicates how big n should be compared to d. For fixed $\alpha \in \mathfrak{m}(\delta)$ one may think that the values of $e(\alpha F(\mathbf{x}))$ will be randomly distributed over the unit circle when ranging over all $\mathbf{x} \in [-B, B]^n \cap \mathbb{Z}^n$. We are interested in their sum and the central limit theorem suggests that the absolute value of this sum will tend to $\sqrt{\#([-B, B]^n \cap \mathbb{Z}^n)} \sim (2B)^{n/2}$. On the other hand, the exponent of B appearing in equation (1.3), arising from the major arcs, is $n - d$ as usually the singular integral and singular series converge for $Q \to \infty$. Hence we expect to need $n > 2d$ variables for the circle method to work. In reality however, one often needs many more variables than suggested by this heuristic lower bound.

LEMMA 1.3.11. *As a function in q, the symbol S_q is multiplicative.*

Proof. This proof is taken from [Dav05, Lemma 5.1], adapted to our situation. If q_1 and q_2 are coprime, write $q = q_1 q_2$ and

$$a \equiv a_1 q_2 + a_2 q_1 \,(\mathrm{mod}\ q) \tag{1.4}$$

for any $a \in (\mathbb{Z}/q\mathbb{Z})^\times$. It suffices to prove the validity of $S_{q,a} = S_{q_1,a_1} S_{q_2,a_2}$ since the Chinese Remainder Theorem gives a group isomorphism between $(\mathbb{Z}/q\mathbb{Z})^\times$ and $(\mathbb{Z}/q_1\mathbb{Z})^\times \times (\mathbb{Z}/q_2\mathbb{Z})^\times$, yielding

$$S_q = \sum_{a \in (\mathbb{Z}/q\mathbb{Z})^\times} S_{q,a} = \left(\sum_{a_1 \in (\mathbb{Z}/q_1\mathbb{Z})^\times} S_{q_1,a_1} \right) \left(\sum_{a_2 \in (\mathbb{Z}/q_2\mathbb{Z})^\times} S_{q_2,a_2} \right) = S_{q_1} S_{q_2}.$$

Similarly, using the Chinese Remainder Theorem in its more general statement about the rings $\mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z}$, we may uniquely write any $u \in \mathbb{Z}/q\mathbb{Z}$ as

$$u \equiv q_2 u_1 + q_1 u_2 \,(\mathrm{mod}\ q)\,,$$

where no assumption of coprimality between the u_i and q_i is present. We have

$$\begin{aligned} S_{q,a} &= \sum_{\mathbf{u}\in(\mathbb{Z}/q\mathbb{Z})^n} e\left(\frac{a}{q}F(\mathbf{u})\right) \\ &= \sum_{\mathbf{u}_1\in(\mathbb{Z}/q_1\mathbb{Z})^n}\sum_{\mathbf{u}_2\in(\mathbb{Z}/q_2\mathbb{Z})^n} e\left(\frac{a}{q}F\left(q_2\mathbf{u}_1+q_1\mathbf{u}_2\right)\right). \end{aligned}$$

Since the congruence $aF(\mathbf{u}) \equiv q_2a_1F(q_2\mathbf{u}_1) + q_1a_2F(q_1\mathbf{u}_2)$ holds modulo q_1 and q_2, so does it modulo q. Upon division by q we conclude

$$\frac{a}{q}F(\mathbf{u}) \equiv \frac{a_1}{q_1}F(q_2\mathbf{u}_1) + \frac{a_2}{q_2}F(q_1\mathbf{u}_2) \,(\mathrm{mod}\ 1)\,.$$

Hence we arrive at

$$S_{q,a} = \sum_{\mathbf{u}_1\in(\mathbb{Z}/q_1\mathbb{Z})^n} e\left(\frac{a_1}{q_1}F(\mathbf{u_1}q_2)\right)\sum_{\mathbf{u}_2\in(\mathbb{Z}/q_2\mathbb{Z})^n} e\left(\frac{a_2}{q_2}F(\mathbf{u_2}q_1)\right) = S_{q_1,a_1}S_{q_2,a_2},$$

where in the last step we have renumbered the summation ranges, using that q_2 is invertible in $\mathbb{Z}/q_1\mathbb{Z}$ and vice versa. As announced earlier in the proof, this validates the statement of the lemma. □

With S_q being a multiplicative function, it is determined by its values at prime powers. These values themselves are closely related to zeroes of $F(\mathbf{x})$ modulo corresponding prime powers, according to the following lemma.

LEMMA 1.3.12. *Writing* $N(p^k) = \#\{\mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n \mid F(\mathbf{x}) \equiv 0 \,(\mathrm{mod}\ p^k)\}$, *the following is valid for any prime* p *and* $k \geq 1$*:*

$$S_{p^k} = p^kN(p^k) - p^{n+k-1}N(p^{k-1}).$$

Proof. By definition we have

$$S_{p^k} = \sum_{a\in(\mathbb{Z}/p^k\mathbb{Z})^\times}\sum_{\mathbf{u}\in(\mathbb{Z}/p^k\mathbb{Z})^n} e\left(\frac{a}{p^k}F(\mathbf{u})\right)$$

and we start the proof by switching the two summations.

We recognize $\sum_{a\in(\mathbb{Z}/q\mathbb{Z})^\times} e\left(\frac{a}{q}n\right)$ as the Ramanujan sum $c_q(n)$ with the properties:

$$c_{p^k}(n) = \begin{cases} 0 & \text{if } p^{k-1} \nmid n, \\ -p^{k-1} & \text{if } p^{k-1} | n \text{ and } p^k \nmid n, \\ \phi(p^k) & \text{if } p^k | n \end{cases}$$

for any prime p and $k \geq 1$.

We count the number of times that the second and third cases occur and we find

$$\begin{aligned} S_{p^k} &= \sum_{\mathbf{u}\in(\mathbb{Z}/p^k\mathbb{Z})^n} c_{p^k}(F(\mathbf{u})) \\ &= (-p^{k-1})\left(p^n N(p^{k-1}) - N(p^k)\right) + \varphi(p^k)N(p^k) \\ &= p^k N(p^k) - p^{n+k-1}N(p^{k-1}), \end{aligned}$$

where we have made use of the equality $\varphi(p^k) = (p-1)p^{k-1}$. □

1.3.2 From affine to projective solutions

For many geometric applications, we are interested in rational points of projective, rather than affine, varieties. The circle method can still be a helpful tool, and it hardly needs modification.

Let $F(\mathbf{x}) \in \mathbb{Q}[\mathbf{x}]$ be a homogeneous polynomial and $X \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ its zero locus. Any rational point $P \in X(\mathbb{Q})$ can be written such that its coordinates lie in $\mathbb{Z}$ and are collectively coprime. Hence counting rational points up to height B (as in Definition 1.2.12) is equivalent to counting affine integral solutions of $F(\mathbf{x}) = 0$ under the condition $\gcd(x_1, \ldots, x_n) = 1$ and choosing the sign of $\mathbf{x}$.

Definition 1.3.13. We write $\mathbb{Z}^n_{\text{prim}}$ for $\{\mathbf{x} \in \mathbb{Z}^n \mid \gcd(x_1, \ldots, x_n) = 1\}$.

Definition 1.3.14. The *Möbius function* is the multiplicative function μ defined by

$$\mu(p^k) = \begin{cases} 1 & \text{if } k = 0; \\ -1 & \text{if } k = 1; \\ 0 & \text{if } k > 1. \end{cases}$$

The most important property of the Möbius function is captured by the relation

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise,} \end{cases}$$

where we only sum over positive divisors. This relation and its consequences are commonly known as *Möbius inversion*. One of such consequences is the following lemma, where for $0 \neq \mathbf{x} \in \mathbb{Z}^n$ we have written $H(\mathbf{x}) = \max |x_i|$, and $H(0) = \infty$.

LEMMA 1.3.15. *For any homogeneous $F \in \mathbb{Q}[\mathbf{x}]$ we have the equality*

$$\begin{aligned} &\#\{\mathbf{x} \in \mathbb{Z}^n_{\text{prim}} \mid F(\mathbf{x}) = 0, H(\mathbf{x}) \leq B\} \\ &= \sum_{k=1}^{\infty} \mu(k) \#\{\mathbf{x} \in \mathbb{Z}^n \mid F(\mathbf{x}) = 0, H(\mathbf{x}) \leq B, k|\mathbf{x}\}, \end{aligned} \tag{1.5}$$

where $k|\mathbf{x}$ means that k divides every x_i. Equivalently, writing X for the zero locus of F inside $\mathbb{P}^{n-1}_{\mathbb{Q}}$, we have

$$\#\{x \in X(\mathbb{Q}) \mid H(x) \leq B\} = \frac{1}{2} \sum_{i=1}^{\infty} \mu(k) N_F(B/k).$$

Proof. The condition $\mathbf{x} \in \mathbb{Z}^n_{\text{prim}}$ means that the x_i, $i = 1, \ldots, n$ have no non-trivial joint divisor, or put differently: $\sum_{k|\gcd(\mathbf{x})} \mu(k) = 1$. We use the symbol I for the indicator function with domain $\mathbb{Z}^n$ on the joint condition $F(\mathbf{x}) = 0 \vee H(\mathbf{x}) \leq B$. The left-hand side of (1.5) becomes

$$\sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ \gcd(\mathbf{x}) = 1}} I(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{Z}^n} \sum_{k|\gcd(\mathbf{x})} \mu(k) I(\mathbf{x}) = \sum_{\mathbf{x} \in \mathbb{Z}^{n-1}} \sum_{k|\gcd(\mathbf{x})} \mu(k) \sum_{x_n \in k\mathbb{Z}} I(\mathbf{x}),$$

which after performing this last step for every x_i, turns into

$$\sum_{k=1}^{\infty} \mu(k) \#\{\mathbf{x} \in \mathbb{Z}^n \mid F(\mathbf{x}) = 0, H(\mathbf{x}) \leq B, k|\mathbf{x}\}.$$

Clearly the left-hand side of (1.5) equals $2\#\{x \in X(\mathbb{Q}) \mid H(x) \leq B\}$, the extra factor of 2 coming from choosing the sign of $\mathbf{x}$. By changing variables $\mathbf{x} = k\mathbf{y}$, we may write the right-hand side of (1.5) as

$$\sum_{k=1}^{\infty} \mu(k) \#\{\mathbf{y} \in \mathbb{Z}^n \mid F(\mathbf{y}) = 0, H(\mathbf{y}) \leq B/k\}$$

and invoke the definition of $N_F(B/k)$. □

REMARK 1.3.16. This is the modification that was announced at the beginning of the current subsection. It allows us to use the circle method to count rational points of a projective variety. It is important to remark that the sum over k is actually a finite sum for any given B. Indeed, every term from $k > B$ onwards will be zero.

In the last chapter of his book [Bro09], Browning uses the circle method to produce a heuristic for diagonal cubic surfaces. In turning from counting points on the affine cone to points on the surfaces themselves, he runs into the same problem as we do, which we will now explain.

Counting integral solutions using the circle method, one arrives at

$$N_X(B) = B^{n-d} \sum_{k=1}^{\infty} \frac{\mu(k)}{k^{n-d}} \mathfrak{J}((B/k)^\delta)\mathfrak{S}((B/k)^\delta) + \text{error}.$$

One would hope that the coprimality conditions merely add a factor of $(1 - \frac{1}{p})$ for every prime p, and if the circle method produces an exponent of B that satisfies $n - d > 1$ and if $\mathfrak{J}$ and $\mathfrak{S}$ converge, then based on the formula $\sum_{k=1}^{\infty} \frac{\mu(k)}{k^\alpha} = \zeta(\alpha)^{-1}$ for $\alpha > 1$ it can be proven that the displayed sum equals $B^{n-d}\mathfrak{J}\mathfrak{S}^*$, where $\mathfrak{S}^*(Q)$ is defined as follows.

DEFINITION 1.3.17. The *modified singular series*, denoted by $\mathfrak{S}^*(Q)$, is $\sum_{1 \le q \le Q} q^{-n} S_q^*$, with the modification

$$S_q^* = \sum_{\substack{1 \le a \le q \\ \gcd(a,q)=1}} \sum_{\substack{\mathbf{u} \in (\mathbb{Z}/q\mathbb{Z})^n \\ \gcd(\mathbf{u},q)=1}} e\left(\frac{a}{q} F(\mathbf{u})\right).$$

The only difference with Definition 1.3.9 is the appearance of the requirement $\gcd(\mathbf{u}, q) = 1$ in the summation.

For $n - d \le 1$ we shall have to assume that this replacement may be executed and we will work with $\mathfrak{S}^*(Q)$ instead of $\mathfrak{S}(Q)$. The main reason for doing so is that Corollary 1.3.22 does not hold for the S_q.

The modified S_q^* share many properties of S_q. In particular we have the following.

LEMMA 1.3.18. *As a function in q the symbol S_q^* is multiplicative and for every $k \ge 1$ and every prime p we have*

$$S_{p^k}^* = p^k N^*(p^k) - p^{n+k-1} N^*(p^{k-1})$$

where

$$N^*(q) = \#\{\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n \mid F(\mathbf{x}) \equiv 0 \,(\mathrm{mod}\ q)\,, \gcd(\mathbf{x}, q) = 1\}$$

is modified from $N(q)$ again with a gcd *requirement.*

Proof. The proofs of these two properties are mutatis mutandis the same as the proofs of Lemmas 1.3.11 and 1.3.12. □

The modified S_q^* however also satisfy a very useful property that we will study now.

LEMMA 1.3.19 (Quantitative Hensel). *Let $F = \sum_{i=1}^n a_i x_i^d \in \mathbb{Z}[\mathbf{x}]$ define a smooth projective subvariety of $\mathbb{P}^{n-1}_{\mathbb{Q}}$. Let p be a prime and denote $v_p = \mathrm{ord}_p(d) + \max_i \mathrm{ord}_p(a_i)$. With notation as in Lemma 1.3.18, any $k \geq 2v_p + 2$ validates*

$$N^*(p^k) = p^{n-1} N^*(p^{k-1}).$$

Proof. We apply Hensel's lemma in its shape as in [Bou06, Ch. III, §4.5, Corollaire 1, p. 269]. In the notation of Bourbaki, we work in the ring $A = \mathbb{Z}_p$ with ideal $\mathfrak{m} = p\mathbb{Z}_p$. Let $\mathbf{b} \in (\mathbb{Z}_p/p^{k-1}\mathbb{Z}_p)^n$ be a primitive solution to $F(\mathbf{b}) \equiv 0 \left(\mathrm{mod}\ p^{k-1}\right)$. Without loss of generality assume $b_n \notin p\mathbb{Z}_p$. For every $1 \leq i \leq n-1$ let $b_i' \in \mathbb{Z}_p$ be any lift of b_i modulo p^{k-1}. Then $F(b_1', \ldots, b_{n-1}', x_n) =: G(x_n)$ is a polynomial in the single variable x_n. Write $e := G'(b_n) = da_n(b_n)^{d-1}$. We have

$$\mathrm{ord}_p(e^2) = 2\,\mathrm{ord}_p(da_n) \leq 2v_p \leq k-2.$$

This ensures $e^2 p\mathbb{Z}_p \supset p^{k-1}\mathbb{Z}_p$ and we have $G(b_n) \equiv 0 \left(\mathrm{mod}\ e^2 p\right)$. This is precisely the setup of Corollaire cited above, which yields that there exists a unique $c \in \mathbb{Z}_p$ satisfying both the equality $G(c) = 0$ and $c \equiv b_n \,(\mathrm{mod}\ ep)$. We conclude that while for $1 \leq i \leq n-1$ we may lift b_i to $\mathbb{Z}_p/p^k\mathbb{Z}_p$ in any way we like, afterwards the lift of b_n is fixed. Hence every element counted by $N^*(p^{k-1})$ lifts to p^{n-1} elements counted by $N^*(p^k)$. □

DEFINITION 1.3.20. Given a homogeneous polynomial $F(x_1, \ldots, x_n)$ with integer coefficients, we call p a *good* prime if $F(\mathbf{x}) \equiv 0 \,(\mathrm{mod}\ p)$ defines a smooth projective variety in $\mathbb{P}^{n-1}$ over $\mathbb{Z}/p\mathbb{Z}$. Otherwise we call p a *bad* prime. Usually we write S for the set of bad primes.

REMARK 1.3.21. If $F = \sum_{i=1}^n a_i x_i^d$ is diagonal, then the set of bad primes equals $S = \{p \text{ prime} : p \mid d \prod_i a_i\}$.

COROLLARY 1.3.22. *If $F = \sum_{i=1}^{n} a_i x_i^d$ is diagonal and $p \notin S$ is a good prime, then $S^*_{p^k} = 0$ holds for $k \geq 2$. Moreover, for any prime p we have $S^*_{p^k} = 0$ for $k \geq 2\,\mathrm{ord}_p(d\prod_i a_i) + 2$.*

Proof. This is an immediate consequence of Lemmas 1.3.18 and 1.3.19. □

1.3.3 Birch's circle method

In his famous paper [Bir62], Birch generalized the circle method to apply to multiple homogeneous polynomials of equal degree, rather than merely a single one. In fact, Birch was also the first one to treat general polynomials of any given degree. Our Chapter 3 leans heavily on this paper, so we cite some of its definitions and results here for easy reference. Throughout this subsection, one should take notice of the similarity to §1.3.1, where, in the notation of the current subsection, we have only been concerned with the case $\boldsymbol{\nu} = 0$, and of course $R = 1$.

Birch's setup is as follows. Let $f_1, \ldots, f_R \in \mathbb{Z}[\mathbf{x}]$ be homogeneous polynomials of positive degree d in n variables, subject to the following conditions. For any $\boldsymbol{\mu} \in \mathbb{C}^R$, write $V(\boldsymbol{\mu}) \subset \mathbb{A}^n_{\mathbb{C}}$ for the affine variety defined by $f_i(\mathbf{x}) = \boldsymbol{\mu}_i$, $i = 1, \ldots, R$. Let $V^*(\boldsymbol{\mu})$ be the singular locus of $V(\boldsymbol{\mu})$, and write $V^* = \bigcup_{\boldsymbol{\mu}\in\mathbb{C}^R} V^*(\boldsymbol{\mu})$ and $\sigma = \dim V^*$. Assume

$$K := 2^{1-d}(n-\sigma) > R(R+1)(d-1) \tag{1.6}$$

and let $\mathcal{B}$ be any box inside $[-1,1]^R$. Furthermore, we need to assume $\dim V(0) = n - R$.

REMARK 1.3.23. An equivalent description of V^* defines it as the subset of $\mathbb{C}^n$ of elements $\mathbf{x}$ that satisfy

$$\mathrm{rk}\left(\frac{\partial f_i}{\partial x_j}\right)_{i,j}(\mathbf{x}) < R.$$

Every statement that follows should be preceded by the phrase "with all assumptions from this subsection so far..." or something similar.

DEFINITION 1.3.24. For $\theta \in (0,1]$, $a_1, \ldots, a_R, q \in \mathbb{Z}_{>0}$, and $P \in \mathbb{R}_{>0}$, write

$$\mathcal{M}_{\mathbf{a},q}(\theta) = \left\{\boldsymbol{\alpha} \in [0,1)^R \,\middle|\, 2|q\alpha_i - a_i| \leq P^{-d+R(d-1)\theta}, i = 1, \ldots, R\right\},$$

and

$$\mathcal{M}(\theta) = \bigcup_{1 \le q \le P^{R(d-1)}} \bigcup_{\substack{\mathbf{a}: 0 \le a_i < q \\ \gcd(a_1,\dots,a_R,q)=1}} \mathcal{M}_{\mathbf{a},q}(\theta)$$

for the analogue of the *major arcs* in Definition 1.3.4.

LEMMA 1.3.25. *If $d > 2R(d-1)\theta$ holds then $\mathcal{M}(\theta)$ is a union of disjoint boxes $\mathcal{M}_{\mathbf{a},q}(\theta)$.*

Proof. This is [Bir62, Lemma 4.1]. □

Now let δ and θ_0 be small positive real numbers satisfying

$$1 > \delta + 2(R+2)Rd\theta_0 \tag{1.7}$$

and

$$K - R(R+1)(d-1) > 2\delta\theta_0^{-1}. \tag{1.8}$$

DEFINITION 1.3.26. For $\boldsymbol{\nu} \in \mathbb{Z}^R$ and $P \ge 2$, write

$$S(\boldsymbol{\alpha};\boldsymbol{\nu}) = \sum_{\mathbf{x} \in P\mathcal{B} \cap \mathbb{Z}^n} \mathrm{e}\left(\sum_i \alpha_i f_i(\mathbf{x})\right) \mathrm{e}\left(-\sum_i \alpha_i \nu_i\right).$$

LEMMA 1.3.27. *With δ and θ_0 as above, we have*

$$\int_{\boldsymbol{\alpha} \notin \mathcal{M}(\theta_0)} |S(\boldsymbol{\alpha};\boldsymbol{\nu})| \mathrm{d}\boldsymbol{\alpha} \ll P^{n-Rd-\delta}.$$

Proof. This is [Bir62, Lemma 4.4]. □

In the statement above, the bound is independent of $\boldsymbol{\nu}$. In particular the first step of the proof is noticing the equality $|S(\boldsymbol{\alpha};\boldsymbol{\nu})| = |S(\boldsymbol{\alpha})|$ by the trivial bound on the complex exponential.

Birch's results are in a neater form when one switches viewpoint to major arcs that are slightly modified. Since we will want to quote his results directly, we will adopt these expanded major arcs.

DEFINITION 1.3.28. We write

$$\mathcal{M}'_{\mathbf{a},q}(\theta) = \left\{ \boldsymbol{\alpha} \in [0,1)^R \,\middle|\, |q\alpha_i - a_i| \le qP^{-d+R(d-1)\theta}, i = 1,\dots,R \right\},$$

and

$$\mathcal{M}'(\theta) = \bigcup_{1\le q\le P^{R(d-1)}} \bigcup_{\substack{\mathbf{a}:0\le a_i<q \\ \gcd(a_1,\dots,a_R,q)=1}} \mathcal{M}'_{\mathbf{a},q}(\theta)$$

for the *expanded major arcs*.

Writing $M(P;\boldsymbol{\nu})$ for the number of solutions $\mathbf{x}$ to the system of equations $f_i(\mathbf{x}) = \nu_i$, $i = 1,\dots,R$ with $\mathbf{x} \in P\mathcal{B} \cap \mathbb{Z}^n$, we have the following lemma.

LEMMA 1.3.29. *We have*

$$M(P;\boldsymbol{\nu}) = \sum_{1\le q\le P^{R(d-1)\theta_0}} \sum_{\mathbf{a}} \int_{\mathcal{M}'(\theta_0)} S(\boldsymbol{\alpha};\boldsymbol{\nu})\mathrm{d}\boldsymbol{\alpha} + O(P^{n-Rd-\delta}),$$

where the sum over $\mathbf{a}$ *is over all* R*-tuples* $a_1,\dots,a_R$ *satisfying* $0 \le a_i < q$ *for* $i = 1,\dots,R$ *and* $\gcd(a_1,\dots,a_R,q) = 1$.

Proof. This is [Bir62, Lemma 4.5], which uses that also the expanded major arcs remain disjoint. □

DEFINITION 1.3.30. We write

$$S_{\mathbf{a},q} = \sum_{\mathbf{x}\in(\mathbb{Z}/q\mathbb{Z})^n} \mathrm{e}\left(\sum_i a_i f_i(\mathbf{x})/q\right),$$

and

$$S_{\mathbf{a},q}(\boldsymbol{\nu}) = \mathrm{e}\left(-\sum_i a_i\nu_i/q\right) S_{\mathbf{a},q}$$

for the analogue to $S_{q,a}$ in Definition 1.3.9.

DEFINITION 1.3.31. For a measurable subset $\mathcal{C} \subset [-1,1]^n$, we write

$$I(\mathcal{C};\boldsymbol{\gamma}) = \int_{\boldsymbol{\zeta}\in\mathcal{C}} \mathrm{e}\left(\sum_i \gamma_i f_i(\boldsymbol{\zeta})\right)\mathrm{d}\boldsymbol{\zeta}$$

for the analogue to the integral $I(\theta)$ from Definition 1.3.6.

LEMMA 1.3.32. *For* $\boldsymbol{\alpha} \in \mathcal{M}'_{\mathbf{a},q}(\theta_0)$, $\beta := \boldsymbol{\alpha} - \mathbf{a}/q$, *and* $\eta = R(d-1)\theta_0$, *we have*

$$S(\boldsymbol{\alpha};\boldsymbol{\nu}) = q^{-n}P^n S_{\mathbf{a},q}(\boldsymbol{\nu}) I(\mathcal{B};P^d\beta)\,\mathrm{e}\left(-\sum \beta_i\nu_i\right) + O(P^{n-1+2\eta}).$$

Proof. This is [Bir62, Lemma 5.1]. □

LEMMA 1.3.33. *Let $\mathcal{C} \subset [-1,1]^n$ be any box with side lengths at most $\varsigma < 1$. Then for any $\varepsilon > 0$ we have*

$$I(\mathcal{C}, \boldsymbol{\gamma}) \ll_\varepsilon \varsigma^n \cdot \min\left\{1, \left(\varsigma^d \max\{|\gamma_i|\}^{-\frac{K}{R(d-1)}+\varepsilon}\right)\right\}$$

Proof. This is [Bir62, Lemma 5.2]. □

LEMMA 1.3.34. *For every $\varepsilon > 0$ and $0 \le a_i < q$ for $1 \le i \le R$ satisfying $\gcd(a_1, \ldots, a_R, q) = 1$, we have*

$$|S_{\mathbf{a},q}| \ll_\varepsilon q^{n-\frac{K}{R(d-1)}+\varepsilon}.$$

Proof. This is [Bir62, Lemma 5.4]. □

DEFINITION 1.3.35. We write

$$J(\boldsymbol{\nu}; \Phi) = \int_{|\boldsymbol{\gamma}| \le \Phi} I(\mathcal{B}; \boldsymbol{\gamma})\, \mathrm{e}\left(-\sum_i \gamma_i \nu_i\right) \mathrm{d}\boldsymbol{\gamma}.$$

and

$$J(\boldsymbol{\nu}) = \lim_{\Phi \to \infty} J(\boldsymbol{\nu}; \Phi)$$

if the limit exists. The limit $J(\boldsymbol{\nu})$ is the analogue of $\mathfrak{J}$ in Definition 1.3.9.

LEMMA 1.3.36. *Writing*

$$\mathfrak{S}(\boldsymbol{\nu}) = \sum_{q=1}^{\infty} q^{-n} \sum_{\mathbf{a}} S_{\mathbf{a},q}(\boldsymbol{\nu})$$

where the sum over $\mathbf{a}$ is over all R-tuples $(a_1, \ldots, a_R)$ satisfying $0 \le a_i < q$ for $i = 1, \ldots, R$ and $\gcd(a_1, \ldots, a_R, q) = 1$, then $P \ge 2$ validates

$$M(P; \boldsymbol{\nu}) = P^{n-Rd}\mathfrak{S}(\boldsymbol{\nu})J(P^{-d}\boldsymbol{\nu}) + O(P^{n-Rd-\delta})$$

Proof. This is [Bir62, Lemma 5.5]. □

The lemmas above, combined with a more detailed study of the singular integral, culminate in the main theorem of Birch's paper, namely his Theorem 1 on page 260, which further states some conditions under which $\mathfrak{S}(\boldsymbol{\nu})$ and $J(\boldsymbol{\nu})$ are positive. The formula for $M(P; \boldsymbol{\nu})$ that appears in this main result is essentially the one from Lemma 1.3.36 above.

1.3.4 Dirichlet characters

DEFINITION 1.3.37. A *Dirichlet character* modulo q is a group homomorphism $\chi : (\mathbb{Z}/q\mathbb{Z})^\times \to \mathbb{C}^\times$. A *trivial* Dirichlet character is one that is constant and is denoted χ_0, the modulus q being implicit.

DEFINITION 1.3.38. For a Dirichlet character χ, its associated *Dirichlet series* is

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$$

for $\Re(s) > 1$, where χ is extended to $\mathbb{Z}_{>0}$ by setting its value to 0 if n and q are not coprime.

Dirichlet series are well studied, see for example [MV07, Chapter 4]. A fundamental result is that they often have an analytic continuation to a larger domain, although their defining formula only holds for $\Re(s) > 1$.

The series associated to χ_0 has a pole of order 1 at $s = 1$, but non-trivial ones display very different behaviour, as shown in the following foundational theorem. Indeed, $L(\chi_0, s)$ equals $\zeta(s)$ up to a finite number of local factors involving the prime divisors of q.

THEOREM 1.3.39 (Dirichlet). *If $\chi \neq \chi_0$ is a non-trivial Dirichlet character, then $L(\chi, s)$ is analytic in the region $\Re(s) > 0$ and moreover $L(\chi, 1)$ is non-zero.*

Proof. This combines parts of [MV07, Thm. 4.8, Thm. 4.9]. □

Chapter 2

Heuristics for counting rational points on diagonal quartic surfaces

> *If to do were as easy as to know what were good to do, chapels had been churches, and poor men's cottages princes' palaces*
>
> Portia, The Merchant of Venice, Scene 1.2, lines 9-10

This chapter is concerned with finding heuristics for a conjecture in the style of Manin's Conjecture 1.2.15 for some K3 surfaces over $\mathbb{Q}$. In particular we will restrict ourselves to diagonal quartic surfaces. We use the circle method to obtain such heuristics. We do not take into account that such surfaces may have accumulating subvarieties, but we discuss these in relation to the circle method at the very end of this chapter.

In particular, the goal of this chapter is to prove the following main result, where we assume the generalized Riemann hypothesis (hereafter GRH). In fact, we do not need to assume GRH for all L-functions; just some of specific origin, as will come up in Proposition 2.2.5. Recall the singular integral $\mathfrak{J}(Q)$ from Definition 1.3.9 and the modified singular series $\mathfrak{S}^*(Q)$ from Definition 1.3.17. For diagonal quartic surfaces we have $n = d = 4$, so the singular integral and singular series together make up the contribution of the major arcs to counting points up to bounded height, provided that the major arcs do not overlap. In accordance to Lemma 1.3.5 and Remark 1.3.8 we implicitly assume $\delta < \frac{1}{5}$ to have been chosen.

Theorem 2.0.1. *For $a_1, \dots, a_4 \in \mathbb{Z} \setminus \{0\}$, let $F = \sum_{i=1}^{4} a_i x_i$ define a diagonal quartic surface X of Picard rank $\rho \geq 2$. Under the assumption*

of GRH, there exists a constant c_F such that as $Q \to \infty$ the contribution $\mathfrak{J}(Q)\mathfrak{S}^*(Q)$ equals

$$c_F(\log Q)^\rho + o((\log Q)^\rho).$$

This theorem should be viewed in light of computational data produced by van Luijk and available on his website [Lui]. Indeed the heuristic in this theorem matches with the growth that the data seems to imply.

REMARK 2.0.2. Some diagonal quartic surfaces (e.g. those with all a_i positive) have no rational points, so in general one should not expect c_F to be non-zero. Ideally, one would hope that a detailed treatment of c_F would show obstructions to it being positive. Such obstructions should be more complicated than just local obstructions as counterexamples to the Hasse principle are known for diagonal quartic surfaces (see for example [SD00] or [Bri06]).

2.1 Averages of multiplicative functions

In a recent preprint [GK17], Granville and Koukoulopoulos present a very strong theorem dealing with averages of multiplicative functions. Very similar theorems were first discovered by Wirsing using ideas of Selberg and Delange. In fact, the contents of this chapter were first proven using Wirsing's work [Wir61, Satz 1]. The downside of Wirsing's original theorem is that it only deals with non-negative multiplicative functions, restricting us to only apply the result to specific diagonal quartic surfaces. The new theorem of Granville and Koukoulopoulos however needs a good error term in one of its conditions. This is automatically provided by assuming GRH; see Proposition 2.1.11 and the remark following it. This assumption may be removed by knowing good zero-free regions for L-functions of varieties; see Remark 2.2.6.

2.1.1 A powerful result by Granville and Koukoulopoulos

In order to phrase the theorem, we need to introduce some notation. We will let Γ denote the classical Gamma function

$$\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}\mathrm{d}t.$$

In particular, for positive integer z we have $\Gamma(z) = (z-1)!$.

Definition 2.1.1. For any complex number α the multiplicative function τ_α is given on prime powers by

$$\tau_\alpha(p^\nu) = \alpha(\alpha+1)\cdots(\alpha+\nu-1)/\nu!.$$

In particular, on primes the function τ_α evaluates to α, and if α is a positive integer, then $\tau_\alpha(p^e) = \binom{\alpha-1+e}{e}$ holds.

Definition 2.1.2. For a multiplicative function f, its associated Dirichlet series will be denoted by $L_f(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$. Fix some complex number α such that the function $(s-1)^\alpha L_f(s)$ is J times continuously differentiable in the half-plane $\Re(s) \geq 1$. For all $j \leq J$ we set[1]

$$c_j := \frac{1}{j!}\frac{\mathrm{d}^j}{\mathrm{d}s^j}\bigg|_{s=1} \frac{(s-1)^\alpha L_f(s)}{s}.$$

Theorem 2.1.3 (Granville–Koukoulopoulos). *Let f be a multiplicative function for which there exist $\alpha \in \mathbb{C}$ and $A \in \mathbb{R}_{>0}$ such that for $x \geq 2$, the function f satisfies*

$$\sum_{p\leq x} f(p)\log(p) = \alpha x + O\left(\frac{x}{(\log x)^A}\right), \tag{2.1}$$

where the sum is over the prime numbers at most x. Furthermore assume that there exists some $k \in \mathbb{R}_{>0}$ such that $|f| \leq \tau_k$ holds. If $J = \lceil A-1 \rceil$ is the largest integer smaller than A, then with notation c_j as above, $x \geq 2$ validates

$$\sum_{n\leq x} f(n) = x\sum_{j=0}^{J} c_j \frac{(\log x)^{\alpha-j-1}}{\Gamma(\alpha-j)} + O\left(x(\log x)^{k-1-A}(\log\log x)^{\mathbb{I}_{A=J+1}}\right).$$

The implied constant depends at most on k, A and the implied constant from (2.1). The dependence on A is twofold: from its size and its distance from the nearest integer.

Proof. This is [GK17, Theorem 1]. □

[1] Notice that our notation is slightly different from that in [GK17] as we have surpressed some notation from the source since we will only need part of the conclusion of its main theorem.

Remark 2.1.4.

- Implicit in the formulation of the previous theorem is that assumption (2.1) implies that the Dirichlet series associated to f is $\lceil A-1 \rceil$ times continuously differentiable in the half-plane $\Re(s) \geq 1$.
- The Γ-function has poles at all non-positive integers, hence in the result of Theorem 2.1.3, for integer α all terms with $j \geq \alpha$ vanish. In particular, the theorem only yields an asymptotic for $\alpha \neq 0$, and only then if $k - A < \alpha$ holds.

For our purposes we only consider the $j = 0$ term from the conclusion of Theorem 2.1.3, which under the conditions in the remark above yields the dominating term.

The following lemma allows us to convert the conclusion of Theorem 2.1.3 into a form that we prefer. Notice that the case $a = -1$ below does not appear in the conclusion of the theorem – nor do any other cases with negative a.

Lemma 2.1.5. *If $f : \mathbb{Z}_{>0} \to \mathbb{C}$ satisfies $\sum_{n \leq x} f(n) \sim cx(\log x)^a$ for some constants $a \in \mathbb{Z}$ and $c \in \mathbb{C}$, then for $a \neq -1$ we have*

$$\sum_{n \leq x} \frac{f(n)}{n} \sim \frac{c}{a+1}(\log x)^{a+1},$$

and for $a = -1$ we have

$$\sum_{n \leq x} \frac{f(n)}{n} \sim c \log\log x.$$

Proof. This is a simple application of Abel's partial summation formula (cf. Theorem1.3.1). We have

$$\begin{aligned}\sum_{n \leq x} \frac{f(n)}{n} &= \left(\sum_{n \leq x} f(n)\right)\frac{1}{x} + \int_1^x \left(\sum_{n \leq t} f(n)\right)\frac{1}{t^2}\mathrm{d}t \\ &\sim c(\log x)^a + c\int_1^x (\log t)^a \frac{1}{t}\mathrm{d}t.\end{aligned}$$

For $a \neq -1$ the integral evaluates to $\frac{1}{a+1}(\log x)^{a+1}$, whereas for $a = -1$ it evaluates to $\log\log x$, in either case giving the dominating term. □

2.1.2 Chebyshev-like functions

In his study towards the Prime Number Theorem, Chebyshev introduced the function

$$\psi(x) = \sum_{n \le x} \Lambda(n),$$

where

$$\Lambda(n) = \begin{cases} \log(p) & \text{if } n = p^e \text{ is a non-trivial prime power,} \\ 0 & \text{otherwise} \end{cases}$$

is known as the von Mangolt function.

The function $\psi(x)$ relates to the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ which is the Dirichlet series of the constant multiplicative function 1. In studying averages of multiplicative functions, one often works with Chebyshev-like functions that we will now define. We generalize some definitions from §1.3.4.

Definition 2.1.6. Let $f : \mathbb{Z}_{>0} \to \mathbb{C}$ be a function. Its associated *Dirichlet series* is $L_f(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$. If f is multiplicative, the *von Mangoldt function* Λ_f associated with f is defined indirectly through its Dirichlet series as

$$-\frac{L_f'(s)}{L_f(s)} = \sum_{n=1}^{\infty} \Lambda_f(n) n^{-s}$$

and its associated *Chebyshev function* is

$$\psi_f(x) = \sum_{n \le x} \Lambda_f(n).$$

Lemma 2.1.7. *For a completely multiplicative function f we have*

$$L_f(s) = \prod_p \frac{1}{1 - f(p)p^{-s}}.$$

Proof. This follows from writing $L_f(s)$ as a product over primes

$$L_f(s) = \prod_p \left(1 + f(p)p^{-s} + f(p^2)p^{-2s} + \cdots\right)$$

and then recognizing the sums as geometric series. □

LEMMA 2.1.8. *The von Mangoldt function associated with a multiplicative function f is supported on the prime powers and for any prime number p it evaluates as $\Lambda_f(p) = f(p)\log(p)$. If f is completely multiplicative, the von Mangoldt function satisfies*

$$\Lambda_f(n) = \Lambda(n)f(n).$$

Proof. These properties may be found without proof on [IK04, page 17]. For the sake of completeness, we will give a proof here.

First, it is easily seen that $-L_f'(s)$ is the Dirichlet series of $f \cdot \log$. The convolution of two functions $f, g : \mathbb{Z}_{>0} \to \mathbb{C}$ is defined as

$$(f * g)(n) = \sum_{d|n} f(d)g(\tfrac{n}{d})$$

and it is well known (or easily computed) that the Dirichlet series of a convolution is the product of the two Dirichlet series. Hence we get $f * \Lambda_f = f \cdot \log$.

We compute some values of Λ_f. Expanding $(f * \Lambda_f)(1) = f(1)\log(1) = 0$ and using $f(1) = 1$, we find $\Lambda_f(1) = 0$. Using this result, we move on to work out $(f * \Lambda_f)(p) = f(p)\log p$ for any prime number p and conclude $\Lambda_f(p) = f(p)\log p$.

Finally, taking p and q two different prime numbers, using the same strategy we conclude $\Lambda_f(pq) = 0$. Using this as a base case, one may apply induction to prove the same for numbers with more than two prime factors or higher exponents, hence Λ_f is supported on prime powers.

Having already proven $\Lambda_f(p) = f(p)\log p$, we may apply induction to the power of p to show that for completely multiplicative f we have $\Lambda_f(p^k) = f(p)^k \log p = f(p^k)\log p = f(p^k)\Lambda(p^k)$. The strategy is completely analogous to the first part of this proof. □

REMARK 2.1.9. From the last lemma and the definition of Λ it immediately follows that if f is a completely multiplicative function, then for $k \geq 1$ we have

$$\Lambda_f(p^k) = \Lambda(p^k)f(p^k) = f(p)^k \log(p)$$

as was already seen in the proof, but is worth stating separately.

The Chebyshev function associated with a multiplicative function f is often useful to study the sum $\sum_{p\leq x} f(p)\log p$, provided one can bound the contribution of higher prime powers. Indeed, we have

$$\sum_{p\leq x} f(p)\log p = \psi_f(x) - \sum_{k=2}^{\infty}\sum_{p^k\leq x} \Lambda_f(p^k),$$

where the sum over k is actually a finite sum as for $k > \log_2(x)$, the second sum is empty.

LEMMA 2.1.10. *Let f be a multiplicative function for which there exists some $b \in \mathbb{R}_{>0}$ bounding from above every $|f(p)|$ for prime numbers p. For some $a \in \mathbb{Z}_{>0}$ define a completely multiplicative function f^* by*

$$f^*(p^e) = \begin{cases} 1 & \text{if } e = 0, \\ 0 & \text{if } e \geq 1, p \leq a, \\ f(p)^e & \text{if } p > a. \end{cases}$$

Then for sufficiently large x we have

$$\left|\psi_{f^*}(x) - \sum_{a<p\leq x} f(p)\log p\right| = \left|\sum_{k=2}^{\infty}\sum_{\substack{p\\ p^k\leq x}} \Lambda_{f^*}(p^k)\right| \ll x^{1/2+\log_a(b)}.$$

Proof. By definition we have $\sum_{a<p\leq x} f(p)\log p = \sum_{p\leq x} f^*(p)\log p$ and as we have already remarked above, the equality of the statement follows. For the remainder of the proof, we will focus on the absolute value of the sum on the right-hand side of the equality, which we will call S.

After applying the triangle inequality, we begin by switching the order of summation and extending the sum over primes to all p satisfying $p^2 \leq x$, thereby increasing its total value, i.e.

$$|S| \leq \sum_{\substack{p\\ p^2\leq x}} \log p \sum_{k=2}^{\lfloor \log_p(x)\rfloor} |f^*(p)|^k = \sum_{\substack{p>a\\ p^2\leq x}} \log p \sum_{k=2}^{\lfloor \log_p(x)\rfloor} |f(p)|^k.$$

Without loss of generality we may assume $b \geq 2$. The sum over k is bounded from above by

$$\sum_{k=2}^{\lfloor \log_p(x)\rfloor} b^k \leq b^2 \cdot \frac{x^{\log_p(b)} - 1}{b-1} \leq b^2 x^{\log_a(b)}.$$

For sufficiently large x, the number of primes p with $p^2 \leq x$ is of the order $\frac{2x^{1/2}}{\log x}$ and for each of those we may trivially bound $\log p$ by $\frac{1}{2}\log x$. Hence the absolute value of S is bounded by $b^2 \cdot x^{1/2+\log_a(b)}$ as required. □

In order for Theorem 2.1.3 to be useful in the application that we have in mind, and following our proof, we will need (2.1) with an arbitrarily high exponent A. It is not unthinkable that this may be derived with some skilful application of zero-free regions for appropriate L-functions but in our main result of the chapter we opt to take the shortcut of assuming GRH.

Iwaniec and Kowalski dedicate Chapter 5 of their book [IK04] to a wide class of L-functions. They explicitly let their notation remain somewhat vague and suggestive, but they do give a list of requirements to what they call an L-function. For us it is enough to know that Dirichlet series, L-functions of cusp forms, and (sometimes conjecturally) L-functions of varieties fall in the class for which the following proposition is true. In particular, with the knowledge from §1.2.3, we see that the following proposition applies to $L(\mathrm{H}^2(X), s)$.

Proposition 2.1.11. *Let $\frac{1}{2} \leq \sigma < 1$. The following statements are equivalent for an L-function:*

1. *There are neither zeros nor poles of $(s-1)^r L_f(s)$ in $\Re(s) > \sigma$, where r is a non-negative integer.*
2. *Let $r \geq 0$ be the order of the pole of $L_f(s)$ at $s = 1$. Then for all $\varepsilon > 0$ and $x \geq 2$ we have*

$$\psi_f(x) = rx + O\left(x^{\sigma+\varepsilon}\right),$$

the implied constant depending on f and $\varepsilon > 0$.

Proof. This is part of [IK04, Proposition 5.14]. □

Remark 2.1.12.

- The numbers r appearing in the two statements of the previous proposition are necessarily the same. Indeed, if the number r in the first statement is not the order of the pole of $L_f(s)$ at $s = 1$ then $(s-1)^r L_f(s)$ will either have a pole or a zero at $s = 1$.

- GRH asserts that the first statement in the proposition above is true for $\sigma = \frac{1}{2}$, and hence also the second one which is the statement that we want to use.

- Although the notation of the proposition seems to rely on some function f, we do not really need it for the result. Via $L_f'(s)/L_f(s)$ one may define $\Lambda_f(n)$ implicitly and from that also $\psi_f(x)$.

2.2 Evaluating the singular series

We now turn to the main goal of the chapter, namely evaluating the contribution of the major arcs to rational points on those diagonal quartic surfaces X as given in Theorem 2.0.1: defined by $F(\mathbf{x}) = \sum_{i=1}^{4} a_i x_i^4$ with $a_i \in \mathbb{Z} \setminus \{0\}$ such that X has Picard rank $\rho \geq 2$. Throughout the rest of the chapter we write S for the finite set of primes where X has bad reduction.

Section 2.1 provides the tools for evaluating the singular series. The singular integral will have to wait until §2.3.

In order to apply Theorem 2.1.3, we introduce a suitable multiplicative function f such that we have $\sum_{q=1}^{Q} \frac{f(q)}{q} = \mathfrak{S}^*(Q)$. This is provided by the following choice:

Definition 2.2.1. We denote $f(q) = \frac{S_q^*}{q^3}$ where S_q^* is given in Definition 1.3.17.

Indeed, Lemma 1.3.18 shows that f is multiplicative.

Before we proceed, we relate the function f to the geometry of X. Using the Lefschetz trace formula, which gives $\#X(\mathbb{F}_p) = p^2 + T_p \cdot p + 1$ where $T_p \cdot p$ is the trace of Frobenius on $\mathrm{H}^2_{\text{ét}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$, and moreover using that $N^*(p)$ counts the number of non-zero affine zeroes over $\mathbb{Z}/p\mathbb{Z}$ of the equation

$F(\mathbf{x}) = 0$, one finds

$$\begin{aligned} f(p) = \frac{S_p^*}{p^3} &= p\left(\frac{N^*(p)}{p^3} - 1\right) \\ &= p\left(\frac{\#X(\mathbb{F}_p)(p-1)}{p^3} - 1\right) \\ &= p\left(\frac{p^3 + (T_p - 1)p^2 - (T_p - 1)p - 1}{p^3} - 1\right) \\ &= (T_p - 1)\left(1 - \tfrac{1}{p}\right) \\ &= (T_p - 1) + O\left(\tfrac{1}{p}\right). \end{aligned}$$

The first non-trivial equality uses the result of Lemma 1.3.18 with $n = 4$.

The following lemma will be useful in checking the conditions of Theorem 2.1.3 for our chosen function f.

LEMMA 2.2.2. *For every prime p we have $|T_p| \leq 22$.*

Proof. The number $T_p \cdot p$ is the trace of Frobenius on $\mathrm{H}^2_{\text{ét}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$. By the Weil conjectures, each of the eigenvalues has absolute value p. Hence $|T_p \cdot p|$ is bounded by p times the dimension of $\mathrm{H}^2_{\text{ét}}(X_{\overline{\mathbb{F}_p}}, \mathbb{Q}_\ell)$, which by comparison with singular cohomology is the second Betti number b_2. For K3 surfaces, the second Betti number equals 22, completing the proof. □

This description on prime values will be used to check that f satisfies the conditions of Theorem 2.1.3. We first assure ourselves of the assumption that there exists some $k \in \mathbb{R}_{>0}$ such that $|f| \leq \tau_k$ holds, leaving the more involved assumption (2.1) for later.

LEMMA 2.2.3. *There exists a number $k \in \mathbb{R}_{>0}$ validating $|f| \leq \tau_k$.*

Proof. Since for positive real k, both $|f|$ and τ_k are multiplicative and take values in $\mathbb{R}_{\geq 0}$ when applied to positive integers, we need only check the assertion on prime power values.

We first consider the values of $|f|$ on primes. By Lemma 2.2.2, $|T_p|$ is bounded by 22, so for every prime p, the value $|f(p)|$ is bounded by 23. Recalling Corollary 1.3.22, we see that for almost all primes p, we have $f(p^e) = 0$ for all $e \geq 2$. Hence we only need to further consider a finite set of primes T, and moreover, by Lemma 1.3.19, only a finite set of prime powers $P = \{p^e : p \in T,\ f(p^e) \neq 0\}$. Over this finite set, $|f|$ takes a

maximum value. Moreover, for fixed e, the value of $\binom{k+e-1}{e}$ as a function of k is unbounded. Hence there exists some positive integer K such that for all $p^e \in P$ we have

$$|f(p^e)| \leq \binom{K+e-1}{e} = \tau_K(p^e).$$

Hence $|f(p^e)| \leq \tau_{\max\{23,K\}}(p^e)$ holds for all prime powers p^e and therefore the desired inequality $|f| \leq \tau_{\max\{23,K\}}$ holds on all positive integers. Hence we retrieve the statement of the lemma with $k = \max\{23, K\}$. □

Remark 2.2.4. Since the number k in the lemma above is ineffective, and the result of Theorem 2.1.3 is only useful for $k - A < \alpha$, we need to verify condition (2.1) for arbitrarily large A.

To verify condition (2.1) we need to evaluate

$$\sum_{p \leq x} f(p) \log p = \sum_{p \leq x} T_p \log p - \sum_{p \leq x} \log p + O\left(\sum_{p \leq x} \tfrac{1}{p} \log p\right) \tag{2.2}$$

where we have used that the implicit constants in $f(p) = (T_p - 1) + O\left(\frac{1}{p}\right)$ are universally bounded by 23.

We consider this sum in three parts: first, evaluation of

$$\sum_{p \leq x} \tfrac{1}{p} \log p = \log x + O(1)$$

is standard in analytic number theory and is known as Mertens' first theorem.

Then, the middle term $\sum_{p \leq x} \log p$ comes up in the proof of the Prime Number Theorem (Theorem 1.3.2), and the validity of $\sum_{p \leq x} \log p \sim x$ is in fact equivalent to it by application of Abel's summation formula from Theorem 1.3.1.

In order to evaluate $\sum_{p \leq x} T_p \log p$ we will use an L-function involving T_p.

Consider the function g given on primes by $p \mapsto T_p$ and extended to have domain $\mathbb{Z}_{>0}$ by complete multiplicativity. Its Dirichlet series becomes

$$L_g(s) = \prod_p \frac{1}{1 - T_p p^{-s}}$$

by Lemma 2.1.7.

PROPOSITION 2.2.5. *Assuming GRH and writing r for the order of the pole of $L_g(s)$ at $s = 1$, for any $A > 0$ and $x \geq 2$ we have*

$$\sum_{p \leq x} T_p \log p = rx + O\left(\frac{x}{(\log x)^A}\right)$$

and moreover

$$\sum_{p \leq x} f(p) \log p = (r-1)x + O\left(\frac{x}{(\log x)^A}\right).$$

Proof. We apply Lemma 2.1.10 to the completely multiplicative function g defined through $p \mapsto T_p$. Indeed by Lemma 2.2.2 it is applicable with $b = 22$. We may use $a = 22^3$ as this makes the resulting power of x in the conclusion of Lemma 2.1.10 equal to $\frac{1}{2} + \frac{1}{3} = \frac{5}{6} < 1$. In fact, any $a > 22^2$ would also have sufficed.

Having fixed a, the sum $\sum_{p \leq a} T_p \log p$ is bounded, hence with notation of Lemma 2.1.10 we have

$$\sum_{p \leq x} T_p \log p = \psi_{g^*}(x) + O\left(x^{5/6}\right).$$

The Dirichlet series of g^* and $L_g(s)$ are not equal, but their Euler products only differ for primes $p < a$. These are finite in number, so the order of the pole at $s = 1$ is not affected. Hence, by Proposition 2.1.11 we have

$$\psi_{g^*}(x) = rx + O\left(x^{\frac{1}{2}+\varepsilon}\right).$$

Combining these two estimates, we conclude

$$\sum_{p \leq x} T_p \log p = rx + O\left(x^{\max\left\{\frac{5}{6}, \frac{1}{2}+\varepsilon\right\}}\right).$$

Realizing that saving a power of x gives a stricter error term than saving any power of $\log x$, we conclude the proof of the first equality upon choosing any $\varepsilon < \frac{1}{2}$.

The second equality immediately follows by recombining the three terms in (2.2). Indeed the error $O\left(\frac{x}{(\log x)^A}\right)$ also applies to the middle sum $\sum_{p \leq x} \log p \sim x$. □

REMARK 2.2.6. In the proposition above, we did not really need to assume the full power of GRH: by Proposition 2.1.11, a zero-free region $\Re(s) > \sigma$ for any $\sigma > \frac{1}{2}$ would have sufficed.

2.2.1 Identification of the logarithmic exponent

The last step in calculating the singular series is to identify the constant r appearing in Proposition 2.2.5. So far, $L_g(s) = \prod_p (1 - T_p p^{-s})^{-1}$ seemed to have appeared out of nowhere, and a priori it is not obvious what the order r of the pole would be. We will now explain how $L_g(s)$ is related to the variety X and how r is related to the Picard group of X. Recall the L-function $L(\mathrm{H}^2(X), s)$ from Definition 1.2.19.

PROPOSITION 2.2.7. *The order of the pole of $L(\mathrm{H}^2(X), s)$ at $s = 2$ is the Picard rank of X.*

Proof. As was already seen in §1.2.3, this is part of the Tate conjecture, which is known for K3 surfaces and hence in particular for X. □

PROPOSITION 2.2.8. *The shifted Dirichlet series $L_g(s-1)$ and $L(\mathrm{H}^2(X), s)$ have poles of the same order at $s = 2$.*

Proof. First notice that indeed both L-functions have a pole at $s = 2$. We compare the p-adic factors for both Euler products

$$L_g(s-1) = \prod_p \frac{1}{1 - T_p p^{1-s}}$$

and

$$L(\mathrm{H}^2(X), s) = \prod_{p \notin S} \frac{1}{\det(1 - \mathrm{Frob}_p\, p^{-s} \mid \mathrm{H}^2_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)}.$$

Note that there are only finitely many bad primes $p \in S$, so their appearance will not affect the order of the pole. Let α_j for $j = 1, \ldots, b_2 = 22$ be the eigenvalues of Frob_p on $\mathrm{H}^2_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)$. Since one obtains the expression $\det(1 - \mathrm{Frob}_p\, p^{-s} \mid \mathrm{H}^2_{\text{ét}}(\overline{X_p}, \mathbb{Q}_\ell)$ as the characteristic polynomial of the Frobenius endomorphism, read backwards, with p^{-s} substituted, this determinant equals $\prod_{j=1}^{22}(1 - \alpha_j p^{-s})$, which is

$$1 - (T_p \cdot p)p^{-s} + \sum_{i<j} \alpha_i \alpha_j p^{-2s} - \sum_{i<j<k} \alpha_i \alpha_j \alpha_k p^{-3s} + \ldots + \left(\prod_{j=1}^{22} \alpha_j \right) p^{-22s}.$$

Let us study the fraction between p-adic factors for the two L-functions

$L(\mathrm{H}^2(X), s)$ and $L_g(s-1)$ for $p \notin S$:

$$\frac{1-(T_p\cdot p)p^{-s}+\sum_{i<j}\alpha_i\alpha_j p^{-2s}-\sum_{i<j<k}\alpha_i\alpha_j\alpha_k p^{-3s}+\dots}{1-T_p p^{1-s}}$$
$$=1+\frac{\sum_{i<j}\alpha_i\alpha_j p^{-2s}-\sum_{i<j<k}\alpha_i\alpha_j\alpha_k p^{-3s}+\dots}{1-T_p p^{1-s}}=:F(p,s)$$

Each of the α_j has modulus p, so for every l, the term in the numerator involving p^{-ls} has modulus at most $\binom{22}{l}p^{l-ls}$. Moreover, for any $s>\frac{3}{2}$ and $p>44^2$, the denominator is larger than $\frac{1}{2}$. Hence for $s>\frac{3}{2}$ and $p>44^2$ the expression $F(p,s)$ is $1+O(p^{-2(s-1)})$. We need to study $\prod_{p\le t}F(p,s)$ as $t\to\infty$ and subsequently $s\to 2$. Writing C for the implicit constant in the bound for $F(p,s)$, we have

$$\prod_{44^2<p\le t}F(p,s)\le\exp\left(C\sum_{44^2<p\le t}p^{-2(s-1)}\right). \tag{2.3}$$

Since for every positive ε, the sum $\sum_{p\le t}p^{-(1+\varepsilon)}$ converges absolutely as $t\to\infty$, so does the sum in the exponential above for any $s>\frac{3}{2}$ and in particular for $s=2$. Therefore, for fixed s, the product of $F(p,s)$ converges absolutely as $t\to\infty$. Moreover, since the inequality (2.3) is uniform in s, we may switch the limits $t\to\infty$ and $s\to 2$ to conclude that $\prod_p F(p,2)$ has a finite, non-zero value. This confirms the statement of the proposition. □

Corollary 2.2.9. *Assuming GRH, and denoting the Picard rank of X by ρ, there is a constant c such that we have $\mathfrak{S}(Q)\sim c(\log Q)^{\rho-1}$.*

Proof. We take the $j=0$ term from Theorem 2.1.3. Proposition 2.2.5 tells us to use $\alpha=r-1$ and Propositions 2.2.7 and 2.2.8 verify $r=\rho$. Now we apply Lemma 2.1.5 with $a=\rho-2$.

Lemma 2.2.3 provides us with an ineffective k to be used in the assumptions of Theorem 2.1.3. In order for the error term in this theorem not to dominate, we need to take $A>k-\alpha=k+1-\rho$. Indeed, the error term in Proposition 2.2.5 allows such a choice of ineffective A. □

Remark 2.2.10. Following our proof, we have to exclude the case $\rho=1$ from our main result. The specific place where the proof falls short is the case $0=\alpha=\rho-1$ in Theorem 2.1.3.

2.3 Evaluating the singular integral

In this section we will show that in the case of diagonal quartics, the singular integral contributes a factor of $\log(B)$ to the counting function.

Recall that the singular integral is

$$\mathfrak{J}(Q) = \int_{-Q}^{Q} \int_{[-1,1]^n} e(\theta F(\mathbf{x})) \mathrm{d}\mathbf{x} \mathrm{d}\theta$$

for some small power $Q = B^{\delta}$.

Our first step is to evaluate the integral

$$\begin{aligned} I(\theta) &= \int_{[-1,1]^4} e\left(\theta \sum_{i=1}^{4} a_i x_i^4\right) \mathrm{d}\mathbf{x} \\ &= \prod_{i=1}^{4} \int_{-1}^{1} e\left(\theta \cdot a_i x_i^4\right) \mathrm{d}x_i \\ &= \prod_{i=1}^{4} 2 \int_{0}^{1} e\left(\theta \cdot a_i x_i^4\right) \mathrm{d}x_i, \end{aligned}$$

hence we focus on the 1-dimensional integral that appears fourfold. We split the calculation into two cases: where $\theta \cdot a_i > 0$ and where $\theta \cdot a_i < 0$ hold.

For $\theta \cdot a_i > 0$ we substitute $u = \theta a_i x_i^4$, transforming the integral into

$$\frac{1}{4(\theta \cdot a_i)^{1/4}} \int_{0}^{\theta a_i} e(u) u^{-3/4} \mathrm{d}u.$$

For $\theta \cdot a_i < 0$ we substitute $u = -\theta a_i x_i^4$, transforming the integral into

$$\frac{1}{4(-\theta \cdot a_i)^{1/4}} \int_{0}^{-\theta a_i} e(-u) u^{-3/4} \mathrm{d}u.$$

Definition 2.3.1. For any $\sigma \in (-1, 0) \subset \mathbb{R}$ and $t \in \mathbb{R}_{>0}$ we introduce notation

$$\begin{aligned} i_\sigma(t) &= \int_{0}^{t} e(u) u^{\sigma} \mathrm{d}u, \\ j_\sigma(t) &= \int_{0}^{t} e(-u) u^{\sigma} \mathrm{d}u = \overline{i_\sigma(t)}. \end{aligned}$$

Using this notation, we have found the validity of

$$\begin{aligned} I(\theta) &= \frac{1}{16} \prod_{i:\theta a_i>0} \frac{1}{(\theta a_i)^{1/4}} i_{-3/4}(\theta a_i) \cdot \prod_{i:\theta a_i<0} \frac{1}{(-\theta a_i)^{1/4}} j_{-3/4}(-\theta a_i) \\ &= \frac{1}{16|\theta|} \prod_i \frac{1}{|a_i|^{1/4}} \prod_{i:\theta\cdot a_i>0} i_{-3/4}(\theta a_i) \prod_{i:\theta\cdot a_i<0} j_{-3/4}(|\theta a_i|). \end{aligned}$$

2.3.1 The integral over theta

We are left with calculating $\int_{-R}^{R} I(\theta)\mathrm{d}\theta$. Without loss of generality we may assume $R > 1$, and we have

$$\begin{aligned} \int_{-R}^{R} I(\theta)\mathrm{d}\theta &= \int_{-R}^{-1} I(\theta)\mathrm{d}\theta + \int_{-1}^{1} I(\theta)\mathrm{d}\theta + \int_{1}^{R} I(\theta)\mathrm{d}\theta \qquad (2.4) \\ &= \int_{-1}^{1} I(\theta)\mathrm{d}\theta \\ &\quad + \frac{1}{8\prod_i |a_i|^{1/4}} \int_1^R \frac{1}{\theta} \Re \left\{ \prod_{i:a_i>0} i_{-3/4}(\theta a_i) \prod_{i:a_i<0} \overline{i_{-3/4}(-\theta a_i)} \right\} \mathrm{d}\theta, \end{aligned}$$

where we have used $I(-\theta) = \overline{I(\theta)}$.

From

$$I(\theta) = \prod_{i=1}^{4} 2 \prod_{i=1}^{4} \int_0^1 e(\theta \cdot a_i x_i^4)\mathrm{d}x_i$$

we see $|I(\theta)| \le 2^4 \int_0^1 |e((\theta \cdot a_i x_i^4)|\mathrm{d}x_i = 16$, hence we may estimate

$$\int_{-1}^{1} I(\theta)\mathrm{d}\theta = O(1).$$

The integral over the interval $(1, R)$ requires further study.

LEMMA 2.3.2. *For every $\sigma \in (-1, 0)$, there exists a constant c_σ such that the function $i_\sigma(t)$ equals $c_\sigma + O(t^\sigma)$ for $t \ge 1$.*

Proof. We write

$$i_\sigma(t) = \int_0^\infty e(u)u^\sigma \mathrm{d}u - \int_t^\infty e(u)u^\sigma \mathrm{d}u$$

and we prove that $\int_0^\infty e(u)u^\sigma \mathrm{d}u =: c_\sigma$ converges and that the second integral can be estimated by $O(t^\sigma)$.

We split each of the integrals into their real and imaginary parts

$$\int_a^b e(u)u^\sigma = \int_a^b \cos(2\pi u)u^\sigma \mathrm{d}u + i\int_a^b \sin(2\pi u)u^\sigma \mathrm{d}u$$

and we argue on the real parts; the calculation on the imaginary parts is completely analogous.

We first bound the integral over $u > t$; we apply integration by parts:

$$\int_t^\infty \cos(2\pi u)u^\sigma \mathrm{d}u = \left[\frac{1}{2\pi}\sin(2\pi u)u^\sigma\right]_t^\infty - \frac{\sigma}{2\pi}\int_t^\infty \sin(2\pi u)u^{\sigma-1}\mathrm{d}u.$$

The latter integral is bounded from above by $\int_t^\infty u^{\sigma-1}\mathrm{d}u = O(t^\sigma)$.

The convergence of $\int_0^\infty e(u)u^\sigma$ is proven by splitting the positive real line into the two parts $(0,1)$ and $\mathbb{R}_{\geq 1}$. It is easily seen that $\int_0^1 \cos(2\pi u)u^\sigma \mathrm{d}u$ converges: it is bounded from above by $\int_0^1 u^\sigma \mathrm{d}u$ which clearly converges for $\sigma > -1$. The integral over $\mathbb{R}_{\geq 1}$ converges by substituting $t = 1$ in the previous calculation. □

Lemma 2.3.2 clearly also applies to the function $j_\sigma(t)$ with constant $\overline{c_\sigma}$. Write $n \leq 4$ for the number of coefficients a_i that are positive and write $c := \Re\left\{c^n_{-3/4}\overline{c_{-3/4}}^{4-n}\right\}$. The last integral in (2.4) is well approximated by $c\int_1^R \frac{1}{\theta}d\theta$, which provides the logarithm that we were out to find.

Proposition 2.3.3. *With the constant c as given above, the singular integral evaluates as*

$$\mathfrak{J}(Q) = \int_{-Q}^{Q} I(\theta)\mathrm{d}\theta = \frac{c}{8\prod_i |a_i|^{1/4}}\log(Q) + O(1).$$

Proof. The proof is no more than following the arguments and calculations in this section in a linear fashion. □

2.3.2 The proof of the main theorem

Proof of Theorem 2.0.1. The proof of the theorem is now a simple combination of the statements of Corollary 2.2.9 and Proposition 2.3.3 with Q a sufficiently small power of B. □

One might notice that we did not specify any choice for δ in the proof of the theorem. Indeed, we did not make any, other than those mentioned for the machinery to work (cf. Remark 1.3.8). Any actual choice will influence the result in the sense that $Q = B^\delta$ will be affected. Secondarily, through the logarithm that appears in the statement of the theorem, the leading constant c_F will depend on said choice, after switching to the variable B. The overall shape of the major arc contribution however, will not.

2.4 Minor arcs and bad subvarieties

As a variation on the concept of *Hardy–Littlewood systems* where the circle method counts rational points in accordance with Manin's conjecture, Vaughan and Wooley [VW95] have introduced what they call *quasi Hardy–Littlewood systems (QHL models)*. The circle method may not work for QHL models in the sense that the minor arcs give a contribution that is not necessarily dominated by the contribution of the major arcs, but the major arcs nonetheless contribute exactly the rational points away from accumulating subvarieties. The contribution of accumulating subvarieties is found in the minor arcs. Vaughan and Wooley observe that many varieties are QHL models; explicit examples include the zero locus of $x_1x_2 = x_3x_4$ (worked out in [VW95] and the zero locus of $x_1^4 + x_2^4 + x_3^4 = y_1^4 + y_2^4 + y_3^4$ (attributed to Wooley in [Con16, p. 14]). In this light it must also be recorded that in [HB98], Heath-Brown was succesfull in separating out the contribution of accumulating subvarieties, using a modified version of the circle method.

After introducing their terminology, Vaughan and Wooley immediately confess that their notion needs to be adapted to include information on the possible failure of the Hasse principle. As originally stated, diagonal quartic surfaces lie outside the range of expected QHL models. However, neither do diagonal cubic surfaces satisfy the original definition of QHL models, but Browning has produced a heuristic showing that for such surfaces the major arcs indeed give the contribution as predicted by Manin's conjecture, albeit with a leading constant that is different from the one predicted by Peyre [Bro09, Chapter 8]. A further adaptation to the notion of QHL models is not unthinkable and it may not be unreasonable to believe that in the case of diagonal quartic surfaces the major arcs indeed reveal the rational points away from accumulating subvarieties.

Chapter 3

The density of fibres with a rational point for a fibration over hypersurfaces of low degree

A victory is twice itself when the achiever brings home full numbers

Leonato, Much Ado About Nothing, Scene 1.1, line 5

This chapter is an adapted version of a paper that is being prepared jointly with Efthymios Sofos, and for which a preprint is available online [SVM18].

3.1 Introduction

Serre's problem [Ser90] regards the density of elements in a family of varieties defined over $\mathbb{Q}$ that have a $\mathbb{Q}$-rational point. Special cases have been considered by Hooley [Hoo93, Hoo07] Poonen–Voloch [PV04], Sofos [Sof16], Browning–Loughran [BL17], and Loughran–Takloo-Bighash–Tanimoto [LTBT17]. The recent investigation of Loughran [Lou13] and Loughran–Smeets [LS16] provides an appropriate formulation of the problem and proves the conjectured upper bound in considerable generality.

Assume that X is a variety over $\mathbb{Q}$ equipped with a dominant morphism $\phi : X \to \mathbb{P}^n_{\mathbb{Q}}$. Letting H denote the usual Weil height on $\mathbb{P}^n(\mathbb{Q})$, Loughran and Smeets conjectured [LS16, Conj.1.6] under suitable assumptions on ϕ, that for all large enough positive t, the cardinality of points $b \in \mathbb{P}^n(\mathbb{Q})$

with height $H(b) \leq t$ and such that the fibre $\phi^{-1}(b)$ has a point in $\mathbb{R}$ and $\mathbb{Q}_p$ for every prime p, has order of magnitude

$$\frac{\#\{b \in \mathbb{P}^n(\mathbb{Q}) : H(b) \leq t\}}{(\log t)^{\Delta(\phi)}}$$

for a non-negative quantity $\Delta(\phi)$ that is defined in [LS16, Eq.(1.3)].

The cardinality of fibres of height t and possessing a $\mathbb{Q}$-rational point is bounded by the quantity they considered, while the two quantities coincide if every fibre satisfies the Hasse principle. The problem of obtaining the conjectured lower bound for the number of fibres of bounded height with a $\mathbb{Q}$-rational point when ϕ is general is considered rather hard because there is no general machinery for producing $\mathbb{Q}$-rational points on varieties.

There are only two instances in the literature of the subject where asymptotics have been proved unconditionally:

- the base of the fibration is a toric variety (Loughran [Lou13]),
- the base of the fibration is a wonderful compactification of an adjoint semi-simple algebraic group (Loughran–Takloo-Bighash–Tanimoto [LTBT17]).

Our aim in this chapter is to extend the list above by proving asymptotics in a case of a rather different nature. The base of the fibration of our main theorem will be a generic hypersurface of large dimension compared to its degree.

3.1.1 The set-up of our results

Let f_1 and f_2 be homogeneous forms in $\mathbb{Z}[t_0, \ldots, t_{n-1}]$, of equal and even degree $d > 0$ subject to some assumptions which are to follow.

We assume that both the projective varieties defined by $f_1(\mathbf{t}) = 0$ and $f_2(\mathbf{t}) = 0$ are smooth. Moreover we assume that the variety defined by $f_1(\mathbf{t}) = f_2(\mathbf{t}) = 0$ is a complete intersection. This is satisfied for generic f_1 and f_2 of fixed degree and in a fixed number of variables. The next condition is artificial in nature but its presence allows to adapt the arguments of Birch [Bir62] to our problem. Letting $\sigma(f_1, f_2)$ denote the dimension of the variety given by

$$\operatorname{rk}\left(\frac{\partial f_i}{\partial x_j}\right)_{0\leq j\leq n-1}^{1\leq i\leq 2}(\mathbf{x}) \leq 1$$

when considered as a subvariety in $\mathbb{A}^n_{\mathbb{C}}$, we shall demand the validity of

$$n - \sigma(f_1, f_2) > 3(d-1)2^d. \tag{3.1}$$

With more work along the lines of the present chapter, most of these assumptions may be removed. However, the assumption that $\deg(f_1)$ is even seems necessary and (3.1) is vital for the entire strategy of the proof. We discuss some possible adaptations after stating the main result of our work.

Remark 3.1.1. We assume that the varieties defined by $f_i(\mathbf{t}) = 0$ are smooth, so they are also irreducible since smooth hypersurfaces in $\mathbb{P}^{n-1}_{\mathbb{Q}}$ are irreducible if $n \geq 3$ holds. In particular we have $n > 12$ by (3.1).

Let $B \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ be the hypersurface given by $f_2(\mathbf{t}) = 0$. We recall that by the work of Birch [Bir62], B satisfies the Hasse principle, and moreover it satisfies weak approximation by work of Browning and Heath-Brown [BHB17]. From now on we also assume $B(\mathbb{Q}) \neq \emptyset$.

For every $i \in \{0, \dots, n-1\}$ consider the subvariety X_i of $\mathbb{P}^2_{\mathbb{Q}} \times \mathbb{A}^{n-1}_{\mathbb{Q}}$ defined by

$$\begin{aligned} x_0^2 + x_1^2 =& f_1(t_0, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_{n-1}) x_2^2, \\ & f_2(t_0, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_{n-1}) = 0. \end{aligned}$$

The maps $g_i : X_i \to B \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ sending a pair

$$((x : y : z), (t_0, \dots, t_{i-1}, 1, t_{i+1}, \dots, t_{n-1}))$$

to $(t_0 : \dots : t_{i-1} : 1 : t_{i+1} : \dots : t_{n-1})$ glue together, defining a projective bundle X over the base B – this uses that f_1 has even degree. By assumption, f_1 is not a multiple of f_2, so the generic fibre of X is smooth.

If we were interested in counting $\mathbb{Q}$-rational points on X then it would be necessary to make a further study into the equations defining a projective embedding of X (as in [FLS18, §2]). Currently however, we are only interested in counting how many fibres of the conic bundle have a $\mathbb{Q}$-rational point. A *conic bundle* is a dominant morphism whose generic fibre is a smooth conic. In this chapter we consider the conic bundle

$$\phi : X \to B \tag{3.2}$$

defined locally by g_i. We shall estimate asymptotically the probability with which the fibre $\phi^{-1}(b)$ has a $\mathbb{Q}$-point as b ranges over $B(\mathbb{Q})$. For this, we define

$$N(\phi, t) := \#\big\{b \in B(\mathbb{Q}) : H(b) \leq t,\ b \in \phi(X(\mathbb{Q}))\big\},\ t \in \mathbb{R}_{>0},$$

where H is the usual naive Weil height on $\mathbb{P}^{n-1}(\mathbb{Q})$.

Remark 3.1.2. Since the degree of f_1 is even, the question if for a given $b \in B$ the fibre $\phi^{-1}(b)$ contains a rational point is independent of a chosen representative.

Consider the small quantity

$$\varepsilon_d := \frac{1}{5(d-1)2^{d+5}}. \tag{3.3}$$

Theorem 3.1.3. *In the set-up above there exists a constant c_ϕ such that for $t \geq 2$ we have*

$$N(\phi, t) = c_\phi \frac{t^{n-d}}{(\log t)^{\frac{1}{2}}} + O\left(\frac{t^{n-d}}{(\log t)^{\frac{1}{2}+\varepsilon_d}}\right).$$

If ϕ has a smooth fibre with a $\mathbb{Q}$-point then c_ϕ is positive. This will be shown in Theorem 3.5.23, where we shall also provide an interpretation for the leading constant c_ϕ. The proof of Theorem 3.1.3 will be given in §3.4.3.

In fact, the assumption that the base B has a rational point could be removed, as Theorem 3.5.23 will show that in this case, the constant c_ϕ would vanish. It is however convenient for our methods to keep the assumption anyway. And indeed, if $B(\mathbb{Q})$ were empty, the study of $N(\phi, t)$ would be a trivial exercise.

Theorem 3.1.3 settles the first case in the literature of an asymptotic for the natural extension of Serre's problem to fibrations over a base that does not have the structure of a toric variety nor a wonderful compactification of an adjoint semi-simple algebraic group. Fibrations that have a basis other than the projective space were also studied in the recent work of Browning and Loughran [BL17, §1.2.2]. In light of the work of Birch [Bir62], our assumptions imply

$$\#\big\{b \in B(\mathbb{Q}) : H(b) \leq t\big\} \asymp t^{n-d}.$$

A very special case of [BL17, Thm 1.4] proves $\lim_{t\to\infty} N(\phi, t)/t^{n-d} = 0$, whereas Theorem 3.1.3 provides asymptotics.

The requirements $\deg(f_1) = \deg(f_2)$ and that the variety $f_1(\mathbf{t}) = f_2(\mathbf{t}) = 0$ is a complete intersection can be removed by adapting some of the arguments in the work of Browning and Heath-Brown [BHB17]. An inspection of our work reveals that the smoothness assumption can be removed at the cost of making the statement Theorem 3.1.3 more involved. Lastly, we should note that our approach can be adapted to varieties of the form $(\mathrm{N}_{K/\mathbb{Q}}(\mathbf{x}) = f_1(b),\ f_2(b) = 0)$, where K is a number field and $\mathrm{N}_{K/\mathbb{Q}}(\mathbf{x})$ is the associated norm form. For this, one would have to replace Proposition 3.3.4 by a version of the results of Odoni [Odo73], where instead of counting integers represented by the norm of K, one counts integers in an arbitrary arithmetic progression and represented by the norm of K. It would be interesting to obtain asymptotics in cases where K fails the Hasse norm principle. A further desirable goal could be that of obtaining asymptotics in cases where the base of the fibration fails weak approximation.

3.1.2 The logarithmic exponent

The exponent of $\log t$ occurring in our result is the one expected in the literature. Indeed, in the works of Loughran and Smeets [LS16, Eq.(1.4)], and Browning and Loughran [BL17, Eq.(1.3)], one may find the expected exponent $\Delta(\phi)$ defined as follows. For any $b \in B$ with residue field $\kappa(b)$, the fibre $X_b = \phi^{-1}(b)$ is called *pseudo-split* if every element of $\mathrm{Gal}(\overline{\kappa(b)}/\kappa(b))$ fixes some multiplicity-one irreducible component of $X_b \times \mathrm{Spec}(\overline{\kappa(b)})$. The fibre X_b is called *split* if it contains a multiplicity-one irreducible component that is also geometrically irreducible. Note that a split fibre is always pseudo-split and further note that for conic bundles these two notions are the same as the singular fibres are either double lines, or two lines intersecting.

Now for every codimension one point $D \in B^{(1)}$ choose a finite group Γ_D through which the action of $\mathrm{Gal}(\overline{\kappa(D)}/\kappa(D))$ on the irreducible components of $X_{\overline{\kappa(D)}}$ factors. Let Γ_D° be the subset of elements of Γ_D which fix some multiplicity one irreducible component. One sets $\delta_D = \#\Gamma_D^\circ/\#\Gamma_D$ and

$$\Delta(\phi) = \sum_{D\in B^{(1)}} \big(1 - \delta_D\big).$$

By considering the possible singular fibres, it is clear that for a conic bundle, δ_D is different from 1 if and only if D is non-split, in which case it is either 0 (if the fibre is a double line) or $\frac{1}{2}$.

In all the cases in the literature so far the exponent of $(\log t)^{-1}$ turns out to be Δ. Indeed, this is also the case here. The only relevant codimension one point to consider is $D := Z(f_1, f_2)$; every other fibre is smooth and hence split. Suppose that D is geometrically reducible, then the intersection between any two geometrically irreducible components lies in the singular locus of D, say D^{sing}. Being the intersection between varieties in projective space of codimension at most 2, its codimension is at most 4.

The affine cone above D^{sing} is a subvariety of the affine variety defined by

$$\mathrm{rk}\left(\frac{\partial f_i}{\partial x_j}\right)_{0\leq j\leq n-1}^{1\leq i\leq 2}(\mathbf{x}) \leq 1.$$

As a subvariety, the affine cone over D^{sing} has dimension at most $\sigma(f_1, f_2)$, so its codimension is at least $n-\sigma(f_1, f_2)$. Hence the codimension of D^{sing} in $\mathbb{P}^n_{\mathbb{Q}}$ is at least $n - \sigma(f_1, f_2) - 1$. Thus we are led to an inequality

$$4 \geq n - \sigma(f_1, f_2) - 1 > 3(d-1)2^d - 1 \geq 11,$$

violating the combined assumptions (3.1) and $d \geq 2$. We conclude that D is geometrically irreducible.

The fibre above D is given by $x^2+y^2 = 0$ over the function field $\kappa(D)$ and it is split if and only if -1 is a square in $\kappa(D)$. However, it is well known that the function field of a geometrically irreducible variety is primary: it contains no non-trivial separable algebraic extensions of the base field. Since -1 is not a square in $\mathbb{Q}$, neither is it in $\kappa(D)$. Therefore, under the assumptions of Theorem 3.1.3 we find $\Delta(\phi) = \delta_D = \frac{1}{2}$.

NOTATION 3.1.4. As usual, we denote the divisor, Euler and Möbius functions by τ, φ and μ. We shall make frequent use of the estimates

$$\tau(m) \ll m^{\frac{1}{\log\log m}} \tag{3.4}$$

and

$$\varphi(m) \gg m/\log\log m \tag{3.5}$$

found in [Ten95, Th.5.4] and [Ten95, Th.5.6] respectively.

We consider the forms f_1 and f_2 fixed throughout the chapter, thus the implied constants in the Vinogradov/Landau notation $\ll$, $O(\cdot)$ are allowed to depend on ϕ, f_1, f_2, n and d without further mention. Any dependence of the implied constants on other parameters will be explicitly recorded by the appropriate use of a subscript.

For $z \in \mathbb{C}$ we let

$$\mathrm{e}(z) := \exp(2\pi i z).$$

The symbol $v_p(m)$ will refer to the standard p-adic valuation of an integer m. Lastly, we shall use the Ramanujan sum, defined for $a \in \mathbb{Z}$ and $q \in \mathbb{Z}_{>0}$ as

$$c_q(a) := \sum_{x \in (\mathbb{Z}/q\mathbb{Z})^*} \mathrm{e}(ax/q). \tag{3.6}$$

Denoting the indicator function of a condition A by $\mathbf{1}_A$, we have the following equality:

$$c_{p^m}(a) = p^{m-1}\big(p\mathbf{1}_{v_p(a)\geq m} - \mathbf{1}_{v_p(a)\geq m-1}\big), \ (p \text{ prime}, a \in \mathbb{Z}, m \geq 1). \tag{3.7}$$

When we write $|\mathbf{x}|$, we will mean $\max\{|x_i|\}$. Lastly, we shall make frequent use of the constant

$$\mathcal{C}_0 := \prod_{\substack{p \text{ prime} \\ p \equiv 3 (\mathrm{mod}\ 4)}} \Big(1 - \frac{1}{p^2}\Big)^{1/2}. \tag{3.8}$$

Acknowledgements This work started while Efthymios Sofos had a position at Leiden University. It was completed while Erik Visse–Martindale was visiting the Max Planck Institute in Bonn, the hospitality of which is greatly acknowledged. The authors are very grateful to Daniel Loughran for useful comments that helped improve the introduction and §3.5.4.

3.2 Using the Hardy–Littlewood circle method for Serre's problem

We begin by estimating the main quantity in Theorem 3.1.3 by averages of an arithmetic function over a thin subset of integer vectors. Let us first define $\vartheta_{\mathbb{Q}} : \mathbb{Z} \to \{0, 1\}$ as the indicator function of those integers m such

that the curve $x_0^2 + x_1^2 = mx_2^2$ has a point over $\mathbb{Q}$. For $P \in \mathbb{R}_{>0}$ we let

$$\Theta_{\mathbb{Q}}(P) := \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \cap P[-1,1]^n \\ f_1(\mathbf{x}) \neq 0, f_2(\mathbf{x}) = 0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{x})). \tag{3.9}$$

In order to go from $\mathbb{Q}$-solutions to coprime $\mathbb{Z}$-solutions, we perform a standard Möbius transformation, where we cut off the range of summation at the price of an error term. This is the content of the following lemma.

LEMMA 3.2.1. *Under the assumptions of Theorem 3.1.3 we have*

$$N(\phi, t) = \frac{1}{2} \sum_{l \in \mathbb{Z} \cap [1, \log t]} \mu(l) \Theta_{\mathbb{Q}}(t/l) + O(t^{n-d} (\log t)^{-1}).$$

Proof. For any $b \in \mathbb{P}^n(\mathbb{Q})$ there exists a unique, up to sign, $\mathbf{y} \in \mathbb{Z}^n$ with $\gcd(y_0, \ldots, y_{n-1}) = 1$ and $b = [\pm \mathbf{y}]$. Recalling that the degree of f_1 is even, allows to infer that the fibre $\phi^{-1}(b)$ has a rational point if and only if $\vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = 1$ holds, hence $N(\phi, t)$ equals

$$\frac{1}{2} \#\{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n : \gcd(y_0, \ldots, y_{n-1}) = 1, f_2(\mathbf{y}) = 0, \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = 1\}.$$

For $\mathbf{y}$ such that $f_1(\mathbf{y}) = 0$ holds, we have $\vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = 1$ since $(0:0:1)$ is a point in $\phi^{-1}([\mathbf{y}])$. Therefore the quantity above is

$$\frac{1}{2} \sum_{\substack{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n \\ \gcd(y_0, \ldots, y_{n-1}) = 1 \\ f_2(\mathbf{y}) = 0, f_1(\mathbf{y}) \neq 0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) + O(\#\{\mathbf{y} \in \mathbb{Z}^n \cap [-t,t]^n : f_1(\mathbf{y}) = f_2(\mathbf{y}) = 0\}).$$

The assumption (3.1) allows to apply Lemma 1.3.36 with $R = 2$ to immediately obtain

$$\#\{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n : f_1(\mathbf{y}) = f_2(\mathbf{y}) = 0\} \ll t^{n-2d}.$$

Thus we obtain equality of $N(\phi, t)$ with

$$\frac{1}{2} \sum_{\substack{\mathbf{y} \in \mathbb{Z}^n \cap t[-1,1]^n \\ \gcd(y_0, \ldots, y_{n-1}) = 1 \\ f_1(\mathbf{y}) \neq 0, f_2(\mathbf{y}) = 0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) + O(t^{n-2d}).$$

Using Möbius inversion and letting $\mathbf{y} = l\mathbf{x}$ we see that the sum over $\mathbf{y}$ equals

$$\sum_{\substack{\mathbf{y}\in\mathbb{Z}^n\cap t[-1,1]^n\\ f_1(\mathbf{y})\neq 0, f_2(\mathbf{y})=0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) \sum_{\substack{l\in\mathbb{Z}_{>0}\\ l|\mathbf{y}}} \mu(l) = \sum_{l\leq t}\mu(l) \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\cap \frac{t}{l}[-1,1]^n\\ f_1(\mathbf{x})\neq 0, f_2(\mathbf{x})=0}} \vartheta_{\mathbb{Q}}(f_1(\mathbf{x})),$$

because $\vartheta_{\mathbb{Q}}(f_1(\mathbf{y})) = \vartheta_{\mathbb{Q}}(f_1(\mathbf{x}))$ holds due to $\deg(f_1)$ being even. Hence we have

$$N(\phi, t) = \frac{1}{2}\sum_{l\in\mathbb{Z}\cap[1,t]} \mu(l)\Theta_{\mathbb{Q}}(t/l) + O(t^{n-2d}),$$

and now the use of (3.1) and Lemma 1.3.36 for $R = 1$ yields

$$|\Theta_{\mathbb{Q}}(t)| \leq \#\{\mathbf{y}\in\mathbb{Z}^n\cap t[-1,1]^n : f_2(\mathbf{y}) = 0\} \ll t^{n-d},$$

which shows that the collective contribution from large l is

$$\begin{aligned}\Big|\sum_{l\in\mathbb{Z}_{>0}\cap(\log t, t]} \mu(l)\Theta_{\mathbb{Q}}(t/l)\Big| &\ll \sum_{l>\log t}(t/l)^{n-d} \ll t^{n-d}\sum_{l>\log t} l^{-2}\\ &\ll t^{n-d}(\log t)^{-1},\end{aligned}$$

where we used that $n - d \geq 2$ holds due to (3.1). □

For $m < 0$ the curve $x_0^2 + x_1^2 = mx_2^2$ has no $\mathbb{R}$-point, and therefore no $\mathbb{Q}$-point, in other words: $\vartheta_{\mathbb{Q}}(m) = 0$. Thus, writing $\max\{f_1([-1,1]^n)\}$ for $\max\{f_1(\mathbf{t}) : \mathbf{t}\in[-1,1]^n\}$, it is evident that we have the equality

$$\Theta_{\mathbb{Q}}(P) = \sum_{\substack{m\in\mathbb{Z}_{>0}\\ m\leq\max\{f_1([-1,1]^n)\}P^d}} \vartheta_{\mathbb{Q}}(m) \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n\cap P[-1,1]^n\\ f_1(\mathbf{x})=m, f_2(\mathbf{x})=0}} 1.$$

Writing $\mathrm{d}\boldsymbol{\alpha}$ for $\mathrm{d}\alpha_1\mathrm{d}\alpha_2$ and using the identity

$$\int_{\boldsymbol{\alpha}\in[0,1)^2} \mathrm{e}(\alpha_1(f_1(\mathbf{x})-m)+\alpha_2 f_2(\mathbf{x}))\mathrm{d}\boldsymbol{\alpha} = \begin{cases}1, & \text{if } f_1(\mathbf{x}) = m \text{ and } f_2(\mathbf{x}) = 0,\\ 0, & \text{otherwise,}\end{cases}$$

shows the validity of

$$\Theta_{\mathbb{Q}}(P) = \int_{\boldsymbol{\alpha}\in[0,1)^2} S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\mathrm{d}\boldsymbol{\alpha}, \tag{3.10}$$

where one uses the notation

$$S(\boldsymbol{\alpha}) := \sum_{\mathbf{x}\in\mathbb{Z}^n\cap P[-1,1]^n} \mathrm{e}(\alpha_1 f_1(\mathbf{x}) + \alpha_2 f_2(\mathbf{x})) \tag{3.11}$$

and

$$E_{\mathbb{Q}}(\alpha_1) := \sum_{\substack{m\in\mathbb{Z}_{>0}\\ m\leq \max\{f_1([-1,1]^n)\}P^d}} \vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(\alpha_1 m) \tag{3.12}$$

to match the notation in Birch's work as outlined in §1.3.3. One has the obvious bound $E_{\mathbb{Q}}(\alpha_1) \ll P^d$ from the triangle inequality.

Recall the notation from Definition 1.3.24. We pick small positive θ_0 and δ as in (1.7) and (1.8), that is, such that we have $1 > \delta + 16\theta_0$ and $\frac{n-\sigma}{2^d} - 3(d-1) > \delta\theta_0^{-1}$. By the triangle inequality we have

$$\int_{\boldsymbol{\alpha}\notin\mathcal{M}(\theta_0)} \big|S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\big|\mathrm{d}\boldsymbol{\alpha} \leq \Big(\int_{\boldsymbol{\alpha}\notin\mathcal{M}(\theta_0)} |S(\boldsymbol{\alpha})|\mathrm{d}\boldsymbol{\alpha}\Big) \max_{\alpha_1\in[0,1)} |E_{\mathbb{Q}}(\alpha_1)|,$$

hence applying the result of Lemma 1.3.27 on the first factor, and using the trivial bound $E_{\mathbb{Q}}(\alpha_1) \ll P^d$ leads to the following bound on the integral away from $\mathcal{M}(\theta_0)$:

$$\int_{\boldsymbol{\alpha}\notin\mathcal{M}(\theta_0)} \big|S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\big|\mathrm{d}\boldsymbol{\alpha} \ll P^{n-d-\delta}.$$

By (3.10) this shows

$$\Theta_{\mathbb{Q}}(P) = \int_{\boldsymbol{\alpha}\in\mathcal{M}(\theta_0)} S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\mathrm{d}\boldsymbol{\alpha} + O(P^{n-d-\delta}).$$

Consistently modifying the setup, the following lemma is analogous to Lemma 1.3.29 and its proof is the same, using the notation introduced above. The essence of the lemma is the statement that in the expression for $\Theta_{\mathbb{Q}}(P)$ above, we may slightly modify the intervals of integration such that they are still disjoint.

LEMMA 3.2.2. *For any θ_0, δ satisfying* (1.7) *and* (1.8) *and under the assumptions of Theorem 3.1.3 we have*

$$\Theta_{\mathbb{Q}}(P) = \sum_{q\leq P^{2(d-1)\theta_0}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \int_{\mathcal{M}'_{\mathbf{a},q}(\theta_0)} S(\boldsymbol{\alpha})\overline{E_{\mathbb{Q}}(\alpha_1)}\mathrm{d}\boldsymbol{\alpha} + O(P^{n-d-\delta}),$$

where the modified set $\mathcal{M}'_{\mathbf{a},q}(\theta_0)$ consists of those $\boldsymbol{\alpha}\in[0,1]^2$ satisfying $|q\alpha_i - a_i| \leq qP^{-d+2(d-1)\theta_0}$.

Proof. Every modified interval $\mathcal{M}'_{\mathbf{a},q}(\theta_0)$ extends the associated interval $\mathcal{M}_{\mathbf{a},q}(\theta_0)$, so the estimate of the integral away from these intervals remains valid. One should only check that the modified intervals do not overlap. □

For $\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2$, write

$$S_{\mathbf{a},q} := \sum_{\mathbf{x} \in (\mathbb{Z} \cap [0,q))^n} \mathrm{e}\Big(\frac{a_1 f_1(\mathbf{x}) + a_2 f_2(\mathbf{x})}{q}\Big), \tag{3.13}$$

and for $\mathbf{\Gamma} \in \mathbb{R}^2$ define

$$I(\mathbf{\Gamma}) := \int_{\boldsymbol{\zeta} \in [-1,1]^n} \mathrm{e}(\Gamma_1 f_1(\boldsymbol{\zeta}) + \Gamma_2 f_2(\boldsymbol{\zeta}))\mathrm{d}\boldsymbol{\zeta}. \tag{3.14}$$

Recalling the notation $\eta = 2(d-1)\theta_0$, we now employ Lemma 1.3.32 with $\boldsymbol{\nu} = 0$ to evaluate $S(\alpha)$ and to see that under the assumptions of Lemma 3.2.2, with $\boldsymbol{\beta} := \boldsymbol{\alpha} - \mathbf{a}/q$, we have

$$\begin{aligned}\Theta_{\mathbb{Q}}(P) - P^n \sum_{q \le P^{2(d-1)\theta_0}} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\boldsymbol{\beta}| \le P^{-d+\eta}} I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1 + a_1/q)}\mathrm{d}\boldsymbol{\beta} \\ \ll P^{n-d-\delta} + P^{n-1+2\eta} \sum_{q \le P^\eta} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} \int_{|\boldsymbol{\beta}| \le P^{-d+\eta}} |E_{\mathbb{Q}}(\beta_1 + a_1/q)|\mathrm{d}\boldsymbol{\beta}.\end{aligned}$$

By using $E_{\mathbb{Q}}(\alpha) \ll P^d$ once more we infer that the sum over q in the error term above is

$$\ll \sum_{q \le P^\eta} q^2 P^{2(-d+\eta)} P^d \ll P^{-d+5\eta},$$

hence we have proved the following lemma.

LEMMA 3.2.3. *Under the assumptions of Lemma 3.2.2,* $\Theta_{\mathbb{Q}}(P)P^{-n+d}$ *is*

$$\sum_{q \le P^\eta} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\boldsymbol{\beta}| \le P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1 + a_1/q)}\mathrm{d}\boldsymbol{\beta}$$

up to an error term that is $O(P^{-\delta} + P^{-1+7\eta})$.

Proof. The proof consists merely of the calculations above. □

3.3 Exponential sums with terms detecting the existence of rational points

In this section we write x for $\max\{f_1([-1,1]^n)\}P^d$. As made clear by Lemma 3.2.3, to verify Theorem 3.1.3 we will asymptotically estimate the expression

$$E_{\mathbb{Q}}\Big(\frac{a_1}{q}+\beta_1\Big)=\sum_{\substack{m\in\mathbb{Z}_{>0}\cap[1,x]\\ x_0^2+x_1^2=mx_2^2 \text{ has a } \mathbb{Q}\text{-point}}} \mathrm{e}\left(\left(\frac{a_1}{q}+\beta_1\right)m\right),$$

for integers a_1, q, $\beta_1 \in \mathbb{R}$, and $x \in \mathbb{R}_{\geq 1}$. It suffices to first study the case $\beta_1 = 0$, and then to apply Lemma 3.3.7 at the end of this section. To study $E_{\mathbb{Q}}(a_1/q)$ we shall rephrase the condition on m in a way that it only regards the prime factorisation of m and then use the Rosser–Iwaniec sieve.

We begin by applying the formulas regarding Hilbert symbols in [Ser73, Ch.III,Th.1], which show that for strictly positive integers m one has

$$\vartheta_{\mathbb{Q}}(m)=\begin{cases}1, & \text{if } p\equiv 3 \,(\mathrm{mod}\ 4)\Rightarrow v_p(m)\equiv 0\,(\mathrm{mod}\ 2)\,,\\ 0, & \text{otherwise.}\end{cases} \tag{3.15}$$

Indeed, for $m \in \mathbb{Z}_{>0}$, the curve $x_0^2+x_1^2 = mx_2^2$ defines a smooth conic in $\mathbb{P}^2_{\mathbb{Q}}$ with an $\mathbb{R}$-point and the Hasse principle combined with Hilbert's product formula [Ser73, Ch.III,Th.3] proves (3.15). The function in (3.15) is the characteristic function of those integers m that are sums of two integral squares, see [Ten95, §4.8]. Landau [Ten95, Eq.(4.90)] proved the following asymptotic:

$$\sum_{1\leq m\leq x}\vartheta_{\mathbb{Q}}(m)=\frac{1}{2^{1/2}\mathcal{C}_0}\frac{x}{(\log x)^{1/2}}+O\bigg(\frac{x}{(\log x)^{3/2}}\bigg),\ x\in\mathbb{R}_{>1}, \tag{3.16}$$

but this is not sufficient for us since we will need a similar result restricted to those m in an arithmetic progression. Observe that the following holds

due to periodicity:

$$E_{\mathbb{Q}}\Big(\frac{a_1}{q}\Big) = \sum_{\substack{m\in\mathbb{Z}_{>0}\cap[1,x]\\ x_0^2+x_1^2=mx_2^2 \text{ has a } \mathbb{Q}\text{-point}}} \mathrm{e}\left(\frac{a_1}{q}m\right)$$
$$= \sum_{\ell\in\mathbb{Z}\cap[0,q)} \mathrm{e}(a_1\ell/q) \sum_{\substack{1\le m\le x\\ m\equiv\ell \pmod q}} \vartheta_{\mathbb{Q}}(m).$$

The work of Rieger [Rie65, Satz 1] could now be invoked to study the sum over $m \equiv \ell \pmod q$ when $\gcd(\ell, q) = 1$. One could attempt to use this to get asymptotic formulas for the cases with $\gcd(\ell, q) > 1$. However, we found it more straightforward to work instead with the function ϖ in place of $\vartheta_{\mathbb{Q}}$. This function $\varpi : \mathbb{Z}_{>0} \to \{0, 1\}$ is defined as

$$\varpi(m) := \begin{cases} 1, & \text{if } p \mid m \Rightarrow p \equiv 1 \pmod 4, \\ 0, & \text{otherwise.} \end{cases} \tag{3.17}$$

It is obvious that for all $m, k \in \mathbb{Z}_{>0}$ we have

$$\varpi(mk) = \varpi(m)\varpi(k) \tag{3.18}$$

so ϖ is completely multiplicative, while $\vartheta_{\mathbb{Q}}$ is merely multiplicative (to see this take $m = k = p$, where p is any prime which is $3 \pmod 4$). This is the reason for choosing to work with ϖ rather than $\vartheta_{\mathbb{Q}}$. Our next lemma shows how one can replace $\vartheta_{\mathbb{Q}}$ by ϖ, while simultaneously restricting the summation at the price of an error term.

LEMMA 3.3.1. *For $x, u \in \mathbb{R}_{\ge 1}$, $q \in \mathbb{Z}_{>0}$, $a_1 \in \mathbb{Z} \cap [0, q)$ we have*

$$\sum_{1\le m\le x} \vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q) = \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\ge 0}\\ 2^tk^2\le u\\ p\mid k\Rightarrow p\equiv 3 \pmod 4}} \sum_{\ell\in\mathbb{Z}\cap[0,q)} \mathrm{e}(a_1\ell/q) \sum_{\substack{r\in\mathbb{Z}_{>0}\\ 2^tk^2r\equiv\ell \pmod q\\ 1\le r\le x2^{-t}k^{-2}}} \varpi(r)$$

up to an error term that is $O\Big(\frac{x}{\sqrt{u}}\Big)$ with an absolute implied constant.

Proof. It is easy to see that for positive m one has $\vartheta_{\mathbb{Q}}(m) = 1$ if and only if we can write $m = 2^tk^2r$ for $t \in \mathbb{Z}_{\ge 0}$, k a positive integer all of whose

primes are $3 \pmod 4$ and r which satisfies $\varpi(r) = 1$. This shows that the sum over m is

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \sum_{\substack{r\in\mathbb{Z}_{>0}\\ 1\leq r\leq x2^{-t}k^{-2}}} \varpi(r)\,\mathrm{e}(a_1 2^t k^2 r/q).$$

The contribution of the pairs (k,t) with $2^t k^2 > u$ is at most

$$\sum_{t\geq 0}\sum_{k>\sqrt{u2^{-t}}} x2^{-t}k^{-2} < 2x\sum_{t\geq 0}\frac{2^{-t}}{\sqrt{u2^{-t}}} \ll \frac{x}{\sqrt{u}},$$

where the (first) inequality comes from Lemma 3.3.2.

Noting that $\mathrm{e}(a_1 2^t k^2 r/q)$ as a function of r is periodic modulo q allows to partition all r in congruences $\ell \in \mathbb{Z}/q\mathbb{Z}$, thus concluding the proof. □

Lemma 3.3.2. *For any $a \in \mathbb{R}_{>0}$ we have*

$$Z_a := \sum_{k\in\mathbb{Z}_{>a}} k^{-2} < 2a^{-1}.$$

Proof. For $a \geq 2$ we estimate the sum as a lower sum of the associated integral:

$$\sum_{k\in\mathbb{Z}_{>a}} k^{-2} \leq \int_{\lfloor a\rfloor}^{\infty} t^{-2}\mathrm{d}t = \lfloor a\rfloor^{-1}.$$

If a is an integer, then $\lfloor a\rfloor^{-1} < 2a^{-1}$ is obvious. If a is not an integer, then we have $\lfloor a\rfloor^{-1} = \lceil a-1\rceil^{-1} < (a-1)^{-1} < 2a^{-1}$ since a was at least 2.

We only still need to prove the statement for $a \in (0,2)$, for which we consider the sum separately. For $a \in (0,1)$ we have $Z_a = \zeta(2) < 2 < 2a^{-1}$ and for $a \in [1,2)$ we have $Z_a = \zeta(2) - 1 < 1 < 2a^{-1}$ again. □

The terms in the sum involving ϖ in Lemma 3.3.1 are in an arithmetic progression that is not necessarily primitive. We next show that we can reduce the evaluation of these sums to similar expressions where the summation is over an arithmetic progression that is primitive. The property (3.18) will be used for this.

LEMMA 3.3.3. *Let $t \in \mathbb{Z}_{\geq 0}$, $q \in \mathbb{Z}_{>0}$, $\ell \in \mathbb{Z} \cap [0, q)$ and $k \in \mathbb{Z}_{>0}$ be such that every prime divisor of k is $3 \pmod 4$. For $y \in \mathbb{R}_{>0}$ consider the sum*

$$\sum_{\substack{r \in \mathbb{Z}_{>0} \cap [1,y] \\ 2^t k^2 r \equiv \ell \pmod q}} \varpi(r).$$

The sum vanishes if $\gcd(2^t k^2, q) \nmid \ell$ holds, and it otherwise equals

$$\varpi\Big(\frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)}\Big) \sum_{\substack{s \in \mathbb{Z}_{>0} \cap [1, y \gcd(2^t k^2, q) \gcd(\ell, q)^{-1}] \\ \frac{2^t k^2}{\gcd(2^t k^2, q)} s \equiv \frac{\ell}{\gcd(\ell, q)} \left(\mathrm{mod}\ \frac{q}{\gcd(\ell, q)}\right)}} \varpi(s).$$

Proof. If $\gcd(2^t k^2, q) \nmid \ell$ then the congruence $2^t k^2 r \equiv \ell \pmod q$ does not have a solution r, in which case the sum over r vanishes. On the other hand, if $\gcd(2^t k^2, q)$ divides ℓ, then we see that the congruence for r can be written equivalently as

$$\frac{2^t k^2}{\gcd(2^t k^2, q)} r \equiv \frac{\ell}{\gcd(2^t k^2, q)} \left(\mathrm{mod}\ \frac{q}{\gcd(2^t k^2, q)}\right).$$

Note that any solution r of this must necessarily satisfy

$$\gcd\Big(\frac{\ell}{\gcd(2^t k^2, q)}, \frac{q}{\gcd(2^t k^2, q)}\Big) \Big| \frac{2^t k^2}{\gcd(2^t k^2, q)} r,$$

the left-hand gcd being equal to $\gcd(\ell, q) \gcd(2^t k^2, q)^{-1}$. The fact of

$$\gcd\Big(\frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)}, \frac{2^t k^2}{\gcd(2^t k^2, q)}\Big) = 1$$

shows that r must be divisible by $\gcd(\ell, q) \gcd(2^t k^2, q)^{-1}$. Therefore there exists an $s \in \mathbb{Z}_{>0}$ with

$$r = \frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)} s$$

and substituting this into the sum over r in our lemma concludes the proof because

$$\varpi(r) = \varpi\Big(\frac{\gcd(\ell, q)}{\gcd(2^t k^2, q)}\Big) \varpi(s)$$

holds due to the complete multiplicativity seen in (3.18). □

We are now in a position to apply [FI10, Th.14.7], which is a result on the distribution of the function ϖ along primitive arithmetic progressions and which we include as a proposition for the convenience of the reader. We first introduce the following notation for $Q \in \mathbb{Z}_{>0}$:

$$\dot{Q} := \prod_{p \equiv 1 (\mathrm{mod}\ 4)} p^{v_p(Q)} \text{ and } \ddot{Q} := \prod_{p \equiv 3 (\mathrm{mod}\ 4)} p^{v_p(Q)}. \tag{3.19}$$

Proposition 3.3.4 ([FI10] Th.14.7). *Let Q be a positive integer multiple of 4, let $a \equiv 1 \,(\mathrm{mod}\ 4)$ satisfy $\gcd(a, Q) = 1$, and let z be any real number with $z \geq Q$. Then*

$$\sum_{\substack{r \in \mathbb{Z}_{>0} \cap [1,z] \\ r \equiv a (\mathrm{mod}\ Q)}} \varpi(r) = 2^{1/2} \mathcal{C}_0 \frac{\ddot{Q}}{\varphi(\ddot{Q})} \frac{z}{Q\sqrt{\log z}} \left\{ 1 + O\left(\left(\frac{\log Q}{\log z} \right)^{1/7} \right) \right\}$$

holds with an absolute implied constant.

Remark 3.3.5. This result is proven using the semi-linear Rosser–Iwaniec sieve. We should remark that there is a typo in the reference, namely[FI10, Eq.(14.22)] should instead read

$$V(D) = \prod_{2<p<D} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}} \prod_{p<D} \left(1 - \frac{\chi(p)}{p}\right)^{-\frac{1}{2}} \prod_{\substack{2<p<D \\ p \equiv 3 (\mathrm{mod}\ 4)}} \left(1 - \frac{1}{p^2}\right)^{\frac{1}{2}},$$

and as a result, [FI10, Eq.(14.39)] must be replaced by the asymptotic in Proposition 3.3.4. After fixing this typo, one can show, as in the proof of [FI10, Eq.(14.24)], that for $D \geq 2$, we have

$$\prod_{\substack{p<D \\ p \equiv 3 (\mathrm{mod}\ 4)}} \left(1 - \frac{1}{p}\right) = \frac{\sqrt{\pi}}{\sqrt{2}\exp(\gamma)} \mathcal{C}_0 \frac{1}{\sqrt{\log D}} + O\left(\frac{1}{(\log D)^{3/2}}\right). \tag{3.20}$$

There is a further typo in [FI10, Eq.(14.26)], namely, $c\sqrt{2}$ should be replaced by $2^{1/2}\mathcal{C}_0/4$.

We will now proceed to the application of Proposition 3.3.4. For any

$q \in \mathbb{Z}_{>0}, a_1 \in \mathbb{Z} \cap [0,q)$ define

$$\mathfrak{F}(a_1,q) := \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \frac{\gcd(2^t k^2,q)}{2^t k^2} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell \\ (3.22)}} \frac{\varpi\big(\frac{\gcd(\ell,q)}{\gcd(2^t k^2,q)}\big)\,\mathrm{e}\left(\frac{a_1\ell}{q}\right)}{\gcd(\ell,q)\mathrm{lcm}\big(4,\frac{q}{\gcd(\ell,q)}\big)} \times \prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ v_p(q)>v_p(\ell)}} \Big(1-\frac{1}{p}\Big)^{-1}, \tag{3.21}$$

where ℓ in the summation satisfies

$$\frac{2^t k^2}{\gcd(2^t k^2,q)} \equiv \frac{\ell}{\gcd(\ell,q)} \left(\mathrm{mod}\ \gcd\Big(4,\frac{q}{\gcd(\ell,q)}\Big)\right). \tag{3.22}$$

The result of the following lemma aims to separate out the dependence on x from the apparent pandemonium that is hidden in $\mathfrak{F}(a_1,q)$.

Lemma 3.3.6. *For $x \in \mathbb{R}_{\geq 1}$, $A \in \mathbb{R}_{>0}, q \in \mathbb{Z}_{>0}, a_1 \in \mathbb{Z}\cap[0,q)$ with $q \leq (\log x)^A$ we have*

$$\sum_{\substack{m\in\mathbb{Z}\cap[1,x]\\ x_0^2+x_1^2=mx_2^2 \text{ has}\\ a\ \mathbb{Q}\text{-point}}} \mathrm{e}\left(a_1\frac{m}{q}\right) = 2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)\frac{x}{(\log x)^{1/2}} + O_A\left(\frac{q^3 x}{(\log x)^{1/2+1/7}}\right),$$

where the implied constant depends at most on A.

Proof. Combining Lemma 3.3.1 with $u = (\log x)^{100}$ and Lemma 3.3.3 shows that, up to an error term which is $\ll x(\log x)^{-50}$, the sum over m in our lemma equals

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^t k^2\leq(\log x)^{100}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell}} \varpi\Big(\frac{\gcd(\ell,q)}{\gcd(2^t k^2,q)}\Big)\,\mathrm{e}(a_1\ell/q) \times \sum_{\substack{s\in\mathbb{Z}_{>0}\cap[1,x2^{-t}k^{-2}\gcd(2^t k^2,q)\gcd(\ell,q)^{-1}]\\ \frac{2^t k^2}{\gcd(2^t k^2,q)}s\equiv\frac{\ell}{\gcd(\ell,q)}\left(\mathrm{mod}\ \frac{q}{\gcd(\ell,q)}\right)}} \varpi(s).$$

We note that $\varpi(s)$ vanishes unless s satisfies $s \equiv 1 \,(\mathrm{mod}\ 4)$. This means that we can add the condition $s \equiv 1 \,(\mathrm{mod}\ 4)$ in the last sum over s, thus

resulting with the double congruence

$$s \equiv 1 \,(\mathrm{mod}\ 4)\,, \frac{2^t k^2}{\gcd(2^t k^2, q)} s \equiv \frac{\ell}{\gcd(\ell, q)} \left(\mathrm{mod}\ \frac{q}{\gcd(\ell, q)}\right).$$

By the Chinese remainder theorem this has a solution if and only if (3.22) is satisfied. Assuming that this happens, the solution is unique modulo

$$Q := \mathrm{lcm}\Big(4, \frac{q}{\gcd(\ell, q)}\Big).$$

Hence by Proposition 3.3.4 we get that the sum over m in our lemma equals

$$\begin{aligned}\mathrm{MT} :&= 2^{1/2}\mathcal{C}_0 \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^t k^2 \leq (\log x)^{100}\\ p|k \Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q),(3.22)\\ \gcd(2^t k^2, q)|\ell}} \varpi\Big(\frac{\gcd(\ell,q)}{\gcd(2^t k^2, q)}\Big)\, \mathrm{e}(a_1\ell/q)\\ &\times \frac{\ddot{Q}}{\varphi(\ddot{Q})} \frac{1}{\mathrm{lcm}(4, q/\gcd(\ell,q))} \frac{x 2^{-t} k^{-2} \gcd(2^t k^2, q)\gcd(\ell,q)^{-1}}{\sqrt{\log(x 2^{-t} k^{-2}\gcd(2^t k^2, q)\gcd(\ell,q)^{-1})}}\end{aligned}$$

up to an error term which is

$$\begin{aligned}&\ll \frac{x}{(\log x)^{50}} \qquad (3.23)\\ &+ \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^t k^2 \leq (\log x)^{100}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell\\ (3.22)}} (\log\log\ddot{Q}) \frac{x 2^{-t}k^{-2}\gcd(2^t k^2, q)}{\gcd(\ell,q)\sqrt{\log x}} \Big(\frac{\log Q}{\log x}\Big)^{1/7}\end{aligned}$$

owing to (3.5), which gives $\ddot{Q}/\varphi(\ddot{Q}) \ll \log\log\ddot{Q} \leq \log\log Q$, combined with the trivial bounds $\varpi(\cdot), \mathrm{e}(a_1\ell/q), Q^{-1} \leq 1$. Note that we have made use of

$$\log(x 2^{-t} k^{-2}\gcd(2^t k^2, q)\gcd(\ell,q)^{-1}) = \log x + O_A(\log\log x), \qquad (3.24)$$

which follows from

$$\frac{x}{(\log x)^{100+A}} \leq \frac{x}{2^t k^2 q} \leq x 2^{-t} k^{-2} \frac{\gcd(2^t k^2, q)}{\gcd(\ell, q)} \leq xq \leq x(\log x)^A.$$

The bound $\ddot{Q} \le Q \le 4q$ shows that the sum over t, k in (3.23) is

$$\begin{aligned}
&\ll (\log\log q)(\log q)^{1/7} \frac{x}{(\log x)^{1/2+1/7}} \sum_{(k,t)} \sum_{\ell \in \mathbb{Z} \cap [0,q)} 2^{-t} k^{-2} \gcd(2^t k^2, q) \\
&\ll (\log\log q)(\log q)^{1/7} \frac{x}{(\log x)^{1/2+1/7}} q^2 \sum_{(k,t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0}} 2^{-t} k^{-2} \\
&\ll q^3 \frac{x}{(\log x)^{1/2+1/7}},
\end{aligned}$$

which is satisfactory. To conclude the proof, it remains to show that the quantity MT gives rise to the main term as stated in our lemma. By (3.24) we see that

$$\frac{1}{\sqrt{\log(x 2^{-t} k^{-2} \gcd(2^t k^2, q) \gcd(\ell, q)^{-1})}} = \frac{1}{\sqrt{\log x}} + O\Big(\frac{\log\log x}{(\log x)^{3/2}}\Big),$$

hence $\mathrm{MT} = \mathrm{M}' + \mathrm{R}$, where M' is defined by

$$\begin{aligned}
&\frac{x 2^{1/2} \mathcal{C}_0}{(\log x)^{1/2}} \sum_{\substack{(k,t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0} \\ 2^t k^2 \le (\log x)^{100} \\ p \mid k \Rightarrow p \equiv 3 \pmod 4}} \frac{\gcd(2^t k^2, q)}{2^t k^2} \\
&\qquad \times \sum_{\substack{\ell \in \mathbb{Z} \cap [0,q) \\ \gcd(2^t k^2, q) \mid \ell \\ (3.22)}} \frac{\varpi(\gcd(\ell, q)/\gcd(2^t k^2, q)) \, \mathrm{e}(a_1 \ell / q) \ddot{Q}}{\gcd(\ell, q) \mathrm{lcm}(4, q/\gcd(\ell, q)) \varphi(\ddot{Q})}
\end{aligned}$$

and R is a quantity that satisfies

$$\mathrm{R} \ll \sum_{(k,t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0}} \sum_{\ell \in \mathbb{Z} \cap [0,q)} \frac{\ddot{Q}}{\varphi(\ddot{Q})} \frac{x 2^{-t} k^{-2} \gcd(2^t k^2, q)}{(\log\log x)^{-1} (\log x)^{3/2}} \ll q^3 \frac{x \log\log x}{(\log x)^{3/2}},$$

where we again have made use of the trivial upper bound 1 for $\varpi(\cdot)$ and $|\mathrm{e}(\cdot)|$, now combined with the lower bound 1 for $\mathrm{lcm}(\cdot)$ and $\gcd(\cdot)$. The cubic power of q arises from bounding both $\gcd(2^t k^2, q)$ and $\ddot{Q}/\varphi(\ddot{Q})$ from above by q, and then having q terms in the sum $\sum_{\ell \in \mathbb{Z} \cap [0,q)} 1$. As we have seen before, we could have bounded $\ddot{Q}/\varphi(\ddot{Q})$ from above by $\log\log q$, but this extra saving is unnecessary for our goals.

We complete the summation over t, k in M' to the whole range $\mathbb{Z}_{>0} \times \mathbb{Z}_{\ge 0}$

appearing in (3.21). To do so, we use the bound

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^tk^2>(\log x)^{100}}}\frac{\gcd(2^tk^2,q)}{2^tk^2}\sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ (3.22)\\ \gcd(2^tk^2,q)|\ell}}\frac{\ddot{Q}}{\varphi(\ddot{Q})}\ll q^3\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ 2^tk^2>(\log x)^{100}}}\frac{1}{2^tk^2}\ll\frac{q^3}{(\log x)^{50}},$$

while the observation

$$\frac{\ddot{Q}}{\varphi(\ddot{Q})}=\prod_{\substack{p\equiv 3(\mathrm{mod}\ 4)\\ p|q(\gcd(\ell,q))^{-1}}}\Big(1-\frac{1}{p}\Big)^{-1}=\prod_{\substack{p\equiv 3(\mathrm{mod}\ 4)\\ v_p(q)>v_p(\ell)}}\Big(1-\frac{1}{p}\Big)^{-1}$$

allows to remove $\ddot{Q}$ from M′. □

We note that one immediate corollary of the last lemma is the bound

$$\mathfrak{F}(a_1,q)\ll 1, \tag{3.25}$$

with an absolute implied constant. Indeed, this can be shown by taking $A=1/100$ in Lemma 3.3.6, dividing throughout by $x/\sqrt{\log x}$ in the asymptotic it provides and applying (3.16) to obtain

$$\begin{aligned}2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)&\ll\frac{(\log x)^{1/2}}{x}\Big|\sum_{1\leq m\leq x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q)\Big|+\frac{q^3}{(\log x)^{1/7}}\\&\ll 1+\frac{(\log x)^{3/100}}{(\log x)^{1/7}}.\end{aligned}$$

We remark that although this argument may feel somewhat circular at first glance, it is in fact not since the second estimate in the above equality follows not from the lemma, but from the triangle inequality combined with (3.16).

As announced at the beginning of this section, studying $E_{\mathbb{Q}}\Big(\frac{a_1}{q}+\beta_1\Big)$ is first done in the case $\beta_1=0$ as in Lemma 3.3.6 with $x=\max\{f([-1,1]^n)\}P^d$. The following lemma shows that this is sufficient, up to introducing an extra factor.

Lemma 3.3.7. *For $\Gamma_1\in\mathbb{R}$, $A\in\mathbb{R}_{>0}$, $q\in\mathbb{Z}_{>0}$ with $q\leq(\log P)^A$, and $a_1\in\mathbb{Z}\cap[0,q)$ we have*

$$E_{\mathbb{Q}}\bigg(\frac{a_1}{q}+\frac{\Gamma_1}{P^d}\bigg)=2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)\bigg(\int_2^{\max\{f_1([-1,1]^n)\}P^d}\frac{\mathrm{e}(\Gamma_1P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\bigg)$$

up to an error term that is $O_A\Big(\frac{q^3(1+|\Gamma_1|)P^d}{(\log P)^{1/2+1/7}}\Big)$.

Proof. To ease the notation we temporarily put $c := 2^{1/2}\mathcal{C}_0\mathfrak{F}(a_1,q)$. Fix $\beta\in\mathbb{R}$. By applying partial summation[1] with $a_m = \vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q))$ and $\varphi(t)=\mathrm{e}(\beta t)$, we see that $\sum_{m\le x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(m(\beta+a_1/q))$ equals

$$\Big(\sum_{m\le x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q)\Big)\,\mathrm{e}(x\beta)-\int_0^x \mathrm{e}(\beta t)'\Big(\sum_{m\le t}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(a_1m/q)\Big)\mathrm{d}t.$$

For $q\le(\log x)^A$, Lemma 3.3.6 shows that this equals

$$c\Big(\Big(\frac{x}{\sqrt{\log x}}\,\mathrm{e}(x\beta)-\int_2^x\frac{t}{\sqrt{\log t}}\,\mathrm{e}(\beta t)'\mathrm{d}t\Big)+O_A\Big(\frac{q^3x(1+|\beta|x)}{(\log x)^{1/2+1/7}}\Big),$$

with an implied constant depending at most on A. Using partial integration this is plainly

$$c\Big(\int_2^x\Big(\frac{t}{\sqrt{\log t}}\Big)'\,\mathrm{e}(\beta t)\mathrm{d}t\Big)+O_A\Big(\frac{q^3(1+|\beta|x)x}{(\log x)^{1/2+1/7}}\Big),$$

and using $(t(\log t)^{-1/2})' = (\log t)^{-1/2}-2^{-1}(\log t)^{-3/2}$ shows that the last integral can be evaluated as $\int_2^x\mathrm{e}(\beta t)(\log t)^{-1/2}\mathrm{d}t+O(x(\log x)^{-3/2})$. Invoking the bound $c\ll 1$ (that is implied by (3.25)) we obtain

$$\sum_{m\le x}\vartheta_{\mathbb{Q}}(m)\,\mathrm{e}(m(\beta+a_1/q))=c\Big(\int_2^x\frac{\mathrm{e}(\beta t)}{\sqrt{\log t}}\mathrm{d}t\Big)+O\Big(\frac{q^3(1+|\beta|x)x}{(\log x)^{1/2+1/7}}\Big).$$

Using this for $x=\frac12\min\{f_1([-1,1]^n)\}P^d$ and putting $\beta=\Gamma_1P^{-d}$ concludes the proof. □

3.4 Proof of the asymptotic

We are ready to prove the asymptotic in Theorem 3.1.3. We shall do so with different leading constants than those given in Theorem 3.1.3; showing equality of the constants is delayed until §3.5.

[1] See Theorem 1.3.1.

3.4.1 Restricting the range in the major arcs

The first reasonable step for the proof of the asymptotics would be to inject Lemma 3.3.7 into Lemma 3.2.3. However, this would give poor results because the error term in Lemma 3.3.7 is only powerful when Γ_1 is close to zero and q is small in comparison to P. For this reason we restrict the sum over q and the integration over $\boldsymbol{\beta}$ in Lemma 3.2.3. For its proof we shall need certain bounds. First, by (3.16) and the triangle inequality, one has

$$E_{\mathbb{Q}}(\alpha_1) \ll P^d(\log P)^{-1/2} \tag{3.26}$$

where the implied constant is independent of α_1. Recall the definition of $I(\mathbf{\Gamma})$ from (3.14). Letting $K := (n-\sigma(f_1,f_2))2^{-d+1}$, we use Lemmas 1.3.33 and 1.3.34 to obtain the following bounds valid for every $\varepsilon > 0$, $\mathbf{\Gamma} \in \mathbb{R}^2$ and $\mathbf{a} \in \mathbb{Z}^2, q \in \mathbb{Z}_{>0}$ satisfying $\gcd(a_1,a_2,q)=1$:

$$I(\mathbf{\Gamma}) \ll_\varepsilon \min\{1, |\mathbf{\Gamma}|^{-K/(2(d-1))+\varepsilon}\} \text{ and } S_{\mathbf{a},q} \ll_\varepsilon q^{n-K/(2(d-1))+\varepsilon}.$$

By our assumption (3.1), we have

$$I(\mathbf{\Gamma}) \ll \min\{1, |\mathbf{\Gamma}|^{-5/2}\}, \tag{3.27}$$

and furthermore, for all $0 < \lambda < 2^{-d}(d-1)^{-1}$ we have

$$S_{\mathbf{a},q} \ll_\lambda q^{n-3-\lambda}. \tag{3.28}$$

Lemma 3.4.1. *Keep the assumptions of Lemma 3.2.2 and let $Q_1, Q_2 \in \mathbb{R}_{\geq 1}$ with $Q_1, Q_2 \leq P^\eta$ for some fixed positive η. Then for any λ satisfying*

$$0 < \lambda < \min\Big\{1, \frac{1}{2}\Big(\frac{n-\sigma(f_1,f_2)}{2^d(d-1)} - 3\Big)\Big\} \tag{3.29}$$

we have

$$\begin{aligned}
&\sum_{q \leq P^\eta} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\boldsymbol{\beta}| \leq P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta}) \overline{E_{\mathbb{Q}}(\beta_1 + a_1/q)} \mathrm{d}\boldsymbol{\beta} \\
&= \sum_{q \leq Q_1} q^{-n} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2 \\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} \int_{|\mathbf{\Gamma}| \leq Q_2} \frac{I(\mathbf{\Gamma})}{P^d} \overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d} + a_1/q)} \mathrm{d}\mathbf{\Gamma} \\
&+ O_{\delta,\lambda,\theta_0}\big((\log P)^{-1/2} \min\big\{Q_1^{-\lambda}, Q_2^{-1/2}\big\}\big).
\end{aligned}$$

Proof. Using the change of variables $P^d\boldsymbol{\beta} = \boldsymbol{\Gamma}$ we obtain equality between

$$\int_{P^{-d}Q_2<|\boldsymbol{\beta}|\leq P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1+a_1/q)}\mathrm{d}\boldsymbol{\beta}$$

and

$$P^{-d}\int_{Q_2<|\boldsymbol{\Gamma}|\leq P^{\eta}} I(\boldsymbol{\Gamma})\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}\mathrm{d}\boldsymbol{\Gamma}.$$

We bound $\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}$ by $P^d(\log P)^{-1/2}$ from (3.26), where the implied constant did not depend on the argument of $E_{\mathbb{Q}}$. We bound $I(\boldsymbol{\Gamma})$ using (3.27), and we extend the range of integration to $Q_2 < |\boldsymbol{\Gamma}|$.

The bound $\int_{Q_2<|\boldsymbol{\Gamma}|} I(\boldsymbol{\Gamma})\mathrm{d}\boldsymbol{\Gamma} \ll Q_2^{-1/2}$ may be computed in a straightforward manner using (3.27) and dividing up the range of integration to make use of the symmetry of the problem. These estimates together show the validity of

$$\int_{P^{-d}Q_2<|\boldsymbol{\beta}|\leq P^{-d+\eta}} P^d I(P^d\boldsymbol{\beta})\overline{E_{\mathbb{Q}}(\beta_1+a_1/q)}\mathrm{d}\boldsymbol{\beta} \ll \frac{1}{\sqrt{Q_2\log P}}. \tag{3.30}$$

This shows that the sum over $q \leq P^{\eta}$ in the statement of our lemma equals

$$\sum_{q\leq P^{\eta}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}\int_{|\boldsymbol{\Gamma}|\leq Q_2} \frac{I(\boldsymbol{\Gamma})}{P^d}\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}\mathrm{d}\boldsymbol{\Gamma}$$

up to a term that is

$$\ll \frac{1}{\sqrt{Q_2\log P}}\sum_{q\leq P^{\eta}}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{|S_{\mathbf{a},q}|}{q^n} \ll \frac{\sum_{q\leq P^{\eta}} q^{-1-\lambda}}{\sqrt{Q_2\log P}} \ll \frac{1}{\sqrt{Q_2\log P}},$$

where (3.28) has been utilised. Note that the bound $\int_{\mathbb{R}^2}|I(\boldsymbol{\Gamma})|\mathrm{d}\boldsymbol{\Gamma} < \infty$ is a consequence of (3.27). Using this with (3.26) shows

$$\sum_{q>Q_1}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{S_{\mathbf{a},q}}{q^n}\int_{|\boldsymbol{\Gamma}|\leq Q_2} I(\boldsymbol{\Gamma})\overline{E_{\mathbb{Q}}(\Gamma_1 P^{-d}+a_1/q)}\mathrm{d}\boldsymbol{\Gamma} \ll \frac{\sum_{q>Q_1} q^{-1-\lambda}}{\sqrt{\log P}}$$
$$\ll \frac{Q_1^{-\lambda}}{\sqrt{\log P}},$$

where we have used (3.28). This concludes the proof of the lemma. □

LEMMA 3.4.2. *Keep the assumptions of Lemma 3.2.2, fix any two positive A_1, A_2, and let*

$$\lambda_0 := \frac{1}{2}\min\left\{1, \frac{1}{2}\left(\frac{n-\sigma(f_1,f_2)}{2^d(d-1)} - 3\right)\right\}. \tag{3.31}$$

Then for all sufficiently large P the quantity $\Theta_{\mathbb{Q}}(P)P^{-n+d}$ equals

$$\sum_{q\le(\log P)^{A_1}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{S_{\mathbf{a},q}}{q^n} \int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} \frac{I(\mathbf{\Gamma})}{P^d}\overline{E_{\mathbb{Q}}\left(\frac{a_1}{q}+\frac{\Gamma_1}{P^d}\right)}\mathrm{d}\mathbf{\Gamma}$$

up to an error term that is $O_{A_1,A_2}\big((\log P)^{-1/2-\min\{A_1\lambda_0,A_2/2\}}\big)$.

Proof. The proof follows immediately from application of Lemma 3.4.1 with $Q_i = (\log P)^{A_i}$ and Lemma 3.2.3 with some fixed δ and θ_0 satisfying (1.7) and (1.8) and subject to $\eta = 2(d-1)\theta_0 < 1/7$ in order to get a negative power of P in the error term coming from Lemma 3.4.1. □

3.4.2 Injecting the sieve estimates into the restricted major arcs

We are now in a position to inject Lemma 3.3.7 into Lemma 3.4.2. It may be uncommon to use sieve estimates to study major arcs, but the reason that we do this is not very deep: the availability of the sieve estimates allowed us to not worry about the behaviour of $\vartheta_{\mathbb{Q}}(m)$ in residue classes. It is not at all unlikely that good results on $\vartheta_{\mathbb{Q}}(m)$ in residue classes allow for a much more direct approach.

It will be convenient to start by studying the archimedean density, but before we do all that, we state a basic lemma that will be used twice in this chapter.

LEMMA 3.4.3. *For $x \ge 2$ we have*

$$\int_2^x (\log t)^{-1/2}\mathrm{d}t \ll \frac{x}{\sqrt{\log x}}.$$

Proof. Note that $\frac{t}{\sqrt{\log t}}$ is the anti-derivative of $\frac{2\log t-1}{2(\log t)^{3/2}}$ and that we have

$$(\log t)^{-1/2} \ll \frac{2\log t - 1}{2(\log t)^{3/2}}.$$

Hence we get

$$\int_2^x (\log t)^{-1/2}\mathrm{d}t \ll \frac{x}{\sqrt{\log x}}.$$

□

Now recall (3.14) and define for all P with $2 \le \max\{f_1([-1,1]^n)\}P^d$ the integral

$$\mathfrak{J}_\phi(P) := \int_{\mathbf{\Gamma}\in\mathbb{R}^2} \frac{I(\mathbf{\Gamma})}{P^d}\bigg(\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{e}(-\Gamma_1 P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\bigg)\mathrm{d}\mathbf{\Gamma}. \quad (3.32)$$

The assumptions of Theorem 3.1.3 ensure that the integral converges absolutely, since by (3.27) and application of Lemma 3.4.3 we have

$$\begin{aligned}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} \frac{|I(\mathbf{\Gamma})|}{P^d}\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{d}t\mathrm{d}\mathbf{\Gamma}}{\sqrt{\log t}} &\ll \int_{\mathbf{\Gamma}\in\mathbb{R}^2} \frac{\min\{1,|\mathbf{\Gamma}|^{-5/2}\}}{P^d}\frac{P^d\mathrm{d}\mathbf{\Gamma}}{\sqrt{\log P}}\\ &\ll \frac{1}{\sqrt{\log P}}.\end{aligned}$$

Lemma 3.4.4. *Under the assumptions of Theorem 3.1.3 we have*

$$\mathfrak{J}_\phi(P) = \frac{1}{\sqrt{\log(P^d)}}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma})\bigg(\int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu)\mathrm{d}\mu\bigg)\mathrm{d}\mathbf{\Gamma}$$

up to an error term that is $O((\log P)^{-3/2})$.

Proof. Observe that the change of variables $\mu = P^{-d}t$ in (3.32) shows

$$\mathfrak{J}_\phi(P) = \int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma})\bigg(\int_{2P^{-d}}^{\max\{f_1([-1,1]^n)\}} \frac{\mathrm{e}(-\Gamma_1\mu)}{\sqrt{\log(\mu P^d)}}\mathrm{d}\mu\bigg)\mathrm{d}\mathbf{\Gamma}.$$

For $|x| < 1$ we have $(1+x)^{-1/2} = 1 + O(x)$, hence for fixed μ we have

$$\begin{aligned}\big(\log(\mu P^d)\big)^{-1/2} &= \big(\log(P^d)\big)^{-1/2}\bigg(1+\frac{\log\mu}{\log(P^d)}\bigg)^{-1/2}\\ &= \big(\log(P^d)\big)^{-1/2} + O\bigg(\frac{\log\mu}{(\log P)^{3/2}}\bigg).\end{aligned}$$

Using this for $0 < \mu \le \max\{f_1([-1,1]^n)\}$, we infer the following estimate for all sufficiently large P, where the integral $\int_{2P^{-d}}^{\max\{f_1([-1,1]^n)\}}\log\mu\mathrm{d}\mu$ is bounded by a constant. The difference

$$\mathfrak{J}_\phi(P) - \frac{1}{\sqrt{\log(P^d)}}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma})\int_{2P^{-d}}^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu)\mathrm{d}\mu\mathrm{d}\mathbf{\Gamma}$$

can be estimated as

$$\ll \frac{1}{(\log P)^{3/2}} \int_{\mathbf{\Gamma}\in\mathbb{R}^2} |I(\mathbf{\Gamma})| \mathrm{d}\mathbf{\Gamma} \ll (\log P)^{-3/2}$$

due to (3.27). □

Define

$$\mathfrak{J} := \int_{\Gamma\in\mathbb{R}} \int_{\{\mathbf{t}\in[-1,1]^n : x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has an } \mathbb{R}\text{-point}\}} \mathrm{e}(\Gamma f_2(\mathbf{t})) \mathrm{d}\mathbf{t}\mathrm{d}\Gamma \tag{3.33}$$

and note that the integral converges absolutely owing to (3.1) and Lemma 1.3.33 with $R = 1$. The arguments in [Bir62, §6] show that if the set $\{\mathbf{t} \in [-1,1]^n : f_1(\mathbf{t}) \geq 0\}$ contains a non-singular real point of $f_2 = 0$ then $\mathfrak{J} > 0$. This condition holds in the situation of Theorem 3.1.3 because its assumptions include $B(\mathbb{Q}) \neq \emptyset$ and that f_2 is non-singular. This will again come up in the proof of Theorem 3.5.23, where we give more details.

Lemma 3.4.5. *Under the assumptions of Theorem 3.1.3 we have*

$$\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \bigg(\int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \bigg) \mathrm{d}\mathbf{\Gamma} = \mathfrak{J}.$$

Proof. This proof will follow the same arguments as [DS18, Lem. 4.3 and 4.4]. First we will show that the left-hand side of the equation in the lemma is equal to $\lim_{m\to\infty} \mathfrak{J}_m$ with

$$\mathfrak{J}_m = \int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \exp\left(-\pi^2\Gamma_1^2 m^{-2}\right) \int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \mathrm{d}\mathbf{\Gamma}.$$

We consider

$$\begin{aligned}
&\left| \int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \bigg(\int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \bigg) \mathrm{d}\mathbf{\Gamma} - \mathfrak{J}_m \right| \\
&= \left| \int_{\Gamma_1\in\mathbb{R}} \big(1 - \exp(-\pi^2\Gamma_1^2 m^{-2}\big) \int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu) \mathrm{d}\mu \int_{\Gamma_2\in\mathbb{R}} I(\mathbf{\Gamma}) \mathrm{d}\Gamma_2 \mathrm{d}\Gamma_1 \right| \\
&\ll \left| \int_{\Gamma_1\in\mathbb{R}} \big(1 - \exp(-\pi^2\Gamma_1^2 m^{-2}\big) \int_{\Gamma_2\in\mathbb{R}} I(\mathbf{\Gamma}) \mathrm{d}\Gamma_2 \mathrm{d}\Gamma_1 \right|.
\end{aligned}$$

We split the integration range of Γ_1 into two parts: $|\Gamma_1| \leq \log m$ and $|\Gamma_1| > \log m$. Making use of (3.27) we estimate the first part of the integral as

$$O\left((1-\exp(-\pi^2 m^{-2}(\log m)^2))\log m\right),$$

which goes to 0 for $m \to \infty$.

For the second part, we bound $1-\exp(-\pi^2\Gamma_1^2 m^{-2})$ by 1, and again make use of (3.27) to conclude that the integral is $O\left((\log m)^{-1/2}\right)$, which goes to 0 for $m \to \infty$. Therefore, we have proven that the integral in the statement of the lemma is equal to the limit $\lim_{m\to\infty}\mathfrak{J}_m$. We continue with the proof that this limit also equals $\mathfrak{J}$.

Define for $m \in \mathbb{Z}_{>0}$ the function $\phi_m : \mathbb{R} \to \mathbb{R}$ by

$$\phi_m(x) := \pi^{-1/2} m \exp\left(-m^2x^2\right).$$

The Fourier transform of $\phi_m(x)$ is $\exp(-\pi^2\xi^2 m^{-2})$, hence by Fourier's inversion formula, we have

$$\phi_m(x) = \int_{\mathbb{R}} \exp\left(-\pi^2\Gamma_1^2 m^{-2}\right) \mathrm{e}(x\Gamma_1)\mathrm{d}\Gamma_1.$$

Using this with $x = f_1(\mathbf{t}) - \mu$, and inserting the definition of $I(\mathbf{\Gamma})$, allows us to rewrite $\mathfrak{J}_m$ as

$$\int_{\substack{\mathbf{t}\in[-1,1]^n : f_1(\mathbf{t})\neq 0 \\ f_1(\mathbf{t})\neq \max\{f_1([-1,1]^n)\}}} \left(\int_0^{\max\{f_1([-1,1]^n)\}} \phi_m(f_1(\mathbf{t})-\mu)\mathrm{d}\mu\right)\left(\int_{\Gamma_2\in\mathbb{R}} \mathrm{e}(\Gamma_2 f_2(\mathbf{t}))\mathrm{d}\Gamma_2\right)\mathrm{d}\mathbf{t}.$$

Note that we replaced $\mathbf{t} \in [-1,1]^n$ by the range of integration in the expression above; this is allowed as it only removes a set of measure zero from the integration in (3.14).

The following identity for real numbers $a < b$ and $a \neq c \neq b$ is well known and easily proven:

$$\lim_{m\to\infty}\int_a^b \phi_m(c-\mu)\mathrm{d}\mu = \begin{cases} 1 & \text{if } a < c < b, \\ 0 & \text{otherwise.} \end{cases}$$

Hence if $\mathbf{t} \in [-1,1]^n$ satisfies $f_1(\mathbf{t}) > 0$ and $f_1(\mathbf{t}) \neq \max\{f_1([-1,1]^n)\}$, then we have

$$\lim_{m\to\infty}\int_0^{\max\{f_1([-1,1]^n)\}} \phi_m(f_1(\mathbf{t})-\mu)\mathrm{d}\mu = 1,$$

while for $f_1(\mathbf{t}) < 0$ the limit vanishes. The dominated convergence theorem allows us to switch the order of the limit over m and the integral over $\mathbf{t}$, providing

$$\begin{aligned}\int_{\mathbf{\Gamma}\in\mathbb{R}^2} I(\mathbf{\Gamma}) \int_0^{\max\{f_1([-1,1]^n)\}} \mathrm{e}(-\Gamma_1\mu)\mathrm{d}\mu\mathrm{d}\mathbf{\Gamma}&\\ = \int_{\substack{\mathbf{t}\in[-1,1]^n: f_1(\mathbf{t})>0\\ f_1(\mathbf{t})\neq\max\{f_1([-1,1]^n)\}}} \left(\int_{\Gamma_2\in\mathbb{R}} \mathrm{e}(\Gamma_2 f_2(\mathbf{t}))\mathrm{d}\Gamma_2\right)\mathrm{d}\mathbf{t}&\\ = \int_{\substack{\mathbf{t}\in[-1,1]^n\\ f_1(\mathbf{t})>0}} \left(\int_{\Gamma_2\in\mathbb{R}} \mathrm{e}(\Gamma_2 f_2(\mathbf{t}))\mathrm{d}\Gamma_2\right)\mathrm{d}\mathbf{t} = \mathfrak{J},&\end{aligned}$$

which concludes the proof. □

The integral part of Lemma 3.2.3 is calculated in successive steps by Lemmas 3.3.7, 3.4.4 and 3.4.5. Hence we may now turn our attention to the summation part. Recall the definition of $S_{\mathbf{a},q}$ and $\mathfrak{F}(a_1,q)$ respectively in (3.13) and (3.21) and let

$$\mathbb{L}_\phi := \sum_{q\in\mathbb{Z}_{>0}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}\overline{\mathfrak{F}(a_1,q)}. \tag{3.34}$$

Under the assumptions of Theorem 3.1.3, the sum $\mathbb{L}_\phi$ converges absolutely since by (3.25) and (3.28) we have for all $x > 1$:

$$\begin{aligned}\sum_{\substack{q\in\mathbb{Z}_{>0}\\ q>x}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \left|S_{\mathbf{a},q}\overline{\mathfrak{F}(a_1,q)}\right| &\ll \sum_{\substack{q\in\mathbb{Z}_{>0}\\ q>x}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} q^{n-3-\lambda_0}\\ &\leq \sum_{\substack{q\in\mathbb{Z}_{>0}\\ q>x}} q^{-1-\lambda_0} \ll x^{-\lambda_0}.\end{aligned} \tag{3.35}$$

Lemma 3.4.6. *Under the assumptions of Theorem 3.1.3, any $P \geq 2$ validates*

$$\Theta_{\mathbb{Q}}(P) = \mathcal{C}_0\mathfrak{J}\frac{\mathbb{L}_\phi\sqrt{2}}{d^{1/2}}\frac{P^{n-d}}{(\log P)^{1/2}} + O\left((\log P)^{-\frac{1}{40}\frac{1}{(d-1)2^{d+2}}}\frac{P^{n-d}}{(\log P)^{1/2}}\right).$$

Proof. Combining Lemmas 3.3.7 and 3.4.2 shows

$$\frac{\Theta_{\mathbb{Q}}(P)}{P^{n-d}} = 2^{1/2}\mathcal{C}_0\mathcal{R}_1\mathcal{R}_2 + \mathcal{R}_3 + O\big((\log P)^{-1/2-\min\{A_1\lambda_0, A_2/2\}}\big), \tag{3.36}$$

with

$$\mathcal{R}_1 := \sum_{q\le(\log P)^{A_1}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}\overline{\mathfrak{F}(a_1,q)},$$

$$\mathcal{R}_2 := \int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} \frac{I(\mathbf{\Gamma})}{P^d}\Big(\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{e}(-\Gamma_1 P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\Big)\mathrm{d}\mathbf{\Gamma},$$

and where $\mathcal{R}_3$ is a quantity that satisfies

$$\mathcal{R}_3 \ll \sum_{q\le(\log P)^{A_1}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{|S_{\mathbf{a},q}|}{q^n}\int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} \frac{|I(\mathbf{\Gamma})|}{P^d}\frac{q^3(1+|\Gamma_1|)P^d}{(\log P)^{1/2+1/7}}\mathrm{d}\mathbf{\Gamma}.$$

Bounding q and Γ_1 in the integrand by $(\log P)^{A_1}$ and $(\log P)^{A_2}$ respectively, we find

$$\mathcal{R}_3 \ll_{A_2} \frac{(\log P)^{3A_1+A_2}}{(\log P)^{1/2+1/7}} \sum_{q\le(\log P)^{A_1}} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} \frac{|S_{\mathbf{a},q}|}{q^n}\int_{|\mathbf{\Gamma}|\le(\log P)^{A_2}} |I(\mathbf{\Gamma})|\mathrm{d}\mathbf{\Gamma}.$$

By (3.27) and (3.28) the sum over q is convergent, and so is the integral over $\mathbf{\Gamma}$. Therefore we bound

$$\mathcal{R}_3 \ll_{A_2} (\log P)^{3A_1+A_2-1/2-1/7}. \tag{3.37}$$

Notice that $\mathcal{R}_2$ and $\mathcal{R}_1$ are truncated versions of $\mathfrak{J}_\phi(P)$ and $\mathbb{L}_\phi$ respectively. Next we will estimate the parts that are cut off. Using (3.27) we infer

$$\begin{aligned}
&\int_{|\mathbf{\Gamma}|>(\log P)^{A_2}} \frac{|I(\mathbf{\Gamma})|}{P^d}\Big(\int_2^{\max\{f_1([-1,1]^n)\}P^d} \frac{\mathrm{e}(-\Gamma_1 P^{-d}t)}{\sqrt{\log t}}\mathrm{d}t\Big)\mathrm{d}\mathbf{\Gamma}\\
\ll\ &\int_{|\mathbf{\Gamma}|>(\log P)^{A_2}} |I(\mathbf{\Gamma})|\frac{1}{\sqrt{\log P}}\mathrm{d}\mathbf{\Gamma}\\
\ll_{A_2}\ &(\log P)^{-1/2-A_2/2},
\end{aligned}$$

where in going from the first to the second line in the above, we have again bounded $|\,\mathrm{e}(\cdot)|$ by 1, and we bounded $P^{-d}\int_2^{\max\{f_1([-1,1]^n)\}P^d}(\log t)^{-1/2}\mathrm{d}t$ by application of Lemma 3.4.3.

Therefore we have

$$\mathcal{R}_2 = \mathfrak{J}_\phi(P) + O_{A_2}((\log P)^{-1/2-A_2/2}). \tag{3.38}$$

Furthermore, by (3.35) we deduce

$$\mathcal{R}_1 = \mathbb{L}_\phi + O_{A_1}((\log P)^{-A_1\lambda_0}). \tag{3.39}$$

We have already seen just before Lemma 3.4.4 that we have

$$\mathfrak{J}_\phi(P) \ll (\log P)^{-1/2},$$

thus injecting (3.37), (3.38) and (3.39) into (3.36) provides us with

$$\frac{\Theta_{\mathbb{Q}}(P)}{P^{n-d}} = 2^{1/2}\mathcal{C}_0\mathfrak{J}_\phi(P)\mathbb{L}_\phi + O((\log P)^{-1/2-\beta}),$$

with $\beta := \min\{A_1\lambda_0, A_2/2, -3A_1 - A_2 + 1/7\}$. A moment's thought affirms that assumption (3.1) ensures the validity of $\lambda_0 \geq (d-1)^{-1}2^{-d-2}$ and choosing $A_1 = \frac{1}{40} = A_2/2$ gives $\beta \geq (40(d-1)2^{d+2})^{-1}$. Finally, using Lemmas 3.4.4 and 3.4.5 concludes the proof. □

3.4.3 Proof of Theorem 3.1.3

Define

$$c_\phi := \frac{\mathfrak{J}}{d^{1/2}}\frac{2^{1/2}}{\zeta(n-d)}\frac{\mathbb{L}_\phi}{2}\mathcal{C}_0. \tag{3.40}$$

By Lemmas 3.2.1 and 3.4.6 the quantity $N(\phi, t)$ equals

$$\frac{\sqrt{2}}{2}\mathcal{C}_0\mathfrak{J}\mathbb{L}_\phi\frac{t^{n-d}}{d^{1/2}}\sum_{l\leq\log t}\frac{\mu(l)}{l^{n-d}(\log(t/l))^{1/2}}$$

up to an error term that is

$$\ll \frac{t^{n-d}}{\log t} + \sum_{l\leq\log t}\frac{(t/l)^{n-d}}{(\log(t/l))^{\frac{1}{2}+\frac{1}{40}\frac{1}{(d-1)2^{d+2}}}} \ll \frac{t^{n-d}}{(\log t)^{\frac{1}{2}+\frac{1}{40}\frac{1}{(d-1)2^{d+2}}}},$$

where the last estimate in the previous line is established as follows. First notice that the term $\frac{t^{n-d}}{\log t}$ falls under the estimate. For the sum we need to do a little bit more work. We begin with

$$\begin{aligned}\log(t/l) &= \log t - \log l\\ &\geq \log t\left(1 - \frac{\log\log t}{\log t}\right)\\ &\gg \log t,\end{aligned}$$

which allows us to take the denominator out of the sum. We moreover take t^{n-d} out of the sum, and then we notice that for $n-d \geq 2$ (which is valid because of (3.1)) the series $\sum_{l=1}^{\infty} l^{d-n}$ converges, so we may as well complete the sum and bound it by a constant.

Note that for $l \leq \log t$ we have $(\log(t/l))^{-1/2} = (\log t)^{-1/2} + O((\log t)^{-1})$, hence

$$\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}(\log(t/l))^{1/2}} = (\log t)^{-1/2} \left(\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}} \right) + O((\log t)^{-1}),$$

where the sum disappeared into the error term by completing to the range $l \in \mathbb{Z}_{>0}$, which gives a series converging to $\zeta(n-d)^{-1}$.

For the sum in the main term we use the completed sum again, but we include the error term arising from the cut-off, i.e.

$$\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}} = \sum_{l=1}^{\infty} \frac{\mu(l)}{l^{n-d}} - \sum_{l > \log t} \frac{\mu(l)}{l^{n-d}} = \zeta(n-d)^{-1} + O\left(\frac{1}{(\log t)^{n-d-1}} \right)$$

where from the tail of the sum we arrive at the error term by bounding $|\mu(l)| \leq 1$ and comparing the sum to an integral, similarly to Lemma 3.4.3. Putting these arguments together we obtain

$$\sum_{l \leq \log t} \frac{\mu(l)}{l^{n-d}(\log(t/l))^{1/2}} = \zeta(n-d)^{-1}(\log t)^{-1/2} + O((\log t)^{-1})$$

and therefore

$$\frac{N(\phi, t)}{t^{n-d}(\log t)^{-1/2}} - \frac{\mathfrak{J}\mathbb{L}_{\phi}\mathcal{C}_0}{\zeta(n-d)\sqrt{2d}} \ll \frac{1}{(\log t)^{\varepsilon_d}}, \tag{3.41}$$

which concludes our proof. □

3.5 Interpretation of the leading constant

The circle method and the half-dimensional sieve allowed us to obtain a proof of the asymptotic in a technical, yet straightforward manner. However, this came at a cost because the leading constant c_{ϕ} in (3.40) is complicated. In this section we shall give an interpretation of c_{ϕ} via certain p-adic densities; this will not be straightforward.

In §3.5.1 we shall write $\mathbb{L}_\phi$ as an Euler product over all primes, with each factor involving complete exponential sums. Next, in §3.5.2 we shall show that for primes $p \equiv 3 \pmod 4$ these factors are connected to a particular kind of p-adic density. An analogous result will be proved in §3.5.3 for the prime 2. Finally, putting all partial results of §3.5 together, we shall provide in §3.5.4 an interpretation of the leading constant in Theorem 3.1.3, see Theorem 3.5.23.

3.5.1 Factorising $\mathbb{L}_\phi$

LEMMA 3.5.1. *For every integer $q \geq 3$ we have*

$$\sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3 (\mathrm{mod}\ 4)}} \frac{\gcd(2^t k^2, q)}{2^t k^2} \ll q^{\frac{1}{\log\log q}}.$$

Proof. By multiplicativity the sum in the lemma equals

$$\left(\sum_{t=0}^{\infty} \frac{\gcd(2^t, q)}{2^t}\right) \prod_{p\equiv 3 (\mathrm{mod}\ 4)} \left(\sum_{i=0}^{\infty} \frac{\gcd(p^{2i}, q)}{p^{2i}}\right).$$

The sum over t is easily seen to be $2 + v_2(q)$, while the sum over i equals

$$\begin{cases} \frac{1+v_p(q)}{2} + \frac{p}{p^2-1}, & \text{if } 2 \nmid v_p(q), \\ 1 + \frac{v_p(q)}{2} + \frac{1}{p^2-1}, & \text{if } 2 \mid v_p(q). \end{cases}$$

This is at most $(1+v_p(q))(1+\frac{1}{p^2-1})$, hence we obtain the following bound for the sum in the lemma:

$$(2+v_2(q)) \prod_{p\neq 2} \Big[\big(1+(p^2-1)^{-1}\big)(1+v_p(q))\Big] \ll (2+v_2(q)) \frac{\tau(q)}{(1+v_2(q))} \leq 2\tau(q),$$

where τ is the divisor function. Using (3.4) allows to conclude the proof. □

For $q \in \mathbb{Z}_{>0}$, $a_1 \in \mathbb{Z} \cap [0, q)$ and $(k, t) \in \mathbb{Z}_{>0} \times \mathbb{Z}_{\geq 0}$, we define

$$T_{a_1,q}(t,k) := \sum_{\substack{\ell\in\mathbb{Z}\cap[0,q)\\ \gcd(2^t k^2,q)|\ell\\ (3.22)}} \frac{\varpi(\gcd(\ell,q)/\gcd(2^t k^2,q))\, \mathrm{e}(-a_1\ell/q)}{\gcd(\ell,q)\mathrm{lcm}(4, q/\gcd(\ell,q))} \prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ v_p(q)>v_p(\ell)}} \Big(1-\frac{1}{p}\Big)^{-1} \tag{3.42}$$

and we furthermore let

$$\mathbb{L}_{\phi}(k,t) := \sum_{q\in\mathbb{Z}_{>0}} \frac{\gcd(2^t k^2, q)}{q^n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q} T_{a_1,q}(t,k). \tag{3.43}$$

LEMMA 3.5.2. *Under the assumptions of Theorem 3.1.3 we have*

$$\mathbb{L}_{\phi} = \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \frac{\mathbb{L}_{\phi}(k,t)}{k^2 2^t}.$$

Proof. The lemma follows immediately by combining (3.21) with (3.34) and inverting the order of summation, provided that one proves

$$\sum_{q\in\mathbb{Z}_{>0}} q^{-n} \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} |S_{\mathbf{a},q}| \sum_{\substack{(k,t)\in\mathbb{Z}_{>0}\times\mathbb{Z}_{\geq 0}\\ p|k\Rightarrow p\equiv 3(\mathrm{mod}\ 4)}} \frac{\gcd(2^t k^2, q)}{2^t k^2} |T_{a_1,q}(t,k)| < \infty.$$

To bound $T_{a_1,q}(t,k)$, observe that every prime p in the product in (3.42) must necessarily divide q, hence the product is at most

$$\prod_{p|q} \Big(1-\frac{1}{p}\Big)^{-1} = \frac{q}{\varphi(q)} \ll \log\log q,$$

where we used (3.5). Recalling $\varpi(m) \in \{0,1\}$ for all m and using the obvious bound $\mathrm{lcm}(4,b) \geq b$, valid for all $b \in \mathbb{Z}_{>0}$, we obtain the following bound with an absolute implied constant,

$$T_{a_1,q}(t,k) \ll \sum_{\ell\in\mathbb{Z}\cap[0,q)} \frac{1}{q} \log\log q = \log\log q.$$

Using this with Lemma 3.5.1 and (3.28) concludes the proof. □

In Lemmas 3.5.3–3.5.6, we show that for fixed a_1, t and k, the expression $T_{a_1,q}(t,k)$ can be analysed according to the prime factorisation of q. Before stating the lemmas we introduce the following notation. Recall the notation (3.19) and for $t, a \in \mathbb{Z}_{\geq 0}$, $q \in \mathbb{Z}_{>0}$ define

$$\mathcal{K}_{a,q}(t) := \sum_{\substack{\ell\in\mathbb{Z}\cap[0,2^{v_2(q)}),(3.44)\\ \gcd(\ell,2^{v_2(q)})=2^{\min\{t,v_2(q)\}}}} \mathrm{e}(-a\ell/2^{v_2(q)}),$$

with the summation condition

$$\frac{2^t}{2^{\min\{t,v_2(q)\}}} \equiv \frac{\ell\ddot{q}}{2^{\min\{t,v_2(q)\}}} \left(\mathrm{mod}\ 2^{\min\{2,v_2(q)-\min\{t,v_2(q)\}\}}\right). \tag{3.44}$$

For $a \in \mathbb{Z}_{\geq 0}$ and $q, k \in \mathbb{Z}_{>0}$ we furthermore let

$$\mathcal{W}_{a,q}(k) := \sum_{\substack{\ell \in \mathbb{Z} \cap [0,q) \\ \gcd(\ell,q)=\gcd(k^2,q)}} \mathrm{e}(-a\ell/q) \prod_{\substack{p \text{ prime} \\ v_p(q)>v_p(\ell)}} \left(1-\frac{1}{p}\right)^{-1}. \tag{3.45}$$

It is clear that if c is an integer coprime to q then we have

$$\mathcal{W}_{ca,q}(k) = \mathcal{W}_{a,q}(k). \tag{3.46}$$

LEMMA 3.5.3. *For all $k \in \mathbb{Z}_{>0}$ satisfying $k = \ddot{k}$, all $a, t \in \mathbb{Z}_{\geq 0}$ and $q \in \mathbb{Z}_{>0}$ we have*

$$T_{a,q}(t,k) = \frac{\mathcal{K}_{a,q}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}(4, 2^{v_2(q)-\min\{t,v_2(q)\}})} \frac{\mathcal{W}_{a,\ddot{q}}(k)}{\ddot{q}} \times \begin{cases} 1, & \text{if } \dot{q} \mid a, \\ 0, & \text{if } \dot{q} \nmid a. \end{cases}$$

Proof. We observe that $T_{a_1,q}(t,k)$ equals

$$\sum_{\substack{\ell \in \mathbb{Z} \cap [0, 2^{v_2(q)}\dot{q}\ddot{q}) \\ \gcd(2^t k^2, 2^{v_2(q)}\ddot{q}) \mid \ell}} \frac{\varpi(\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q})/\gcd(2^t k^2, 2^{v_2(q)}\ddot{q}))\, \mathrm{e}(-a_1\ell/(2^{v_2(q)}\dot{q}\ddot{q}))}{\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q})\mathrm{lcm}(4, 2^{v_2(q)}\dot{q}\ddot{q}/\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q}))}$$
$$\times \prod_{\substack{p \text{ prime} \\ v_p(\ddot{q})>v_p(\ell)}} \left(1-\frac{1}{p}\right)^{-1},$$

where the sum is over ℓ with

$$\frac{2^t k^2}{\gcd(2^t k^2, 2^{v_2(q)}\ddot{q})} \equiv \frac{\ell}{\gcd(\ell, 2^{v_2(q)}\dot{q}\ddot{q})} \left(\mathrm{mod}\ \gcd\left(4, \frac{2^{v_2(q)}}{\gcd(\ell, 2^{v_2(q)})}\right)\right).$$

We now use the fact that replacing ℓ by $\ell + 2^{v_2(q)}\dot{q}\ddot{q}$ leaves the last sum invariant. The Chinese remainder theorem allows to uniquely write

$$\ell \equiv \ell_1\dot{q}\ddot{q} + \ell_2 2^{v_2(q)}\ddot{q} + \ell_3 2^{v_2(q)}\dot{q} \left(\mathrm{mod}\ 2^{v_2(q)}\dot{q}\ddot{q}\right)$$

for some

$$\ell_1 \in \mathbb{Z} \cap [0, 2^{v_2(q)}),\ \ell_2 \in \mathbb{Z} \cap [0, \dot{q}) \text{ and } \ell_3 \in \mathbb{Z} \cap [0, \ddot{q}).$$

Then $T_{a_1,q}(t,k)$ becomes

$$\sum_{\substack{\ell_1\in\mathbb{Z}\cap[0,2^{v_2(q)})\\ \ell_2\in\mathbb{Z}\cap[0,\dot q)\\ \ell_3\in\mathbb{Z}\cap[0,\dot q)\\ \gcd(k^2,\ddot q)\mid\ell_3\\ 2^{\min\{t,v_2(q)\}}\mid\ell_1}} \frac{\varpi\big(\frac{\gcd(\ell_1,2^{v_2(q)})}{2^{\min\{t,v_2(q)\}}}\gcd(\ell_2,\dot q)\frac{\gcd(\ell_3,\ddot q)}{\gcd(k^2,\ddot q)}\big)\,\mathrm{e}\big(\frac{-a_1\ell_1}{2^{v_2(q)}}\big)\,\mathrm{e}\big(\frac{-a_1\ell_2}{\dot q}\big)\,\mathrm{e}\big(\frac{-a_1\ell_3}{\ddot q}\big)}{\gcd(\ell_1,2^{v_2(q)})\mathrm{lcm}(4,2^{v_2(q)}/\gcd(\ell_1,2^{v_2(q)}))\dot q\ddot q}$$

$$\times \prod_{\substack{p\text{ prime}\\ v_p(\ddot q)>v_p(\ell_3)}}\Big(1-\frac{1}{p}\Big)^{-1},$$

where the sum is over ℓ_1,ℓ_3 with

$$\frac{2^{t-\min\{t,v_2(q)\}}}{\gcd(k^2,\ddot q)}\equiv\frac{\ell_1\ddot q}{\gcd(\ell_1,2^{v_2(q)})\gcd(\ell_3,\ddot q)}\left(\mathrm{mod}\ \gcd\Big(4,\frac{2^{v_2(q)}}{\gcd(\ell_1,2^{v_2(q)})}\Big)\right).$$

Indeed, modulo $\gcd\Big(4,\frac{2^{v_2(q)}}{\gcd(\ell_1,2^{v_2(q)})}\Big)$, the term $\ell_2 2^{v_2(q)}\ddot q+\ell_3 2^{v_2(q)}\dot q$ vanishes. Note furthermore that we have used that each of k^2, $\dot q$ and $\gcd(\ell_2,\dot q)$ is $1\,(\mathrm{mod}\ 4)$. This holds because k is odd and each prime divisor of $\dot q$ is $1\,(\mathrm{mod}\ 4)$. Moreover, the presence of the $\varpi(\cdot)$ means that we may freely restrict to the case

$$\gcd(\ell_1,2^{v_2(q)})=2^{\min\{t,v_2(q)\}}\ \text{and}\ \gcd(\ell_3,\ddot q)=\gcd(k^2,\ddot q).$$

Put together, these two facts show that $T_{a_1,q}(t,k)$ equals

$$\frac{\mathcal{K}_{a_1,q}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}(4,2^{v_2(q)-\min\{t,v_2(q)\}})}\frac{\mathcal{W}_{a_1,\ddot q}(k)}{\ddot q}\frac{1}{\dot q}\sum_{\ell_2\in\mathbb{Z}/\dot q\mathbb{Z}}\mathrm{e}(-a_1\ell_2/\dot q),$$

thus concluding the proof. □

Essentially, the last lemma breaks up the information of the prime 2, carried by the factor involving $\mathcal{K}_{a,q}(t)$, and the information on the primes $p\equiv 3\,(\mathrm{mod}\ 4)$, carried by the factor involving $\mathcal{W}_{a,\ddot q}(k)$. The last factor with values in $\{0,1\}$ sieves out possible values of a for any given q and arises from a Ramanujan sum in the last line of the proof.

LEMMA 3.5.4. *For fixed $k\in\mathbb{Z}_{>0}$, $a\in\mathbb{Z}$ the function $\mathcal{W}_{a,q}(k)$ is multiplicative with respect to q.*

Proof. For positive coprime integers q_1 and q_2 we note that any element $\ell \in \mathbb{Z}/q_1q_2\mathbb{Z}$ can be written uniquely as $\ell_1 q_2 + \ell_2 q_1$, for $\ell_1 \in \mathbb{Z}/q_1\mathbb{Z}$ and $\ell_2 \in \mathbb{Z}/q_2\mathbb{Z}$. From this the validity of $\mathcal{W}_{a,q_1q_2}(k) = \mathcal{W}_{a,q_1}(k)\mathcal{W}_{a,q_2}(k)$ follows easily. □

Before we state the next lemma, recall the Ramanujan sum from (3.6).

LEMMA 3.5.5. *For fixed $a, m \in \mathbb{Z}_{\geq 0}$, $k \in \mathbb{Z}_{>0}$, and any prime p define $j := m - 2v_p(k)$. Then we have*

$$\mathcal{W}_{a,p^m}(k) = \begin{cases} c_{p^j}(-a)(1-1/p)^{-1}, & \text{if } 2v_p(k) < m, \\ 1, & \text{if } 2v_p(k) \geq m. \end{cases}$$

Proof. For $2v_p(k) \geq m$, only the term $\ell = 0$ contributes towards $\mathcal{W}_{a,p^m}(k)$, in which case the sum equals 1. For $0 \leq 2v_p(k) < m$, every ℓ in (3.45) must be of the form $\ell = xp^{2v_p(k)}$, where $x \in \mathbb{Z} \cap [0, p^j)$ and $p \nmid x$ hold, which concludes the proof. □

Define for $a, \varrho, t \in \mathbb{Z}_{\geq 0}$ the symbol

$$\Lambda_{a,\varrho}(t) := \mathrm{e}(-a/2^{\varrho-t})\mathbf{1}_{v_2(a)\geq \varrho-t-2}. \tag{3.47}$$

LEMMA 3.5.6. *For $q \in \mathbb{Z}_{>0}$, let q_0 be any integer satisfying the congruence $q_0 \equiv \ddot{q} \pmod{2^{\min\{2,v_2(q)\}}}$. Then for all $a, t \in \mathbb{Z}_{\geq 0}$ and $q \in \mathbb{Z}_{>0}$ we have*

$$\frac{\mathcal{K}_{a,q}(t)}{\mathrm{lcm}(4, 2^{v_2(q)-\min\{t,v_2(q)\}})} = \frac{\Lambda_{aq_0,v_2(q)}(t)}{4}.$$

Proof. If $v_2(q) \leq t$ holds then we have

$$\mathcal{K}_{a,q}(t) = \sum_{\substack{\ell \in \mathbb{Z}\cap[0,2^{v_2(q)}) \\ 2^{v_2(q)}\mid \ell}} \mathrm{e}(-a\ell/2^{v_2(q)}) = 1,$$

so the left-hand side equals 1/4. On the right-hand side of the equation, we see that $v_2(q)-t-2$ is negative, so $v_2(aq_0)$ is certainly larger. Moreover, $-aq_0/2^{t-v_2(q)}$ is an integer. Hence both the exponential and the indicator take the value 1.

If $v_2(q) > t$ holds then we have

$$\begin{aligned}\mathcal{K}_{a,q}(t) &= \sum_{\substack{\ell \in \mathbb{Z} \cap [0, 2^{v_2(q)}) \\ 2^t \mid \ell, 2^{t+1} \nmid \ell \\ 1 \equiv \frac{\ell \ddot{q}}{2^t} \left(\mathrm{mod}\ 2^{\min\{2, v_2(q)-t\}}\right)}} \mathrm{e}(-a\ell/2^{v_2(q)}) \\ &= \sum_{\substack{x \in \mathbb{Z} \cap [0, 2^{v_2(q)-t}) \\ x \equiv \ddot{q} \left(\mathrm{mod}\ 2^{\min\{2, v_2(q)-t\}}\right)}} \mathrm{e}(-ax/2^{v_2(q)-t}),\end{aligned}$$

where the condition $x \equiv \ddot{q}$ is equivalent to $1 \equiv x\ddot{q}$ as $\ddot{q}^2 \equiv 1 \,(\mathrm{mod}\ 2)$ and $\ddot{q}^2 \equiv 1 \,(\mathrm{mod}\ 4)$ hold.

If $v_2(q) - t$ equals 1 then this becomes $\mathrm{e}(a/2)$, while, for $v_2(q) - t = 2$ this is equal to $\mathrm{e}(-a\ddot{q}/4)$. In the remaining cases we have $v_2(q) - t > 2$, hence also

$$\begin{aligned}\mathcal{K}_{a,q}(t) &= \sum_{\substack{x \in \mathbb{Z} \cap [0, 2^{v_2(q)-t}) \\ x \equiv \ddot{q} (\mathrm{mod}\ 4)}} \mathrm{e}(-ax/2^{v_2(q)-t}) \\ &= \mathrm{e}(-a\ddot{q}/2^{v_2(q)-t}) \sum_{y \in \mathbb{Z} \cap [0, 2^{v_2(q)-t-2})} \mathrm{e}(-ay/2^{v_2(q)-t-2}),\end{aligned}$$

which vanishes in case a is not a multiple of $2^{v_2(q)-t-2}$ and otherwise equals $\mathrm{e}(-a\ddot{q}/2^{v_2(q)-t})2^{v_2(q)-t-2}$. □

For each a and q having separated out the contributions to $T_{a,q}(t,k)$, we now do the same for their sums (weighted by $S_{\mathbf{a},q}$) over all possible values of $\mathbf{a}$ for given q.

LEMMA 3.5.7. *For all $k, q \in \mathbb{Z}_{>0}$ with $k = \ddot{k}$ and all $t \in \mathbb{Z}_{\geq 0}$ we have*

$$\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,q))^2\\ \gcd(a_1,a_2,q)=1}} S_{\mathbf{a},q}T_{a_1,q}(t,k) = \frac{1}{2^{2+\min\{t,v_2(q)\}}} \times \left(\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{v_2(q)}))^2\\ \gcd(b_1,b_2,2^{v_2(q)})=1}} S_{\mathbf{b},2^{v_2(q)}}\Lambda_{b_1,v_2(q)}(t) \right) \times \left(\sum_{\substack{b\in\mathbb{Z}\cap[0,\dot{q})\\ \gcd(b,\dot{q})=1}} \sum_{\mathbf{t}\in(\mathbb{Z}/\dot{q}\mathbb{Z})^n} \mathrm{e}\left(bf_2(\mathbf{t})/\dot{q}\right) \right) \times \left(\frac{1}{\ddot{q}} \sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,\ddot{q}))^2\\ \gcd(b_1,b_2,\ddot{q})=1}} S_{\mathbf{b},\ddot{q}}\mathcal{W}_{b_1,\ddot{q}}(k) \right).$$

Proof. By the Chinese remainder theorem we can uniquely write every $a_i \in \mathbb{Z}/q\mathbb{Z}$ as

$$a_i \equiv a_i'\dot{q}\ddot{q} + a_i''2^{v_2(q)}\ddot{q} + a_i'''2^{v_2(q)}\dot{q} \pmod{q}, \ (i = 1, 2),$$

with

$$a_i' \in \mathbb{Z}/2^{v_2(q)}\mathbb{Z}, a_i'' \in \mathbb{Z}/\dot{q}\mathbb{Z}, a_i''' \in \mathbb{Z}/\ddot{q}\mathbb{Z}.$$

Thus we see that the sum over $\mathbf{a} \in (\mathbb{Z} \cap [0, q))^2$ in the lemma equals

$$\sum_{\substack{\mathbf{a}''\in(\mathbb{Z}\cap[0,\dot{q}))^2,\gcd(a_1'',a_2'',\dot{q})=1\\ \mathbf{a}'''\in(\mathbb{Z}\cap[0,\ddot{q}))^2,\gcd(a_1''',a_2''',\ddot{q})=1\\ \mathbf{a}'\in(\mathbb{Z}\cap[0,2^{v_2(q)}))^2,\gcd(a_1',a_2',2^{v_2(q)})=1}} S_{\mathbf{a}'\dot{q}\ddot{q}+\mathbf{a}''2^{v_2(q)}\ddot{q}+\mathbf{a}'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}} \times T_{a_1'\dot{q}\ddot{q}+a_1''2^{v_2(q)}\ddot{q}+a_1'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t,k).$$

It is easy to check that whenever q_1 and q_2 are coprime positive integers and $\mathbf{a} \in \mathbb{Z}^2$, then, much like as in the proof of Lemma 1.3.11, we have

$$S_{\mathbf{a},q_1q_2} = S_{q_2^{d-1}\mathbf{a},q_1}S_{q_1^{d-1}\mathbf{a},q_2},$$

by the fact that for fixed $r \in \mathbb{Z}_{>0}$ the sum $S_{\mathbf{b},r}$ only depends on $\mathbf{b} \pmod{r}$.

From the above, we see that if q_1, q_2, q_3 are any positive integers that are coprime in pairs then we have

$$S_{\mathbf{a},q_1q_2q_3} = S_{(q_2q_3)^{d-1}\mathbf{a},q_1} S_{(q_1q_3)^{d-1}\mathbf{a},q_2} S_{(q_1q_2)^{d-1}\mathbf{a},q_3}.$$

Applying this for $\mathbf{a} = \mathbf{a}'\dot{q}\ddot{q} + \mathbf{a}''2^{v_2(q)}\ddot{q} + \mathbf{a}'''2^{v_2(q)}\dot{q}$, $q_1 = 2^{v_2(q)}$, $q_2 = \dot{q}$ and $q_3 = \ddot{q}$, we obtain

$$S_{\mathbf{a}'\dot{q}\ddot{q}+\mathbf{a}''2^{v_2(q)}\ddot{q}+\mathbf{a}'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}} = S_{(\dot{q}\ddot{q})^d\mathbf{a}',2^{v_2(q)}} S_{(2^{v_2(q)}\ddot{q})^d\mathbf{a}'',\dot{q}} S_{(2^{v_2(q)}\dot{q})^d\mathbf{a}''',\ddot{q}},$$

where we again made use of the fact that for fixed $r \in \mathbb{Z}_{>0}$ the sum $S_{\mathbf{b},r}$ only depends on $\mathbf{b} \pmod r$, as we will also do for $\mathcal{W}_{a,q}(k)$ and $\mathcal{K}_{a,q}(t)$ below.

By Lemma 3.5.3 one sees that $T_{a_1'\dot{q}\ddot{q}+a_1''2^{v_2(q)}\ddot{q}+a_1'''2^{v_2(q)}\dot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t,k)$ equals

$$\frac{\mathcal{K}_{a_1'\dot{q}\ddot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}\big(4, 2^{v_2(q)-\min\{t,v_2(q)\}}\big)} \frac{\mathcal{W}_{a_1'''2^{v_2(q)}\dot{q},\ddot{q}}(k)}{\ddot{q}} \times \begin{cases} 1, & \text{if } \dot{q} \mid a_1'', \\ 0, & \text{if } \dot{q} \nmid a_1'', \end{cases}$$

thus showing that the sum over $\mathbf{a} \in (\mathbb{Z} \cap [0,q))^2$ in the lemma equals $\mathcal{L}'\mathcal{L}''\mathcal{L}'''$, where we write

$$\mathcal{L}' := \sum_{\substack{\mathbf{a}' \in (\mathbb{Z}\cap[0,2^{v_2(q)}))^2 \\ \gcd(a_1',a_2',2^{v_2(q)})=1}} S_{(\dot{q}\ddot{q})^d\mathbf{a}',2^{v_2(q)}} \frac{\mathcal{K}_{a_1'\dot{q}\ddot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t)}{2^{\min\{t,v_2(q)\}}\mathrm{lcm}\big(4, 2^{v_2(q)-\min\{t,v_2(q)\}}\big)},$$

$$\mathcal{L}'' := \sum_{\substack{\mathbf{a}'' \in (\mathbb{Z}\cap[0,\dot{q}))^2, \dot{q} \mid a_1'' \\ \gcd(a_1'',a_2'',\dot{q})=1}} S_{(2^{v_2(q)}\ddot{q})^d\mathbf{a}'',\dot{q}},$$

$$\mathcal{L}''' := \sum_{\substack{\mathbf{a}''' \in (\mathbb{Z}\cap[0,\ddot{q}))^2 \\ \gcd(a_1''',a_2''',\ddot{q})=1}} S_{(2^{v_2(q)}\dot{q})^d\mathbf{a}''',\ddot{q}} \frac{\mathcal{W}_{a_1'''2^{v_2(q)}\dot{q},\ddot{q}}(k)}{\ddot{q}}.$$

To simplify $\mathcal{L}''$ we make an invertible change of variables, namely we will write $b \equiv (2^{v_2(q)}\ddot{q})^d a_2'' \pmod{\dot{q}}$. This results in

$$\mathcal{L}'' = \sum_{\substack{b \in \mathbb{Z}\cap[0,\dot{q}) \\ \gcd(b,\dot{q})=1}} \sum_{\mathbf{t} \in (\mathbb{Z}/\dot{q}\mathbb{Z})^n} \mathrm{e}\big(bf_2(\mathbf{t})/\dot{q}\big).$$

Similarly, for $\mathcal{L}'''$ we make the change of variables $\mathbf{b} \equiv (2^{v_2(q)}\dot{q})^d \mathbf{a}''' \pmod{\ddot{q}}$ and use (3.46) to show the validity of

$$cL''' = \frac{1}{\ddot{q}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,\ddot{q}))^2 \\ \gcd(b_1,b_2,\ddot{q})=1}} S_{\mathbf{b},\ddot{q}} \mathcal{W}_{b_1,\ddot{q}}(k).$$

Finally, put $\mathbf{b} \equiv (\dot{q}\ddot{q})^d \mathbf{a}' \pmod{2^{v_2(q)}}$ and find some $y \in \mathbb{Z}$ which satisfies $y\dot{q}\ddot{q} \equiv 1 \pmod{2^{v_2(q)}}$. Observing that $\dot{q}\ddot{q}a_1' \equiv b_1 y^{d-1} \pmod{2^{v_2(q)}}$ holds, we see $\mathcal{K}_{a_1'\dot{q}\ddot{q},2^{v_2(q)}\dot{q}\ddot{q}}(t) = \mathcal{K}_{b_1 y^{d-1},2^{v_2(q)}\dot{q}\ddot{q}}(t)$. Note that d is even and that y is odd, hence the proof is concluded by application of Lemma 3.5.6 with $a = b_1 y^{d-1}$ and $q_0 := y^{d-1}$, made possible by the validity of

$$y^{d-1} \equiv y \equiv (\dot{q}\ddot{q})^{-1} \equiv \ddot{q} \pmod{2^{\min\{2,v_2(q)\}}}.$$

Indeed, we have $\Lambda_{b_1(y^{d-1})^2,v_2(q)}(t) = \Lambda_{b_1,v_2(q)}(t)$ since $\Lambda_{a,\varrho}(t)$ only depends on a through $a \pmod{2^{\varrho-t}}$. □

We will continue our journey in splitting into factors coming from different primes with $\mathbb{L}_\phi(k,t)$. We will first need some notation.

For $t \in \mathbb{Z}_{\geq 0}$ and $k \in \mathbb{Z}_{>0}$ with $\ddot{k} = k$ define

$$\Upsilon_1(k) := \sum_{\substack{q_3 \in \mathbb{Z}_{>0} \\ p|q_3 \Rightarrow p \equiv 3 \pmod 4}} \frac{\gcd(k^2,q_3)}{q_3^{n+1}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,q_3))^2 \\ \gcd(b_1,b_2,q_3)=1}} S_{\mathbf{b},q_3} \mathcal{W}_{b_1,q_3}(k) \tag{3.48}$$

and

$$\Upsilon_2(t) := \frac{1}{4} \sum_{\varrho \in \mathbb{Z}_{\geq 0}} \frac{1}{2^{\varrho n}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,2^\varrho))^2 \\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho} \Lambda_{b_1,\varrho}(t). \tag{3.49}$$

For a prime p define

$$\tau_{f_2}(p) := \lim_{N \to \infty} \frac{\#\{\mathbf{t} \in (\mathbb{Z} \cap [0,p^N))^n : f_2(\mathbf{t}) \equiv 0 \pmod{p^N}\}}{p^{N(n-1)}} \tag{3.50}$$

and let us now see why the limit exists. Our set-up and assumption (3.1) ensure that the work of Birch [Bir62] applies to the hypersurface $f_2 = 0$. In particular, the constant $K = K(f_2)$, defined in (1.6) equals $2^{1-d}n$ because f_2 has no singularities. Furthermore, one should notice that we have

$$\tau_{f_2}(p) = 1 + \sum_{m=1}^{\infty} \frac{1}{p^{mn}} \sum_{a \in (\mathbb{Z}/p^m\mathbb{Z})^*} \sum_{\mathbf{t} \in (\mathbb{Z} \cap [0,p^m))^n} \mathrm{e}\left(\frac{af_2(\mathbf{t})}{p^m}\right) \tag{3.51}$$

coming from the fact that

$$p^{N(n-1)}\sum_{m=0}^{N}\frac{1}{p^{mn}}\sum_{a\in(\mathbb{Z}/p^m\mathbb{Z})^*}\sum_{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n}\mathrm{e}\Big(\frac{af_2(\mathbf{t})}{p^m}\Big) \tag{3.52}$$

equals $\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : f_2(\mathbf{t})\equiv 0\big(\mathrm{mod}\ p^N\big)\big\}$ and that the $m=0$ term equals 1. Alternatively, the existence of the limit $\tau_{f_2}(p)$ could be established by using Hensel's lemma and the fact that f_2 defines a smooth hypersurface over $\mathbb{Q}_p$.

Using Lemma 1.3.34 to bound the sum over $\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n$ by an order of magnitude $\ll_\varepsilon p^{m(\varepsilon-n+n(d-1)^{-1}2^{-d+1})}$ (valid for all fixed $\varepsilon>0$), shows that, when (3.1) is used in the form $n\geq 1+3(d-1)2^d$ and $\varepsilon=(d-1)^{-1}2^{-d+1}$ is taken, the last series over m converges absolutely. Therefore the limit in (3.50) exists. In addition we get

$$\tau_{f_2}(p)=1+O(p^{\varepsilon-5+(d-1)^{-1}2^{-d+1}})=1+O(p^{-2}). \tag{3.53}$$

Lemma 3.5.8. *Under the assumptions of Theorem 3.1.3, for all $t\in\mathbb{Z}_{\geq 0}$ and $k\in\mathbb{Z}_{>0}$ with $\ddot{k}=k$, the sums in* (3.48) *and* (3.49) *both converge absolutely. We furthermore have*

$$\mathbb{L}_\phi(k,t)=\Upsilon_1(k)\Upsilon_2(t)\prod_{p\equiv 1(\mathrm{mod}\ 4)}\tau_{f_2}(p).$$

Proof. The assumptions of Theorem 3.1.3 allow us to use the bound from equation (3.28), which, when combined with the bounds $\gcd(k^2,q_3)\leq k^2$ and $|\mathcal{W}_{b_1,q_3}(k)|\leq q_3$, shows that the sum over q_3 in (3.48) converges absolutely. To prove the analogous statement for the sum over ϱ in (3.49) we use the bound (3.28) as well as the inequality $|\Lambda_{b_1,\varrho}(t)|\leq 1$ that is apparent from (3.47).

To complete the proof of the lemma, we write each q in (3.43) as $q=2^\varrho q_1q_3$, denoting $q_1=\dot{q}$ and $q_3=\ddot{q}$ and we inject Lemma 3.5.7 into (3.43) to obtain $\mathbb{L}_\phi(k,t)=\Upsilon_1(k)\Upsilon_2(t)\Xi$, with

$$\Xi:=\sum_{\substack{q_1\in\mathbb{Z}_{>0}\\ p|q_1\Rightarrow p\equiv 1(\mathrm{mod}\ 4)}}\frac{1}{q_1^n}\sum_{b\in(\mathbb{Z}/q_1\mathbb{Z})^*}\sum_{\mathbf{t}\in(\mathbb{Z}/q_1\mathbb{Z})^n}\mathrm{e}\big(bf_2(\mathbf{t})/q_1\big).$$

It is standard that the sum over $b\in(\mathbb{Z}/q_1\mathbb{Z})^*$ forms a multiplicative function of q_1, see, for example, [Bir62, §7] with $R=1$ or Lemma 1.3.11. Thus, using the expression for $\tau_{f_2}(p)$ in (3.51), we obtain the equality of Ξ with the product over the primes $p\equiv 1\,(\mathrm{mod}\ 4)$ in the lemma. □

Let us now define the quantities $E_\phi(p)$ for every prime $p \equiv 3 \pmod 4$ and for $p = 2$ as follows: if $p \equiv 3 \pmod 4$ then we let

$$E_\phi(p) := \sum_{\kappa,m \in \mathbb{Z}_{\geq 0}} \Phi_{\kappa,m} p^{-2\kappa}, \tag{3.54}$$

with

$$\Phi_{\kappa,m} := \frac{\gcd(p^{2\kappa}, p^m)}{p^{m(n+1)}} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0,p^m))^2 \\ \gcd(a_1,a_2,p^m)=1}} S_{\mathbf{a},p^m} \mathcal{W}_{a_1,p^m}(p^\kappa). \tag{3.55}$$

We furthermore define

$$E_\phi(2) := \frac{1}{4} \sum_{t,\varrho \in \mathbb{Z}_{\geq 0}} \frac{1}{2^t} \frac{1}{2^{\varrho n}} \sum_{\substack{\mathbf{b} \in (\mathbb{Z} \cap [0,2^\varrho))^2 \\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho} \, \mathrm{e}(-b_1 2^{t-\varrho}) \mathbf{1}_{v_2(b_1) \geq \varrho - t - 2}. \tag{3.56}$$

With this newest notation, we are finally ready to write $\mathbb{L}_\phi$ itself as a product of factors coming from each of the primes.

LEMMA 3.5.9. *Keep the assumptions of Theorem 3.1.3. Then the sums in* (3.54) *and* (3.56) *converge absolutely. In addition, the infinite product*

$$E_\phi(2) \Big(\prod_{p \equiv 1 \pmod 4} \tau_{f_2}(p) \Big) \Big(\prod_{p \equiv 3 \pmod 4} E_\phi(p) \Big)$$

converges absolutely and equals $\mathbb{L}_\phi$.

Proof. Our first task is to show that the sum in (3.54) converges absolutely. For this we use Lemma 3.5.5 and the obvious bound $|c_{p^j}(-a)| \leq p^j$ to obtain

$$|\mathcal{W}_{a_1,p^m}(p^\kappa)| \leq 2 \frac{p^m}{\gcd(p^{2\kappa}, p^m)}.$$

Therefore, by (3.28), for every $0 < \lambda < 2^{-d}(d-1)^{-1}$ we have

$$\Phi_{\kappa,m} \ll \frac{\gcd(p^{2\kappa}, p^m)}{p^{m(n+1)}} p^{2m} p^{m(n-3-\lambda)} \frac{p^m}{\gcd(p^{2\kappa}, p^m)} \ll_\lambda p^{-m(1+\lambda)},$$

with an implied constant that depends at most on λ, f_1 and f_2. This shows that for all integers $M \geq 0$ and every $0 < \lambda < 2^{-d}(d-1)^{-1}$ one has

$$\sum_{\kappa \geq 0} \frac{1}{p^{2\kappa}} \sum_{m \geq M} |\Phi_{\kappa,m}| \ll_\lambda \frac{1}{p^{M(1+\lambda)}}. \tag{3.57}$$

This completes our first task. The proof of the absolute convergence for the sum in (3.56) can be completed in a similar way by using (3.28) again. To show that the product over the primes $p \equiv 1 \,(\mathrm{mod}\, 4)$ in our lemma converges absolutely one can simply utilise (3.53). The product over the primes $p \equiv 3 \,(\mathrm{mod}\, 4)$ converges absolutely because the use of (3.57) with $M = 1$ and (3.54) yields

$$E_{\phi}(p) = \sum_{\kappa \in \mathbb{Z}_{\geq 0}} \Phi_{\kappa,0} p^{-2\kappa} + O(p^{-1-\lambda}) = \sum_{\kappa \in \mathbb{Z}_{\geq 0}} p^{-2\kappa} + O(p^{-1-\lambda})$$

and using $\sum_{\kappa \geq 0} p^{-2\kappa} = 1 + O(p^{-2})$ and $\lambda < 1$ provides us with

$$\lambda \in (0, 2^{-d}(d-1)^{-1}) \Rightarrow E_{\phi}(p) = 1 + O_{\lambda}(p^{-1-\lambda}). \tag{3.58}$$

Since for every $\lambda > 0$, the sum $\sum_{p \equiv 3 (\mathrm{mod}\ 4)} p^{-1-\lambda}$ converges absolutely, we conclude that so does the product $\prod_{p \equiv 3 (\mathrm{mod}\ 4)} E_{\phi}(p)$.

To prove the claimed equality of our lemma we combine Lemma 3.5.2 and Lemma 3.5.8 to obtain

$$\mathbb{L}_{\phi} = \Big(\sum_{t \in \mathbb{Z}_{\geq 0}} \frac{\Upsilon_2(t)}{2^t} \Big) \Big(\prod_{p \equiv 1 (\mathrm{mod}\ 4)} \tau_{f_2}(p) \Big) \Big(\sum_{\substack{k \in \mathbb{Z}_{>0} \\ p|k \Rightarrow p \equiv 3 (\mathrm{mod}\ 4)}} \frac{\Upsilon_1(k)}{k^2} \Big). \tag{3.59}$$

By (3.48) we can write the sum over $k \in \mathbb{Z}_{>0}$ as a double sum over k and q_3 and one obtains the infinite product over the primes $p \equiv 3 \,(\mathrm{mod}\, 4)$ in our lemma by application of a two-dimensional analogue for converting infinite sums into Euler products. Such an analogue can for example be found in [Hoo93, Lemma 4, pg.20] Lastly, the sum over t in (3.59) can be shown to be equal to $E_{\phi}(2)$ by application of (3.49). □

We are still left with interpreting the factors occurring in the last lemma. Before embarking on the next subsections we introduce some more notation and record some preparatory observations.

For primes p and integers $0 \leq i, j \leq m$ we define the quantity

$$\xi_{i,j}(m) := \#\big\{ \mathbf{t} \in (\mathbb{Z} \cap [0, p^m)^n : p^i \mid f_1(\mathbf{t}), p^j \mid f_2(\mathbf{t}) \big\}. \tag{3.60}$$

The quantity $\xi_{i,j}(m)$ also depends on p, however, we choose to not record this in the notation as it will be clear from the context what the underlying prime is. The following is a restatement of the last equation in [Bir62,

pg.259], and which we have already used in studying (3.50) for the case of a single polynomial, where we now have a pair:

$$\sum_{0\leq m\leq N}\frac{1}{p^{mn}}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ \gcd(a_1,a_2,p^m)=1}} S_{\mathbf{a},p^m}=\frac{\xi_{N,N}(N)}{p^{N(n-2)}}. \tag{3.61}$$

Using it for $m=N$ and $m=N-1$ both, we obtain that for every $N\in\mathbb{Z}_{>0}$ we have

$$\sum_{\substack{\mathbf{a}\in([0,p^N))^2\\ \gcd(a_1,a_2,p^N)=1}} S_{\mathbf{a},p^N}=p^{2N}\xi_{N,N}(N)-p^{2N+n-2}\xi_{N-1,N-1}(N-1). \tag{3.62}$$

Observe that injecting the bound (3.28) into (3.61) shows that for $M\geq 0$ we have

$$\xi_{M,M}(M)=O_p\big(p^{M(n-2)}\big). \tag{3.63}$$

Lemma 3.5.10. *Keep the assumptions of Theorem 3.1.3. Then for every $m_1,m_2,M\in\mathbb{Z}_{>0}$ with $m_1\leq m_2\leq M$, and every prime p we have*

$$\xi_{m_1,m_2}(M)=O_p(p^{Mn-2m_1}).$$

Proof. Notice that we have

$$\xi_{m_1,m_2}(M)\leq \#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^{m_1}))^n : p^{m_1}\mid f_1(\mathbf{t}), p^{m_1}\mid f_2(\mathbf{t})\big\}p^{n(M-m_1)}.$$

Thus using (3.63) we conclude that $\xi_{m_1,m_2}(M)=O_p(p^{m_1(n-2)}p^{n(M-m_1)})$. □

3.5.2 Local density at primes $3\,(\mathrm{mod}\,4)$

The following is the main result of this section.

Proposition 3.5.11. *Let p be a prime number with $p\equiv 3\,(\mathrm{mod}\,4)$. Then under the assumptions of Theorem 3.1.3, the sequence*

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : f_2(\mathbf{t})\equiv 0\,(\mathrm{mod}\,p^N), x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has a } \mathbb{Q}_p\text{-point}\big\}}{p^{N(n-1)}}$$

has a limit for $N\to\infty$. We call the value of this limit ℓ_p and we have $E_\phi(p)=\big(1-1/p\big)^{-1}\ell_p$.

For the rest of §3.5.2 the letter p will always refer to a prime satisfying $p \equiv 3 \pmod 4$. To prove Proposition 3.5.11 we split the sum over κ and m in the definition of $E_\phi(p)$ according to the three ranges $0 \le m \le 2\kappa$, $m = 2\kappa + 1$ and $m \ge 2\kappa + 2$. These ranges will be treated in Lemmas 3.5.12, 3.5.13 and 3.5.16 respectively.

LEMMA 3.5.12. *Keep the assumptions of Theorem 3.1.3. Then for every prime $p \equiv 3 \pmod 4$ and $M \in \mathbb{Z}_{>0}$ the following holds,*

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{0 \le m \le \min\{M, 2\kappa\}} \Phi_{\kappa,m} = \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-1)}} + O(p^{-M}).$$

Proof. By (3.57) the sum over κ, m in the lemma equals

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{0 \le m \le 2\kappa} \Phi_{\kappa,m} + O(p^{-M}).$$

Owing to Lemma 3.5.5 and (3.61), the new sum over κ, m can be expressed as

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{0 \le m \le 2\kappa} \frac{1}{p^{mn}} \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0, p^m))^2 \\ \gcd(a_1, a_2, p^m) = 1}} S_{\mathbf{a}, p^m} = \sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-2)}} = \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-1)}},$$

thus finishing the proof. □

Recall the definition of the Ramanujan sum in (3.6) and for $\kappa, m \in \mathbb{Z}_{\ge 0}$ with $2\kappa < m$ define

$$\Omega_{\kappa,m} := \sum_{\substack{\mathbf{a} \in (\mathbb{Z} \cap [0, p^m))^2 \\ p \nmid \mathbf{a}}} S_{\mathbf{a}, p^m} c_{p^{m-2\kappa}}(-a_1).$$

We then obtain via Lemma 3.5.5 that, in the range $0 \le 2\kappa < m$, we have

$$\frac{\Phi_{\kappa,m}}{p^{2\kappa}} = \left(1 - \frac{1}{p}\right)^{-1} \frac{\Omega_{\kappa,m}}{p^{m(n+1)}}. \tag{3.64}$$

LEMMA 3.5.13. *Keep the assumptions of Theorem 3.1.3. Then for every prime $p \equiv 3 \pmod 4$ and $M \in \mathbb{Z}_{>0}$ the following holds:*

$$\sum_{\kappa \ge 0} \frac{1}{p^{2\kappa}} \sum_{\substack{0 \le m \le M \\ m = 1 + 2\kappa}} \Phi_{\kappa,m} = \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,1+2\kappa}(1+2\kappa) - \xi_{1+2\kappa,1+2\kappa}(1+2\kappa)}{(1-1/p)p^{(1+2\kappa)(n-1)}}$$
$$- \sum_{\kappa \ge 0} \frac{\xi_{2\kappa,2\kappa}(2\kappa)}{p^{2\kappa(n-1)}} + O(p^{-M}).$$

Proof. First, note that by (3.57) the sum over κ and m in the lemma equals

$$\sum_{\kappa\geq 0} p^{-2\kappa}\Phi_{\kappa,1+2\kappa} + O(p^{-M}).$$

Now using (3.7) we get that $\Omega_{\kappa,m}$ is

$$\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\Big(p\mathbf{1}_{p|a_1}-1\Big) = p\Big(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p|a_1,p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\Big)-\Big(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\Big).$$

Writing $a_1 = bp$, we see that $\Omega_{\kappa,m}$ becomes

$$p\left(\sum_{\substack{a_2\in\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ b\in\mathbb{Z}\cap[0,p^{m-1})}} S_{(bp,a_2),p^m}\right) - \left(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}\right)$$

and the first term equals

$$\begin{aligned} &p\sum_{\substack{a_2\in\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ \mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n}} \mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big)\sum_{b\in\mathbb{Z}\cap[0,p^{m-1})} \mathrm{e}\Big(\frac{b f_1(\mathbf{t})}{p^{m-1}}\Big)\\ &\quad = p^m \sum_{\substack{a_2\in\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ \mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n, p^{m-1}|f_1(\mathbf{t})}} \mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big).\end{aligned}$$

The use of the identity (3.7) for the Ramanujan sums appearing in the last line helps in concluding that $\Omega_{\kappa,m}$ equals

$$\begin{aligned} &p^m\left(\Big(\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^m|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} (p-1)p^{m-1}\Big) - \Big(\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m-1}\|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} p^{m-1}\Big)\right)\\ &\quad - \sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m}.\end{aligned}$$

We note that $p^{m-1}\|f_2(\mathbf{t})$ holds if and only if $p^{m-1}|f_2(\mathbf{t})$ does and $p^m \mid f_2(\mathbf{t})$ does not hold. Therefore we have

$$\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m-1}\|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} 1 = \sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m-1}|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} 1 - \sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{m}|f_2(\mathbf{t}),\ p^{m-1}|f_1(\mathbf{t})}} 1,$$

which is obviously equal to $p^n\xi_{m-1,m-1}(m-1)-\xi_{m-1,m}(m)$. Hence $\Omega_{\kappa,m}$ becomes

$$\begin{aligned}
&p^m\Big((p-1)p^{m-1}\xi_{m-1,m}(m)-p^{m-1}\Big\{p^n\xi_{m-1,m-1}(m-1)-\xi_{m-1,m}(m)\Big\}\Big)\\
&\quad-\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}}S_{\mathbf{a},p^m}\\
&=p^{2m}\xi_{m-1,m}(m)-p^{2m-1+n}\xi_{m-1,m-1}(m-1)-\sum_{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2,\ p\nmid\mathbf{a}}S_{\mathbf{a},p^m}.
\end{aligned}$$

Thus, by (3.62) we get

$$\begin{aligned}
\Omega_{\kappa,m}=&p^{2m}\xi_{m-1,m}(m)-p^{2m-1+n}\xi_{m-1,m-1}(m-1)\\
&-\xi_{m,m}(m)p^{2m}+p^{2m+n-2}\xi_{m-1,m-1}(m-1)\\
=&p^{2m}(\xi_{m-1,m}(m)-\xi_{m,m}(m))-\xi_{m-1,m-1}(m-1)p^{2m+n-1}(1-p^{-1}).
\end{aligned}$$

Therefore, using (3.64) we infer that $\sum_{\kappa\geq0}\Phi_{\kappa,2\kappa+1}p^{-2\kappa}$ equals

$$\begin{aligned}
\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{1}{p^{m(n+1)}}&(p^{2m}(\xi_{m-1,m}(m)-\xi_{m,m}(m))\\
&-\xi_{m-1,m-1}(m-1)p^{2m+n-1}(1-p^{-1}))
\end{aligned}$$

which is

$$\begin{aligned}
&\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{p^{2m}(\xi_{m-1,m}(m)-\xi_{m,m}(m))}{p^{m(n+1)}}\\
&\qquad-\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{\xi_{m-1,m-1}(m-1)p^{2m+n-1}}{p^{m(n+1)}}\\
&=\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{(\xi_{m-1,m}(m)-\xi_{m,m}(m))}{p^{m(n-1)}}\\
&\qquad-\sum_{\substack{\kappa\geq0\\ m=1+2\kappa}}\frac{\xi_{m-1,m-1}(m-1)}{p^{(m-1)(n-1)}},
\end{aligned}$$

thus concluding the proof. □

Remark 3.5.14. Taking a step back from the technicalities in the proof, we remark that it is the appearance of the Ramanujan sums that allows us to switch away from the exponential sums in $\Phi_{\kappa,m}$ and into congruential properties of $f_1(\mathbf{t})$ and $f_2(\mathbf{t})$ modulo powers of p.

In order to study the contribution towards $E_\phi(p)$ of the range $\kappa \geq 2+2m$, we shall first need a preparatory lemma.

Lemma 3.5.15. *For each prime $p \equiv 3 \pmod 4$ and all non-negative integers $\kappa \leq -1 + m/2$, the value of $\frac{\Omega_{\kappa,m}}{p^{m(n+1)}}$ equals*

$$\frac{(\xi_{2\kappa,m}(m) - \xi_{1+2\kappa,m}(m))}{p^{m(n-1)}} - \frac{(\xi_{2\kappa,m-1}(m-1) - \xi_{1+2\kappa,m-1}(m-1))}{p^{(m-1)(n-1)}}.$$

Proof. Using (3.7) allows to write $\Omega_{\kappa,m}$ as

$$\begin{aligned}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p\nmid\mathbf{a}}} S_{\mathbf{a},p^m} c_{p^{m-2\kappa}}(-a_1) =& p^{m-2\kappa}\Big(\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m}\Big)\\ &- p^{m-2\kappa-1}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa-1}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m}.\end{aligned}$$

Writing $a_1 = p^{m-2\kappa}b$ shows

$$\begin{aligned}\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m} &= \sum_{\substack{a_2\in(\mathbb{Z}\cap[0,p^m),p\nmid a_2\\ \mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n}} \mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big)\sum_{b\in\mathbb{Z}\cap[0,p^{2\kappa})}\mathrm{e}\Big(\frac{b f_1(\mathbf{t})}{p^{2\kappa}}\Big)\\ &= p^{2\kappa}\sum_{\substack{a_2\in(\mathbb{Z}\cap[0,p^m)\\ \mathbf{t}\in(\mathbb{Z}/p^m\mathbb{Z})^n\\ p^{2\kappa}|f_1(\mathbf{t}),\ p\nmid a_2}}\mathrm{e}\Big(\frac{a_2 f_2(\mathbf{t})}{p^m}\Big).\end{aligned}$$

Recalling (3.6) and using (3.7), this can now be written as

$$\begin{aligned}p^{2\kappa}\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{2\kappa}|f_1(\mathbf{t})}} c_{p^m}(f_2(\mathbf{t})) =& p^{2\kappa+m}\sum_{\substack{\mathbf{t}\in(\mathbb{Z}\cap[0,p^m))^n\\ p^{2\kappa}|f_1(\mathbf{t}),p^m|f_2(\mathbf{t})}} 1\\ &- p^{2\kappa+m-1}\sum_{\substack{\mathbf{t}\in(\mathbb{Z}/p^m\mathbb{Z})^n\\ p^{2\kappa}|f_1(\mathbf{t}),p^{m-1}|f_2(\mathbf{t})}} 1\\ =& p^{2\kappa+m}\xi_{2\kappa,m}(m) - p^{n+2\kappa+m-1}\xi_{2\kappa,m-1}(m-1).\end{aligned}$$

A completely analogous argument shows

$$\sum_{\substack{\mathbf{a}\in(\mathbb{Z}\cap[0,p^m))^2\\ p^{m-2\kappa-1}|a_1,p\nmid a_2}} S_{\mathbf{a},p^m} = p^{1+2\kappa+m}\xi_{1+2\kappa,m}(m) - p^{n+2\kappa+m}\xi_{1+2\kappa,m-1}(m-1).$$

Therefore, we see that $\Omega_{\kappa,m}$ is

$$\begin{aligned} &p^{2m}(\xi_{2\kappa,m}(m) - p^{n-1}\xi_{2\kappa,m-1}(m-1)) \\ &\qquad - p^{2m-1}(p\xi_{1+2\kappa,m}(m) - p^n\xi_{1+2\kappa,m-1}(m-1)) \\ &= p^{2m}(\xi_{2\kappa,m}(m) - \xi_{1+2\kappa,m}(m)) \\ &\qquad - p^{2m-1+n}(\xi_{2\kappa,m-1}(m-1) - \xi_{1+2\kappa,m-1}(m-1)), \end{aligned}$$

thus concluding the proof. □

Lemma 3.5.16. *Under the assumptions of Theorem 3.1.3, fix any prime $p \equiv 3 \pmod 4$. Then for all $M \in \mathbb{Z}_{>0}$ we have equality of*

$$\sum_{\substack{0\le\kappa\le M/2-1\\ 2+2\kappa\le m\le M}} \frac{\Phi_{\kappa,m}}{p^{2\kappa}}$$

and

$$\begin{aligned} &\left(1-\frac{1}{p}\right)^{-1}\frac{\#\left\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\right\}}{p^{M(n-1)}} \\ &-\left(1-\frac{1}{p}\right)^{-1}\sum_{0\le\kappa\le -1+M/2}\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{p^{(1+2\kappa)(n-1)}} \end{aligned}$$

up to an error term that is $O_p(p^{-M})$.

Proof. From (3.64) and Lemma 3.5.15 we get that the sum over κ, m in our lemma equals

$$\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{0\le\kappa\le -1+M/2\\ 2+2\kappa\le m\le M}}\left(\frac{(\xi_{2\kappa,m}(m)-\xi_{1+2\kappa,m}(m))}{p^{m(n-1)}} - \frac{(\xi_{2\kappa,m-1}(m-1)-\xi_{1+2\kappa,m-1}(m-1))}{p^{(m-1)(n-1)}}\right).$$

Noting that for fixed κ the sum over m is telescopic, we can rewrite the last expression as

$$\left(1-\frac{1}{p}\right)^{-1}\sum_{0\le\kappa\le -1+M/2}\left(\frac{(\xi_{2\kappa,M}(M)-\xi_{1+2\kappa,M}(M))}{p^{M(n-1)}}\right.$$
$$\left.-\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{p^{(1+2\kappa)(n-1)}}\right).$$

Let us now focus on the first part of the sum. Definition (3.60) makes immediately apparent that $\sum_{0\le\kappa\le -1+M/2}(\xi_{2\kappa,M}(M)-\xi_{1+2\kappa,M}(M))$ equals

$$\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\cap[0,M-2]\big\}.$$

The contribution of those $\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n$ with $v_p(f_1(\mathbf{t}))\ge M-1$ can be controlled by using Lemma 3.5.10 with $m_1=M-1$ and $m_2=M$. We then obtain

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\cap[0,M-2]\big\}}{p^{M(n-1)}}$$
$$=\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{p^{M(n-1)}}+O_p(p^{-M}),$$

thereby proving that the sum over κ, m in our lemma is

$$\left(1-\frac{1}{p}\right)^{-1}\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{p^{M(n-1)}}$$
$$-\left(1-\frac{1}{p}\right)^{-1}\sum_{0\le\kappa\le -1+M/2}\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{p^{(1+2\kappa)(n-1)}}$$

up to an error term of $O_p(p^{-M})$. □

Lemma 3.5.17. *Under the assumptions of Theorem 3.1.3, fix any prime $p\equiv 3\,(\mathrm{mod}\ 4)$. Then for all $M\in\mathbb{Z}_{>0}$ we have*

$$\left(1-\frac{1}{p}\right)^{-1}\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{p^{M(n-1)}}=E_\Phi(p)$$

up to an error term of $O_p(p^{-M})$

Proof. Putting together Lemmas 3.5.12, 3.5.13 and 3.5.16 and taking into account the occurence of many cancellations, we obtain the equality of $\sum_{\kappa\geq 0}\frac{1}{p^{2\kappa}}\sum_{0\leq m\leq M}\Phi_{\kappa,m}$ and

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^M))^n : p^M \mid f_2(\mathbf{t}), v_p(f_1(\mathbf{t}))\in 2\mathbb{Z}\big\}}{(1-1/p)p^{M(n-1)}}+\mathcal{H}+O_p(p^{-M}),$$

where

$$\mathcal{H}:=\sum_{\kappa>-1+M/2}\frac{(\xi_{2\kappa,1+2\kappa}(1+2\kappa)-\xi_{1+2\kappa,1+2\kappa}(1+2\kappa))}{(1-1/p)p^{(1+2\kappa)(n-1)}}$$

comes from the part of the equation of Lemma 3.5.13 that is not cancelled out by any other terms. Next, note that Lemma 3.5.10 provides us with

$$\frac{|\xi_{2\kappa,1+2\kappa}(1+2\kappa)|+|\xi_{1+2\kappa,1+2\kappa}(1+2\kappa)|}{p^{(1+2\kappa)(n-1)}}\ll_p p^{-2\kappa}$$

and therefore $\mathcal{H}=O_p(p^{-M})$. Finally, (3.57) allows to complete the sum in the statement of the current lemma at the cost of an error term of size $O_p(p^{-M})$. □

Proof of Proposition 3.5.11. By Lemma 3.5.17 it is obvious that the sequence

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : f_1(\mathbf{t})\neq 0, p^N \mid f_2(\mathbf{t}), x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has a } \mathbb{Q}_p\text{-point}\big\}}{p^{N(n-1)}}$$

has a limit for $N\to\infty$, because for a non-zero integer m, the curve $x_0^2+x_1^2=mx_2^2$ has a $\mathbb{Q}_p$-point if and only if $v_p(m)$ is even. Furthermore, if $f_1(\mathbf{t})$ vanishes then p^N divides $f_1(\mathbf{t})$ and therefore the bound (3.63) shows that the condition $f_1(\mathbf{t})\neq 0$ can be removed from the numerator of the limit above. This proves the existence of the limit ℓ_p and it is clear that the equality $E_\Phi(p)=(1-1/p)^{-1}\ell_p$ follows instantly by Lemma 3.5.17. □

3.5.3 Local density at the prime 2

We begin by stating the main result of this section.

Proposition 3.5.18. *Under the assumptions of Theorem 3.1.3, the sequence*

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,2^N))^n : f_2(\mathbf{t})\equiv 0\pmod{2^N}, x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \textit{ has a } \mathbb{Q}_2\textit{-point}\big\}}{2^{N(n-1)}}$$

has a limit for $N \to \infty$ which we call ℓ_2 and we have $\ell_2 = E_\phi(2)$.

The proof of Proposition 3.5.18 will follow steps somewhat similar to those in the proof of Proposition 3.5.11. However, there will be now four cases rather than merely three, the reason being the presence of the term $\mathbf{1}_{v_2(b_1)\geq \varrho-t-2}$ in the definition of $E_\phi(2)$ in (3.56). The four cases will be $\varrho \leq t$, $\varrho = t+1$, $\varrho = t+2$, and $\varrho \geq t+3$ that will be dealt with in Lemmas 3.5.19, 3.5.20, 3.5.21 and 3.5.22 respectively. There are further minor differences between the proofs of Proposition 3.5.11 and Proposition 3.5.18. They are related to the difference between the two formulas $\ell_p = (1-1/p)E_\phi(p)$ and $\ell_2 = E_\phi(2)$.

Recall the definition of $S_{\mathbf{a},q}$ in (3.13) and that of $\xi_{i,j}(m)$ in (3.60).

LEMMA 3.5.19. *Under the assumptions of Theorem 3.1.3 the following two series converge absolutely:*

$$\sum_{t=0}^{\infty}\sum_{\varrho=0}^{t}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho}\,\mathrm{e}(-b_1 2^{t-\varrho})\mathbf{1}_{v_2(b_1)\geq\varrho-t-2},$$

and

$$\sum_{t=0}^{\infty}\frac{\xi_{t,t}(t)}{2^{t(n-1)}}.$$

In addition, they are equal.

Proof. The absolute convergence of the former sum is a direct consequence of (3.28), while the absolutely convergence of the latter sum is a consequence of (3.63). To verify the claimed equality observe that the first sum in the lemma can clearly be written as

$$\sum_{t\geq 0}\frac{1}{2^t}\sum_{0\leq\varrho\leq t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ \gcd(b_1,b_2,2^\varrho)=1}} S_{\mathbf{b},2^\varrho}$$

and by (3.61) the new sum over ϱ equals $\xi_{t,t}(t)2^{-t(n-2)}$. □

LEMMA 3.5.20. *Under the assumptions of Theorem 3.1.3 all series over $t \geq 0$ in the following two expressions converge absolutely:*

$$\sum_{t\geq 0}\frac{1}{2^t}\frac{1}{2^{(t+1)n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{t+1}))^2\\ \gcd(b_1,b_2,2)=1}} S_{\mathbf{b},2^{t+1}}\,\mathrm{e}(-b_1 2^{-1}),$$

and

$$2\sum_{t\ge 0}\frac{(\xi_{t,t+1}(t+1)-\xi_{t+1,t+1}(t+1))}{2^{(1+t)(n-1)}}-\sum_{t\ge 0}\frac{\xi_{t,t}(t)}{2^{t(n-1)}}.$$

In addition, the two expressions are equal.

Proof. The absolute convergence follows from taking $M=t$, $m_2=t$, $m_1=t-1$ in Lemma 3.5.10, as well as (3.28) and (3.63). Furthermore, the sum over $\mathbf{b}$ in the lemma equals

$$\sum_{\substack{b_2\in\mathbb{Z}\cap[0,2^{t+1})\\ \mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n}}\mathrm{e}\left(\frac{b_2f_2(\mathbf{x})}{2^{t+1}}\right)\sum_{\substack{b_1\in\mathbb{Z}\cap[0,2^{t+1})\\ 2\nmid\mathbf{b}}}\mathrm{e}(-b_1/2)\,\mathrm{e}\left(\frac{b_1f_1(\mathbf{x})}{2^{t+1}}\right).$$

The contribution of the even values of b_1 is the following (after writing $b_1=2c$),

$$\mathbf{1}_{2\nmid b_2}\sum_{c\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\left(\frac{cf_1(\mathbf{x})}{2^t}\right)=2^t\mathbf{1}_{2\nmid b_2}\mathbf{1}_{2^t\mid f_1(\mathbf{x})}$$

and the contribution of the odd values equals

$$-\mathrm{e}\left(\frac{f_1(\mathbf{x})}{2^{t+1}}\right)\sum_{c\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\left(\frac{cf_1(\mathbf{x})}{2^t}\right)=-\mathrm{e}\left(\frac{f_1(\mathbf{x})}{2^{t+1}}\right)2^t\mathbf{1}_{2^t\mid f_1(\mathbf{x})}$$

after writing $b_1=2c+1$. Recalling (3.6), we infer that the sum over $\mathbf{b}$ in the lemma is

$$2^t\sum_{\substack{b_2\in\mathbb{Z}\cap[0,2^{t+1})\\ \mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ 2^t\mid f_1(\mathbf{x})}}\mathrm{e}\left(\frac{b_2f_2(\mathbf{x})}{2^{t+1}}\right)\left(\mathbf{1}_{2\nmid b_2}-\mathrm{e}\left(\frac{f_1(\mathbf{x})2^{-t}}{2}\right)\right),$$

which is plainly

$$2^t\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ 2^t\mid f_1(\mathbf{x})}}c_{2^{t+1}}(f_2(\mathbf{x}))\right)-2^{1+2t}\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ 2^{t+1}\mid f_1(\mathbf{x}),2^{t+1}\mid f_2(\mathbf{x})}}1\right)$$
$$+2^{1+2t}\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+1})^n\\ v_2(f_1(\mathbf{x}))=t,2^{t+1}\mid f_2(\mathbf{x})}}1\right).$$

Using (3.7) to simplify the first sum over $\mathbf{x}$ shows that the left side of the equation in the current lemma is

$$\sum_{t\geq 0}\frac{1}{2^t}\frac{1}{2^{(t+1)n}}(2^{2+2t}\xi_{t,t+1}(t+1)-2^{2+2t}\xi_{t+1,t+1}(t+1)-2^{n+2t}\xi_{t,t}(t)),$$

which concludes the proof. □

Write $\lambda_t(M)$ for

$$\#\big\{\mathbf{x}\in\big(\mathbb{Z}\cap[0,2^M)\big)^n : v_2(f_1(\mathbf{x}))=t, 2^M \mid f_2(\mathbf{x}), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1 \,(\mathrm{mod}\ 4)\big\},$$

where for any integer n we write n_{odd} for $n\cdot 2^{-v_2(n)}$.

LEMMA 3.5.21. *Under the assumptions of Theorem 3.1.3 all series over t in the following two quantities converge absolutely:*

$$\sum_{t\geq 0}\frac{1}{2^t}\frac{1}{2^{n(t+2)}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{t+2}))^2\\ \gcd(b_1,b_2,2^{t+2})=1}} S_{\mathbf{b},2^{t+2}}\,\mathrm{e}(-b_1/4),$$

$$4\sum_{t\geq 0}\frac{\lambda_t(t+2)}{2^{(n-1)(t+2)}}-2\sum_{t\geq 0}\frac{(\xi_{t,t+1}(t+1)-\xi_{t+1,t+1}(t+1))}{2^{(n-1)(t+1)}}.$$

Furthermore, the two quantities are equal.

Proof. The first series and the second term in the second series can be proven to converge absolutely in the same way as in the proof of Lemma 3.5.20. To prove absolute convergence for the first term of the second series we note that we may bound $\lambda_t(t+2)\leq\xi_{t,t+2}(t+2)$ and hence by Lemma 3.5.10 we have $\lambda_t(t+2)\ll 2^{nt+2n-2t}$, which is sufficient.

Let us now proceed with the proof of the claimed equality. The sum over $\mathbf{b}$ is

$$\sum_{\substack{b_2\in\mathbb{Z}\cap[0,2^{t+2})\\ \mathbf{x}\in\mathbb{Z}\cap[0,2^{t+2})^n}}\mathrm{e}\left(\frac{b_2f_2(\mathbf{x})}{2^{t+2}}\right)\sum_{\substack{b_1\in\mathbb{Z}\cap[0,2^{t+2})\\ 2\nmid\mathbf{b}}}\mathrm{e}(-b_1/4)\,\mathrm{e}\left(\frac{b_1f_1(\mathbf{x})}{2^{t+2}}\right).$$

The new sum over b_1 can be written as follows (after writing $b_1=4y+j$),

$$\sum_{\substack{j\in\mathbb{Z}\cap[0,4)\\ 2\mid j\Rightarrow 2\nmid b_2}}\mathrm{e}(-j/4)\,\mathrm{e}\Big(\frac{jf_1(\mathbf{x})}{2^{t+2}}\Big)\sum_{y\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\Big(\frac{yf_1(\mathbf{x})}{2^t}\Big)$$

which is equal to

$$2^t \mathbf{1}_{2^t | f_1(\mathbf{x})} \sum_{\substack{j \in \mathbb{Z} \cap [0,4) \\ 2|j \Rightarrow 2 \nmid b_2}} \mathrm{e}(-j/4)\, \mathrm{e}\Big(\frac{j f_1(\mathbf{x})}{2^{t+2}}\Big).$$

A moment's thought allows to verify the following identity for any integer c:

$$\sum_{\substack{j \in \mathbb{Z} \cap [0,4) \\ 2|j \Rightarrow 2 \nmid b_2}} \mathrm{e}(jc/4) = 2(\mathbf{1}_{2 \nmid b_2} + e(c/4))\mathbf{1}_{2|c}.$$

Using this for $c = f_1(\mathbf{x})2^{-t} - 1$ provides us with the equality of the sum over b_1 with

$$2^{t+1} \mathbf{1}_{v_2(f_1(\mathbf{x}))=t} (\mathbf{1}_{2 \nmid b_2} + \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4)).$$

Hence the sum over $\mathbf{b}$ in the lemma is

$$2^{t+1} \sum_{\substack{b_2 \in \mathbb{Z} \cap [0, 2^{t+2}) \\ \mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n, v_2(f_1(\mathbf{x}))=t}} \mathrm{e}\Big(\frac{b_2 f_2(\mathbf{x})}{2^{t+2}}\Big)\Big(\mathbf{1}_{2 \nmid b_2} + \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4)\Big),$$

which is

$$2^{t+1} \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t}} c_{2^{t+2}}(f_2(\mathbf{x})) + 2^{3+2t} \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t, 2^{t+2} | f_2(\mathbf{x})}} \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4).$$

Furthermore we have

$$\sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t \\ 2^{t+2} | f_2(\mathbf{x})}} \mathrm{e}((f_1(\mathbf{x})2^{-t} - 1)/4) = \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t, 2^{t+2} | f_2(\mathbf{x}) \\ f_1(\mathbf{x})_{\mathrm{odd}} \equiv 1 \pmod 4}} 1 - \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t, 2^{t+2} | f_2(\mathbf{x}) \\ f_1(\mathbf{x})_{\mathrm{odd}} \equiv 3 \pmod 4}} 1,$$

and, since $v_2(f_1(\mathbf{x})) = t$ implies $f_1(\mathbf{x})_{\mathrm{odd}} = f_1(\mathbf{x})2^{-t}$, this can now be written as

$$2 \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t \\ 2^{t+2} | f_2(\mathbf{x}) \\ f_1(\mathbf{x})_{\mathrm{odd}} \equiv 1 \pmod 4}} 1 - \sum_{\substack{\mathbf{x} \in \mathbb{Z} \cap [0,2^{t+2})^n \\ v_2(f_1(\mathbf{x}))=t \\ 2^{t+2} | f_2(\mathbf{x})}} 1 = 2\lambda_t(t+2) - (\xi_{t,t+2}(t+2) - \xi_{t+1,t+2}(t+2)).$$

Hence, the sum over $\mathbf{b}$ in the lemma is

$$2^{t+1}\sum_{\substack{\mathbf{x}\in\mathbb{Z}\cap[0,2^{t+2})^n\\ v_2(f_1(\mathbf{x}))=t}} c_{2^{t+2}}(f_2(\mathbf{x}))+2^{3+2t}\Big(2\lambda_t(t+2)-(\xi_{t,t+2}(t+2)-\xi_{t+1,t+2}(t+2))\Big).$$

Utilising (3.7) to evaluate $c_{2^{t+2}}(f_2(\mathbf{x}))$ concludes the proof. □

The next lemma is the last one in the established line of similar results.

LEMMA 3.5.22. *Under the assumptions of Theorem 3.1.3 both series over t in the following expression converge absolutely:*

$$\sum_{t\geq 0}\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}+\frac{1}{4}\sum_{\substack{t\geq 0\\ \varrho\geq t+3}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ 2^{\varrho-t-2}|b_1,2\nmid b_2}} S_{\mathbf{b},2^\varrho}\,\mathrm{e}(-b_1 2^{t-\varrho}).$$

Furthermore, the limit

$$\lim_{M\to\infty}\frac{\#\left\{\mathbf{x}\in\left(\mathbb{Z}\cap[0,2^M)\right)^n : f_2(\mathbf{x})\equiv 0\left(\mathrm{mod}\ 2^M\right), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1\,(\mathrm{mod}\ 4)\right\}}{2^{M(n-1)}}$$

exists and is equal to the previous expression.

Proof. The proof of the absolute convergence is similar to that in the proof of Lemma 3.5.21, thus we shall next concentrate on showing the existence of the limit in the lemma. Writing $b_1=2^{\varrho-t-2}(4y+j)$ and using (3.7), we see that the sum over $\mathbf{b}$ becomes

$$\sum_{\mathbf{x}\in(\mathbb{Z}\cap[0,2^\varrho))^n} c_{2^\varrho}(f_2(\mathbf{x}))\sum_{j\in\mathbb{Z}\cap[0,4)}\mathrm{e}(-j/4)\,\mathrm{e}\Big(\frac{jf_1(\mathbf{x})}{2^{t+2}}\Big)\sum_{y\in\mathbb{Z}\cap[0,2^t)}\mathrm{e}\Big(\frac{yf_1(\mathbf{x})}{2^t}\Big),$$

which equals

$$2^{t+\varrho}\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^\varrho))^n\\ 2^t|f_1(\mathbf{x})}}\Big(\mathbf{1}_{2^\varrho|f_2(\mathbf{x})}-\frac{\mathbf{1}_{2^{\varrho-1}|f_2(\mathbf{x})}}{2}\Big)\sum_{j\in\mathbb{Z}\cap[0,4)}\mathrm{e}(-j/4)\,\mathrm{e}\Big(\frac{jf_1(\mathbf{x})}{2^{t+2}}\Big).$$

Noting that the sum over j equals 4 when $4\mid f_1(\mathbf{x})2^{-t}-1$ holds, and it otherwise vanishes, we obtain

$$2^{t+\varrho+2}\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^\varrho))^n\\ 2^t|f_1(\mathbf{x}),4|f_1(\mathbf{x})2^{-t}-1}}\Big(\mathbf{1}_{2^\varrho|f_2(\mathbf{x})}-\frac{\mathbf{1}_{2^{\varrho-1}|f_2(\mathbf{x})}}{2}\Big),$$

which can be written as

$$2^{t+\varrho+2}\Bigg(\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^{\varrho}))^n\\ v_2(f_1(\mathbf{x}))=t,2^{\varrho}\mid f_2(\mathbf{x})\\ f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1(\mathrm{mod}\ 4)}}1\Bigg)-2^{t+\varrho+1+n}\Bigg(\sum_{\substack{\mathbf{x}\in(\mathbb{Z}\cap[0,2^{\varrho-1}))^n\\ v_2(f_1(\mathbf{x}))=t,2^{\varrho-1}\mid f_2(\mathbf{x})\\ f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1(\mathrm{mod}\ 4)}}1\Bigg).$$

Therefore, whenever M is an integer with $M > t+3$, we have

$$\sum_{\substack{t\geq 0\\ t+3\leq\varrho\leq M}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})$$
$$=4\sum_{t\geq 0}\sum_{\varrho=t+3}^{M}\left(\frac{\lambda_t(\varrho)}{2^{\varrho(n-1)}}-\frac{\lambda_t(\varrho-1)}{2^{(\varrho-1)(n-1)}}\right).$$

The sum over ϱ is telescopic, thus we get

$$\sum_{\substack{t\geq 0\\ t+3\leq\varrho\leq M}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})=4\left(\frac{\lambda_t(M)}{2^{M(n-1)}}-\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}\right).$$

Using the bound (3.28) we obtain

$$\sum_{t\geq 0}\frac{1}{2^t}\sum_{\varrho>M}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}|S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})|\ll\sum_{t\geq 0}\frac{1}{2^t}\sum_{\varrho>M}\frac{1}{2^{\varrho n}}2^{\rho(n-3)}$$
$$\ll 2^{-M},$$

and therefore also

$$\sum_{\substack{t\geq 0\\ \varrho\geq t+3}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^{\varrho}))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}}S_{\mathbf{b},2^{\varrho}}\,\mathrm{e}(-b_1 2^{t-\varrho})-4\sum_{t\geq 0}\left(\frac{\lambda_t(M)}{2^{M(n-1)}}-\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}\right)$$

is $O(2^{-M})$. Taking $M\to\infty$ and noting

$$\sum_{t\geq 0}\frac{\lambda_t(M)}{2^{M(n-1)}}=\frac{\#\big\{\mathbf{x}\in\big(\mathbb{Z}\cap[0,2^M)\big)^n : 2^M\mid f_2(\mathbf{x}), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1\,(\mathrm{mod}\ 4)\big\}}{2^{M(n-1)}}$$

shows that the limit

$$\lim_{M\to\infty}\frac{\#\big\{\mathbf{x}\in\big(\mathbb{Z}\cap[0,2^M)\big)^n : 2^M\mid f_2(\mathbf{x}), f_1(\mathbf{x})_{\mathrm{odd}}\equiv 1\,(\mathrm{mod}\ 4)\big\}}{2^{M(n-1)}}$$

exists and equals

$$\sum_{t\geq 0}\frac{\lambda_t(t+2)}{2^{(t+2)(n-1)}}+\frac{1}{4}\sum_{\substack{t\geq 0\\ \varrho\geq t+3}}\frac{1}{2^t}\frac{1}{2^{\varrho n}}\sum_{\substack{\mathbf{b}\in(\mathbb{Z}\cap[0,2^\varrho))^2\\ 2^{\varrho-t-2}\mid b_1,2\nmid b_2}} S_{\mathbf{b},2^\varrho}\,\mathrm{e}(-b_1 2^{t-\varrho}).$$

This concludes the proof. □

Proof of Proposition 3.5.18. First, the contribution of those $\mathbf{t}$ with $f_2(\mathbf{t})$ being zero in the quantity inside the limit defining ℓ_2 in Proposition 3.5.18 can be dealt with in an identical manner as in our proof of Proposition 3.5.11.

Using Hilbert symbols (see, for example, [Ser73, Ch.III,Th.1]) one can obtain that for an integer m the curve $x_0^2+x_1^2=mx_2^2$ has a point over $\mathbb{Q}_2$ if and only if the odd part of m is $1\,(\mathrm{mod}\ 4)$. Hence the limit ℓ_2 in Proposition 3.5.18 coincides with the limit in Lemma 3.5.22, thus ℓ_2 exists. Finally, to prove $E_\phi(2)=\ell_2$, recall that $E_\phi(2)$ can be represented as the sum over t,ϱ in (3.56) and combine the equalities proved in Lemmas 3.5.19, 3.5.20, 3.5.21 and 3.5.22. □

3.5.4 Concluding steps

For every prime p we define

$$\tau_p:=\frac{(1-\frac{1}{p^{n-d}})}{(1-\frac{1}{p})}\lim_{N\to\infty}L_N$$

where L_N is equal

$$\frac{\#\big\{\mathbf{t}\in(\mathbb{Z}\cap[0,p^N))^n : p^N\mid f_2(\mathbf{t}), x_0^2+x_1^2=f_1(\mathbf{t})x_2^2 \text{ has a } \mathbb{Q}_p\text{-point}\big\}}{p^{N(n-1)}}.$$

This is well defined because for $p\equiv 1\,(\mathrm{mod}\ 4)$ the limit coincides with $\tau_{f_2}(p)$ which was introduced in (3.50), and for $p\not\equiv 1\,(\mathrm{mod}\ 4)$ the limit coincides with ℓ_p and ℓ_2 from Propositions 3.5.11 and 3.5.18 respectively. The definition of τ_p is motivated by the construction of the Tamagawa measure by Loughran in [Lou13, §5.7.2]. It is useful to recall that if one were counting $\mathbb{Q}$-rational points on the hypersurface $f_2=0$ then the corresponding Peyre constant would involve a p-adic density that is the

same as the number τ_p except for the condition on $\mathbb{Q}_p$-solubility, see [PT01, Cor.3.5]. For $s \in \mathbb{C}$ with $\Re(s) > 1$ let

$$L(s) := \sqrt{\zeta(s)} \tag{3.65}$$

denote the p-adic factor of $L(s)$ by $L_p(s)$ and write λ_p for $L_p(1)$, i.e.

$$\lambda_p := \left(1 - \frac{1}{p}\right)^{-1/2}.$$

Recall the definition of the real density $\mathfrak{J}$ in (3.33) and that d denotes the degrees of f_1 and f_2 (which are equal and even).

THEOREM 3.5.23. *Keep the assumptions of Theorem 3.1.3.*

1. *If ϕ has a smooth fibre with a $\mathbb{Q}$-point then the constant c_ϕ in Theorem 3.1.3 is strictly positive.*
2. *The infinite product $\prod_p \frac{\tau_p}{\lambda_p}$ taken over all non-archimedean places converges.*
3. *The constant c_ϕ in Theorem 3.1.3 satisfies*

$$c_\phi = \frac{\frac{1}{\sqrt{d}}\mathfrak{J}\prod_p \frac{\tau_p}{\lambda_p}}{\sqrt{\pi}}.$$

REMARK 3.5.24. Recalling that $\sqrt{\pi}$ is the value of the Euler Gamma function at $1/2$ and noting that

$$1 = \lim_{s \to 1_+} (s-1)^{1/2} L(s)$$

allows for a comparison of Theorem 3.5.23 with the case of [Lou13, Th. 5.15] that corresponds to

$$\rho_{\mathcal{B}}(X) = \frac{1}{2}.$$

Proof of Theorem 3.5.23. To prove *(1)* observe that due to (3.40), it suffices to show that if ϕ has a smooth fibre with a $\mathbb{Q}$-point then

$$\mathfrak{J} > 0 \text{ and } \mathbb{L}_\phi > 0.$$

For the former part, we point the reader to the definition of $\mathfrak{J}$ in (3.33). One should first notice that if $\mathcal{V} \subset [-1,1]^n$ is an area without zeroes of f_2, then the integral

$$\int_{\Gamma \in \mathbb{R}} \int_{\mathbf{t} \in \mathcal{V}} e(\Gamma f_2(\mathbf{t})) \mathrm{d}\mathbf{t} \mathrm{d}\Gamma$$

vanishes.

Let us write $\mathcal{A} := \{\mathbf{t} \in (-1,1)^n \mid f_1(\mathbf{t}) > 0\}$. Then the closure of $\mathcal{A}$ is the region of integration that appears in $\mathfrak{J}$. Since the boundary has measure zero, integrating over $\mathcal{A}$ gives the same result. Divide $\mathcal{A}$ up into sufficiently small boxes with sides parallel to the coordinate axes, not necessarily finite in number and not necessarily of equal sizes. Since we already know that the integral $\mathfrak{J}$ converges to a finite value, this value is equal to the possibly infinite sum of integrals over these boxes.

It is proved in [Bir62, §6], that if $\mathcal{B} \subset (-1,1)^n$ is a box with sides parallel to the coordinate axes and the hypersurface $f_2 = 0$ has a non-singular real point inside $\mathcal{B}$ then the corresponding integral

$$\int_{\Gamma\in\mathbb{R}} \int_{\mathbf{t}\in\mathcal{B}} \mathrm{e}(\Gamma f_2(\mathbf{t}))\mathrm{d}\mathbf{t}\mathrm{d}\Gamma$$

is positive. In our case, every real zero of f_2 is non-singular by assumption. Combined with the vanishing mentioned above, the integral over any box in the subdivision of $\mathcal{A}$ is non-negative, so we only need to prove the existence of one box containing a real zero of f_2.

Now, in *(1)* it is assumed that ϕ has a smooth fibre with a $\mathbb{Q}$-point. This means that there exists a point $\mathbf{t} \in \mathbb{P}^{n-1}(\mathbb{Q})$ such that for any representative $\mathbf{t}_0 \in \mathbb{Q}^n$ we have $f_2(\mathbf{t}_0) = 0$, and moreover the curve $x_0^2 + x_1^2 = f_1(\mathbf{t}_0)x_2^2$ is smooth and has a $\mathbb{Q}$-point, hence in particular an $\mathbb{R}$-point. Therefore we have $f_1(\mathbf{t}_0) > 0$. Choosing such $\mathbf{t}_0$ inside $(-1,1)^n$, we get the desired existence of $\mathbf{t}_0 \in \mathcal{A}$ satisfying $f_2(\mathbf{t}_0) = 0$. Subsequently we find a box $\mathcal{B} \subset \mathcal{A}$ with sides parallel to the coordinate axes containing $\mathbf{t}_0$. Therefore the integral over this particular box is positive, and in conclusion $\mathfrak{J}$ is positive.

To prove $\mathbb{L}_\phi > 0$, we invoke Lemma 3.5.9 to see that it is enough to show

$$\begin{aligned} &E_\phi(2) > 0, \text{ and} \\ &p \equiv 1 \,(\mathrm{mod}\ 4) \Rightarrow \tau_{f_2}(p) > 0, \text{ and} \\ &p \equiv 3 \,(\mathrm{mod}\ 4) \Rightarrow E_\phi(p) > 0. \end{aligned} \tag{3.66}$$

For this, choose a representative $\mathbf{t}_0$ in $\mathbb{Z}^n_{\mathrm{prim}}$ (rather than in $(-1,1)^n$ as in the previous paragraph) and note that for every prime p the point $\mathbf{t}_0$ can be viewed as a smooth $\mathbb{Q}_p$-point on the hypersurface $f_2 = 0$ and such that the curve $x_0^2 + x_1^2 = f_1(\mathbf{t}_0)x_2^2$ has a $\mathbb{Q}_p$-point. For $p \equiv 1 \,(\mathrm{mod}\ 4)$ this forces no condition on $f_1(\mathbf{t}_0)$, thus $\tau_{f_2}(p) > 0$ because, as mentioned

in [Bir62, §7], one can use Hensel's lemma to prove that if $f_2 = 0$ has a smooth $\mathbb{Q}_p$-point then the analogous p-adic density is strictly positive. If $p \equiv 3 \pmod 4$ or if $p = 2$ then the existence of such a $\mathbf{t}_0$ can be used with Hensel's lemma to prove that the quantities ℓ_2 and ℓ_p (defined in Propositions 3.5.11 and 3.5.18 respectively) are strictly positive. The equalities $E_\phi(p) = \ell_p/(1-1/p)$ and $E_\phi(2) = \ell_2$ (proved in Propositions 3.5.11 and 3.5.18) then show the validity of (3.66), which concludes the proof of *(1)*.

Let us now commence the proof of *(2)*. Denoting the limit in the definition of τ_p by ℓ_p we see

$$\begin{aligned}\lim_{t\to\infty}\prod_{p\le t}\frac{\tau_p}{\lambda_p} &= \lim_{t\to\infty}\prod_{p\le t}\frac{(1-\frac{1}{p^{n-d}})}{(1-\frac{1}{p})}\ell_p\Big(1-\frac{1}{p}\Big)^{1/2}\\ &= \frac{\ell_2 2^{1/2}}{\zeta(n-d)}\lim_{t\to\infty}\prod_{2\neq p\le t}\frac{\ell_p}{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}\left(\frac{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}{(1-\frac{\mathbf{1}_{p\equiv 1(\mathrm{mod}\ 4)}}{p})}\right)^{1/2}.\end{aligned}$$

We now let χ stand for the non-trivial Dirichlet character (mod 4) to obtain

$$\prod_{p\le t}\frac{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}{(1-\frac{\mathbf{1}_{p\equiv 1(\mathrm{mod}\ 4)}}{p})} = \left(\prod_{p\le t}\frac{1}{1-\frac{\chi(p)}{p}}\right)\prod_{\substack{p\le t\\ p\equiv 3(\mathrm{mod}\ 4)}}\Big(1-\frac{1}{p^2}\Big).$$

Applying the Leibniz formula for π, or in other words, that the Euler product for the Dirichlet series $L(\chi,s)$ of χ converges to $\pi/4$ for $s=1$, we get

$$\lim_{t\to\infty}\prod_{p\le t}\left(\frac{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}{(1-\frac{\mathbf{1}_{p\equiv 1(\mathrm{mod}\ 4)}}{p})}\right)^{1/2} = \frac{\pi^{1/2}}{2}\mathcal{C}_0,$$

where $\mathcal{C}_0$ was defined in equation (3.8).

We have so far shown the validity of

$$\lim_{t\to\infty}\prod_{p\le t}\frac{\tau_p}{\lambda_p} = \frac{\ell_2 2^{1/2}}{\zeta(n-d)}\left(\lim_{t\to\infty}\prod_{p\le t}\frac{\ell_p}{(1-\frac{\mathbf{1}_{p\equiv 3(\mathrm{mod}\ 4)}}{p})}\right)\frac{\pi^{1/2}}{2}\mathcal{C}_0.$$

It is clear that for $p \equiv 1 \pmod 4$ we have $\ell_p = \tau_{f_2}(p)$, and thus (3.53) leads to the absolute convergence of

$$\lim_{t\to\infty}\prod_{\substack{p\equiv 1(\mathrm{mod}\ 4)\\ p\le t}}\ell_p = \prod_{p\equiv 1(\mathrm{mod}\ 4)}\tau_{f_2}(p).$$

By Proposition 3.5.11 one gets

$$\prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ p\leq t}} \frac{\ell_p}{(1-\frac{1}{p})} = \prod_{\substack{p\equiv 3 (\mathrm{mod}\ 4)\\ p\leq t}} E_\phi(p).$$

It is now clear from Lemma 3.5.9 that the last product converges. Therefore the product $\prod_p \tau_p/\lambda_p$ is convergent, which proves *(2)*.

For the proof of *(3)* we note that the arguments at the end of the proof of *(2)* provided us with the equality

$$\prod_p \frac{\tau_p}{\lambda_p} = \frac{\ell_2 2^{1/2}}{\zeta(n-d)} \left(\prod_{p\equiv 1 (\mathrm{mod}\ 4)} \tau_{f_2}(p) \right) \left(\prod_{p\equiv 3 (\mathrm{mod}\ 4)} E_\phi(p) \right) \frac{\pi^{1/2}}{2} \mathcal{C}_0.$$

We have $E_\phi(2) = \ell_2$ due to Proposition 3.5.18. Recalling Lemma 3.5.9 we get

$$\prod_p \frac{\tau_p}{\lambda_p} = \frac{2^{1/2}}{\zeta(n-d)} \mathbb{L}_\phi \frac{\pi^{1/2}}{2} \mathcal{C}_0.$$

A comparison with (3.40) makes the proof of *(3)* immediately apparent. □

Let us remark that the arguments in the proof of Theorem 3.5.23 can be easily rearranged to show that $\prod_{p\leq t} \tau_p$ diverges. Therefore the numbers λ_p can be viewed as 'convergence factors'. We are very grateful to Daniel Loughran for suggesting this choice for λ_p, as well as for the L-function in (3.65).

In fact, the above proof of *(1)* shows a stronger statement. We thank Jean-Louis Colliot-Thélène for asking the question that prompted us to recognize this.

THEOREM 3.5.25. *If for every prime p there exists a smooth fibre with a $\mathbb{Q}_p$-point, and moreover there exists a smooth fibre with an $\mathbb{R}$-point, then c_ϕ is positive.*

Proof. We have seen in Lemma 3.5.9 that the product

$$\mathbb{L}_\phi = E_\phi(2) \prod_{p\equiv 1 (\mathrm{mod}\ 4)} \tau_{f_2}(p) \prod_{p\equiv 3 (\mathrm{mod}\ 4)} E_\phi(p)$$

converges absolutely. Hence its value is positive if the values of the individual factors are positive. In the proof of Theorem 3.5.23 we showed

that each of the factors in the product above is positive by starting with a $\mathbb{Q}$-point and considering it as a $\mathbb{Q}_p$-point for every p. However, every individual prime was then treated separately, so one may as well have started with $\mathbb{Q}_p$-points for every p which are not necessarily defined over $\mathbb{Q}$.

The same strategy was used to prove $\mathfrak{J} > 0$, and again here one might have started with an $\mathbb{R}$-point that is not necessarily also defined over $\mathbb{Q}$. □

Remark 3.5.26. Theorem 3.5.25 shows that the Hasse principle holds for the total space of smooth fibres. Since the main term in Theorem 3.1.3 only takes care of smooth fibres, the singular fibres lie outside the reach of the proof.

Chapter 4

Effective bounds for Brauer groups of Kummer surfaces over number fields

O dear Ophelia, I am ill at these numbers

Polonius, HAMLET, Scene 2.2, line 123

The following chapter was written together with Victoria Cantoral-Farfán, Yunqing Tang and Sho Tanimoto. It is published in the Journal of the London Mathematical Society as [CFTTV18].

The general idea of the proof of the main result arose from discussions between all authors during the Arizona Winter School in March 2015. Thereafter, the contributions of the author of this thesis largely lie in writing parts of §4.3 and the entirety of §4.5, as well as taking part in discussing and carefully checking every result in this chapter. In particular, the expertise of the author of this thesis does not lie in §4.2.

The numbering of results in this chapter only slightly differs from the published paper. Any result numbered `x` in the published paper, is numbered 4.`x` in this thesis.

4.1 Introduction

In 1971, Manin observed that failures of Hasse principle and weak approximation can be explained by Brauer–Manin obstructions for many

examples [Man71]. Let X be a smooth projective variety defined over a number field k. *The Brauer group of* X is defined as

$$\mathrm{Br}(X) := \mathrm{H}^2_{\text{ét}}(X, \mathbb{G}_m).$$

Then one can define an intermediate set using class field theory

$$X(k) \subset X(\mathbb{A}_k)^{\mathrm{Br}(X)} \subset X(\mathbb{A}_k),$$

where $\mathbb{A}_k$ is the adèlic ring associated to k. It is possible that $X(\mathbb{A}_k) \neq \emptyset$, but $X(\mathbb{A}_k)^{\mathrm{Br}(X)} = \emptyset$, whereby the Hasse principle fails for X. When this happens, we say that there is *a Brauer–Manin obstruction to the Hasse principle*. When $X(\mathbb{A}_k)^{\mathrm{Br}(X)} \neq X(\mathbb{A}_k)$, we say that there is *a Brauer–Manin obstruction to weak approximation*. There is a large body of work on Brauer–Manin obstructions to the Hasse principle and weak approximation (see, e.g., the work by Manin [Man86], or any of the following [BSD75], [CTCS80], [CTSSD87], [CTKS87], [SD93], [SD99], [KT04], [Bri06], [BBFL07], [KT08], [Log08], [VA08], [LvL09], [EJ10], [HVAV11], [ISZ11], [EJ12b], [HVA13], [CTS13], [MSTVA17], [SZ14], [IS15], [Wit16]) and it is an open question if for K3 surfaces, Brauer–Manin obstructions suffice to explain failures of Hasse principle and weak approximation, i.e., $X(k)$ is dense in $X(\mathbb{A}_k)^{\mathrm{Br}(X)}$ (see [HS16] for some evidence supporting this conjecture.)

The main question discussed in this paper is of computational nature: how can one compute $\mathrm{Br}(X)$ explicitly? It is shown by Skorobogatov and Zarhin in [SZ08] that $\mathrm{Br}(X)/\mathrm{Br}(k)$ is finite for any K3 surface X defined over a number field k, but they did not provide any effective bound for this group. Such an effective algorithm is obtained for degree 2 K3 surfaces in [HKT13] using explicit constructions of moduli spaces of degree 2 K3 surfaces and principally polarized abelian varieties. In this paper, we provide an effective algorithm to compute a bound for the order of $\mathrm{Br}(X)/\mathrm{Br}(k)$ when X is the Kummer surface associated to the Jacobian of a curve of genus 2:

Theorem 4.1.1. *There is an effective algorithm that takes as input an equation of a smooth projective curve C of genus 2 defined over a number field k, and outputs an effective bound for the order of $\mathrm{Br}(X)/\mathrm{Br}(k)$ where X is the Kummer surface associated to the Jacobian $\mathrm{Jac}(C)$ of the curve C.*

We obtain the following corollary as a consequence of results in [KT11] and [PTvL15]:

Corollary 4.1.2. *Given a smooth projective curve C of genus 2 defined over a number field k, there is an effective description of the set*

$$X(\mathbb{A}_k)^{\mathrm{Br}(X)}$$

where X is the Kummer surface associated to the Jacobian $\mathrm{Jac}(C)$ *of the curve C.*

Note that given a curve C of genus 2, the surface $Y = \mathrm{Jac}(C)/\{\pm 1\}$ can be realized as a quartic surface in $\mathbb{P}^3$ (see [FS97, §2]) and the Kummer surface X associated to $\mathrm{Jac}(C)$ is the minimal resolution of Y, so one can find defining equations for X explicitly.

The quartic surface Y has sixteen nodes, and by considering the projection from one of these nodes, we may realize Y as a double cover of the plane. Thus X can be realized as a degree 2 K3 surface and our Theorem 4.1.1 follows from [HKT13]. It is remarked in [HKT13] that using the algebraic correspondence between X and $\mathrm{Jac}(C)$ it is possible to make [HKT13] into an actual algorithm for Kummer surfaces. However we take a different approach from [HKT13], and instead of using the Kuga–Satake construction we use a result of [SZ12] reducing our problem to the case of abelian surfaces. In particular, our algorithm provides a large, but explicit bound for the Brauer group of X. (See the example we discuss in §4.6.)

The method in this paper combines many results from the literature. The first key observation is that the Brauer group $\mathrm{Br}(X)$ admits the following stratification:

Definition 4.1.3. Let $\overline{X}$ denote $X \times_k \operatorname{Spec} \overline{k}$ where $\overline{k}$ is a given separable closure of k. Then we write

$$\mathrm{Br}_0(X) = \operatorname{im}\left(\mathrm{Br}(k) \to \mathrm{Br}(X)\right) \text{ and } \mathrm{Br}_1(X) = \ker\left(\mathrm{Br}(X) \to \mathrm{Br}(\overline{X})\right).$$

Elements in $\mathrm{Br}_1(X)$ are called *algebraic elements*; those in the complement $\mathrm{Br}(X) \setminus \mathrm{Br}_1(X)$ are called *transcendental elements*.

Thus to obtain an effective bound for $\mathrm{Br}(X)/\mathrm{Br}_0(X)$, it suffices to study $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ and $\mathrm{Br}(X)/\mathrm{Br}_1(X)$. The group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ is well-studied, and it admits the following isomorphism:

$$\mathrm{Br}_1(X)/\mathrm{Br}_0(X) \cong \mathrm{H}^1(k, \mathrm{Pic}(\overline{X})).$$

Note that for a K3 surface X, we have an isomorphism $\mathrm{Pic}(X) = \mathrm{NS}(X)$. Thus as soon as we compute $\mathrm{NS}(\overline{X})$ as a Galois module, we are able to

compute $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$. An algorithm to compute $\mathrm{NS}(\overline{X})$ is obtained in [PTvL15], but we consider another algorithm which is based on [Cha14].

To study $\mathrm{Br}(X)/\mathrm{Br}_1(X)$, we use effective versions of Faltings' theorem and combine them with techniques in [SZ08] and [HKT13]. Namely, we have an injection

$$\mathrm{Br}(X)/\mathrm{Br}_1(X) \hookrightarrow \mathrm{Br}(\overline{X})^{\Gamma}$$

where Γ is the absolute Galois group of k. As a consequence of [SZ12], we have an isomorphism of Galois modules

$$\mathrm{Br}(\overline{X}) = \mathrm{Br}(\overline{A}),$$

where $A = \mathrm{Jac}(C)$ is the Jacobian of C. Thus it suffice to bound the size of $\mathrm{Br}(\overline{A})^{\Gamma}$. To bound the cardinal of this group, we consider the following exact sequence as in [SZ08]:

$$\begin{aligned} 0 \to \left(\mathrm{NS}(\overline{A})/\ell^n\right)^{\Gamma} \xrightarrow{f_n} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^{\Gamma} \to \mathrm{Br}(\overline{A})^{\Gamma}_{\ell^n} \to \\ \to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \xrightarrow{g_n} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})), \end{aligned}$$

where ℓ is any prime and $\mathrm{Br}(\overline{A})_{\ell^n}$ is the ℓ^n-torsion part of the Brauer group of $\overline{A}$. Using effective versions of Faltings' theorem, we bound the cokernel of f_n and the kernel of g_n independently of n.

We emphasize that our algorithm is practical for any genus 2 curve whose Jacobian has Néron–Severi rank 1, i.e., we can actually implement and compute a bound for such a curve. For example, consider the following hyperelliptic curve of genus 2 defined over $\mathbb{Q}$:

$$C : y^2 = x^6 + x^3 + x + 1.$$

Let $A = \mathrm{Jac}(C)$ and let $X = \mathrm{Kum}(A)$ be the Kummer surface associated to A. The geometric Néron–Severi rank of A is 1. Combining our algorithm with the work of [Die02] and [Sko17], we show that

$$|\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q})| < 2^{10} \cdot 10^{805050}.$$

Our effective bound explicitly depends on the Faltings height of the Jacobian of C, so it does not provide any uniform bound as conjectured in [TVA16], [AVA18], and [VA17]. However, it is an open question whether the Faltings height in Theorem 4.2.13 is needed. If there is a uniform bound for Theorem 4.2.13 which does not depend on the Faltings height,

then our proof provides a uniform bound for the Brauer group. Such a uniform bound is obtained for elliptic curves in [VAV17].

Even though our method can handle any curve of genus 2 defined over a number field k, we will focus on the case of curves whose Jacobians have the geometric Picard rank 1. In other cases (non-simple cases), we can provide better bounds but we will not discuss them in this paper. The reader who is interested in these cases is encouraged to refer to the arXiv version of this paper. ([CFTTV16])

The paper is organized as follows. In §4.2 we review effective versions of Faltings' theorem and consequences that will be useful for our purposes. In §4.3 we review methods from the literature in order to compute the Néron–Severi lattice as a Galois module. §4.4 proves our bounds for the size of the transcendental part. §4.5 is devoted to Magma computations in the lowest rank case and §4.6 explores an example.

Acknowledgments

The authors would like to thank Martin Bright, Edgar Costa, Éric Gaudron, Brendan Hassett, David Holmes, Hendrik Lenstra, Ronald van Luijk, Chloe Martindale, Rachel Newton, Fabien Pazuki, Dan Petersen, Padmavathi Srinivasan and Yuri Tschinkel for useful discussions and comments. In particular they would like to thank Rachel Newton for her comments on the early draft of this paper. They also would like to thank Andreas-Stephan Elsenhans for providing them with the Magma code of the algorithm in [EJ12a]. They would like to thank Alexei Skorobogatov for pointing out a mistake in the earlier version of this paper. They would also like to thank the anonymous referees for suggestions to improve the exposition and the bound in §4.6 using [Die02] and [Sko17].

This paper began as a project in Arizona Winter School 2015 "Arithmetic and Higher-dimensional varieties". The authors would like to thank AWS for their hospitality and travel support. Finally the authors are grateful to Tony Várilly-Alvarado for suggesting this project, many conversations where he patiently answered our questions, and for his constant encouragement. This project and AWS have been supported by NSF grant DMS-1161523. Cantoral-Farfán was supported by the Conacyt fellowship. Tang was a member at the Institute for Advanced Study, supported by NSF grant DMS-1128155 to IAS. Tanimoto is partially supported by Lars Hesselholt's Niels Bohr professorship and MEXT Japan, Leading Initiative for Excellent Young Researchers (LEADER).

4.2 Effective version of Faltings' theorem

One important input of our main theorem is an effective version of Faltings' isogeny theorem. Such a theorem was first proved by Masser and Wüstholz in [MW95] and the computation of the constants involved was made explicit by Bost [Bos96] and Pazuki [Paz12]. The work of Gaudron and Rémond [GR14] gives a sharper bound. Although the general results are valid for any abelian variety over a number field, we will only focus on abelian surfaces.

The main result of this section is in §4.2.4. The reader may skip §4.2.2 and §4.2.3 on a first reading and refer to them later for the proof of the main result. We use the idea of Masser and Wüstholz to reduce the effective Faltings theorem to bound the minimal isogeny degree between certain abelian varieties and to bound the volume of the $\mathbb{Z}$-lattice of the endomorphism ring of the given abelian surface. These two things are bounded by a constant only depending on the Faltings height and the degree of the field of definition using the idea of Gaudron and Rémond. To compute a bound of Faltings height, we use a formula due to Pazuki and Magma.

Let A be an abelian surface defined over a number field k. Without further indication, A will be the Jacobian of some hyperelliptic curve C, principally polarized by the theta divisor, and we use L to denote the line bundle on A corresponding to the theta divisor. Throughout this section, when we say there is an isogeny between abelian varieties A_1 and A_2 of degree at most D, it means that there exist isogenies $A_1 \to A_2$ and $A_2 \to A_1$ both whose degrees are at most D.

4.2.1 Faltings height

The bounds in the effective Faltings theorems discussed in our paper depend on the stable Faltings height of the given abelian surface. We denote the stable Faltings height of A by $h(A)$ (with the normalization as in the original work of Faltings [Fal86]). In order to obtain a bound without Faltings height, we now describe how to obtain an upper bound of $h(\mathrm{Jac}(C))$ using the work of Pazuki [Paz14] and Magma.

Assume that the hyperelliptic curve C is given by $y^2 + G(x)y = F(x)$,

where $G(x), F(x)$ are polynomials in x of degrees at most 3 and 6 respectively.

PROPOSITION 4.2.1. *Given a complex embedding σ of k, we use τ_σ to denote a period matrix of the base change $C_{\mathbb{C}}$ via σ. Let Δ be $2^{-12}\,\mathrm{Disc}_6(4F+G^2)$, where Disc_6 means taking the discriminant of a degree 6 polynomial. Then $h(\mathrm{Jac}(C))$ is bounded from above by*

$$-\log(2\pi^2)+\frac{1}{[k:\mathbb{Q}]}\Big(\frac{1}{10}\log(\Delta)-\sum_{\sigma}\log(2^{-1/5}|J_{10}(\tau_\sigma)|^{1/10}\det(\Im\tau_\sigma)^{1/2})\Big),$$

where σ runs through all complex embeddings of k.

Notice that the functions *AnalyticJacobian* and *Theta* in MAGMA compute period matrices τ_σ of $\mathrm{Jac}(C)$ and $J_{10}(\tau_\sigma)$, which is the square of the product of all even theta functions.

Proof. Let k' be a finite extension of k such that after base change to k', the variety $\mathrm{Jac}(C)_{k'}$ has semistable reduction everywhere. For example, k' can be taken to be the field of definition of all 12-torsion points. Then the stable Faltings height of $\mathrm{Jac}(C)$ is given by the Faltings height of $\mathrm{Jac}(C)$ over k'.

The inequality in the proposition follows from Pazuki's formula [Paz14, Thm. 2.4] once we bound the non-archimedean local term

$$\frac{1}{d}\sum_{v|\Delta_{min}} d_v f_v \log N_{k'/\mathbb{Q}}(v),$$

where $d=[k':\mathbb{Q}]$, $d_v=[k'_v:\mathbb{Q}_p]$ if $v|p$, Δ_{min} is the minimal discriminant of C over k', and $10f_v\le \mathrm{ord}_v(\Delta_{min})$. By definition of minimal discriminant, we have $\Delta_{min}|\Delta$ and hence the local term is bounded by $\frac{1}{d}\sum_{v|\Delta} d_v\frac{\mathrm{ord}_v(\Delta)}{10}\log N_{k'/\mathbb{Q}}(v)=\frac{\log(\Delta)}{10[k:\mathbb{Q}]}$. □

REMARK 4.2.2. Following [Kau99, Sec. 4,5], one can compute the exact local contribution in Pazuki's formula at $v\nmid 2$ by studying the roots of $F(x)$ assuming $G=0$.

4.2.2 Preliminary results

In this subsection, we recall some key facts about Euclidean lattices and results in transcendence theory that will be used to obtain an effective

version of Faltings' theorem.

Let B be the abelian variety $A \times A$ principally polarized by $pr_1^*L \otimes pr_2^*L$ and B' an abelian variety over k isogenous to B over k. Let $\widehat{B}'$ be the dual abelian variety of B' and let $Z(B')$ be the principally polarizable abelian variety $(B')^4 \times (\widehat{B}')^4$. We fix a principal polarization on $Z(B')$.

Since A (resp. B and $Z(B')$) is principally polarized, one defines the Rosati involution $(-)^\dagger$ on $\mathrm{End}_k(A)$ (resp. going from $\mathrm{Hom}_k(B, Z(B'))$ to $\mathrm{Hom}_k(Z(B'), B)$). The quadratic form $\mathrm{Tr}(\varphi\varphi^\dagger)$ defines a norm on $\mathrm{End}_k(A)$ (resp. $\mathrm{Hom}_k(B, Z(B'))$).[1] We use $v(A)$ to denote $\mathrm{vol}(\mathrm{End}_k(A))$ with respect to this norm. Let k_1 be a Galois extension of k. We denote by Λ (resp. Λ', Λ'_{k_1}) the smallest real number which bounds from above the norms of all elements in some $\mathbb{Z}$-basis of some sub-lattice (of finite index) of $\mathrm{End}_k(A)$ (resp. $\mathrm{Hom}_k(B, Z(B'))$, $\mathrm{Hom}_{k_1}(B, Z(B'))$)[2].

By definition, $v(A) \leq \Lambda^r$, where r is the $\mathbb{Z}$-rank of $\mathrm{End}_k(A)$. Moreover, Λ'_{k_1} is also the smallest real number which bounds from above the norms of all elements in some $\mathbb{Z}$-basis of $\mathrm{Hom}_{k_1}(A, Z(B'))$.

LEMMA 4.2.3 ([GR14, Lem. 3.3]). *We have* $\Lambda' \leq [k_1 : k]\Lambda'_{k_1}$.

The following three results are consequences of Faltings' isogeny formula and Bost's lower bound for Faltings heights.

LEMMA 4.2.4 (Faltings). *Let* $\phi : A_1 \to A_2$ *be an isogeny between abelian varieties. Then*

$$h(A_1) - \frac{1}{2}\log\deg(\phi) \leq h(A_2) \leq h(A_1) + \frac{1}{2}\log\deg(\phi).$$

LEMMA 4.2.5 (Bost). *For any abelian variety* A_1*, one has*

$$h(A_1) \geq -\tfrac{3}{2}\dim A_1.$$

LEMMA 4.2.6 (See for example [GR14, p. 2096]). *Let* H *be a sub abelian variety of a principally polarized abelian variety* A_1 *and* $\deg H$ *the degree of* H *with respect to the polarization line bundle on* A_1*. Then we have*

$$h(H) \leq h(A_1) + \log\deg H + \frac{3}{2}(\dim A_1 - \dim H).$$

[1] This quadratic form is positive definite by [Mum70, p. 192] and [GR14, Prop. 2.5].

[2] This means that if r is the rank of $\mathrm{End}_k(A)$, then there exists a free family $w_1, \ldots, w_r \in \mathrm{End}_k(A)$ such that the norm of w_i is no greater than Λ.

The following result is a direct consequence of the Theorem of Periods by Gaudron and Rémond. See for example [GR14, p. 2095–2096].

LEMMA 4.2.7 (Theorem of Periods). *Let H be a polarized abelian variety over k_1. Fix an embedding of k_1 into $\mathbb{C}$ and let Ω_H be the period lattice of $H(\mathbb{C})$ endowed with the norm $||\cdot||$ given by the real part of the Riemann form of the polarization. Assume that $\omega \in \Omega_H$ is not contained in the period lattice of any proper sub abelian variety of H. Then we have*

$$(\deg H)^{1/\dim H} \leq 50[k_1 : \mathbb{Q}]h^{2\dim H+6}\max(1, h(H), \log\deg H)||\omega||^2.$$

Proof. Gaudron and Rémond's Theorem of Periods implies that the same inequality holds by replacing $||\omega||^2$ by δ^2, where δ is the supremum among all proper sub abelian varieties H' of H of the minimum distance from $\omega \in \Omega_H \backslash \Omega'_H$ to the tangent space of H'. By our assumption on ω, one has $\delta \leq ||\omega||$. □

The following lemma is a direct consequence of Autissier's Matrix Lemma and it will be used to bound the norm of elements in period lattices.

LEMMA 4.2.8 (Autissier). *Let A_1 be a principally polarized abelian variety over k_1 and for any embedding $\sigma : k_1 \to \mathbb{C}$, let Ω_σ be the period lattice of $A_{1,\sigma}(\mathbb{C})$. We denote by Λ_σ the smallest real number which bounds the norms of all elements in some $\mathbb{Z}$-basis of some sub-lattice (of finite index) of Ω_σ. Then for any $\epsilon \in (0, 1)$*

$$\sum_\sigma \Lambda_\sigma^2 \leq \frac{6[k_1 : \mathbb{Q}](2\dim A_1)^2}{(1-\epsilon)\pi}\left(h(A_1) + \frac{\dim A_1}{2}\log\left(\frac{2\pi^2}{\epsilon}\right)\right).$$

Proof. This follows from [Aut13, Cor. 1.4] and [GR14, Cor. 3.6]. See also the proof of [GR14, Lem. 8.4]. □

LEMMA 4.2.9 ([Sil92, Thm. 4.1, 4.2, Cor. 3.3]). *Given abelian varieties A_1, A_2 of dimension g, g' defined over k, let K be the smallest field where all the $\overline{k}$-endomorphisms of $A_1 \times A_2$ are defined. Then we have*

$$[K : k] \leq 4(9g)^{2g}(9g')^{2g'}.$$

The following elementary lemma is useful.

LEMMA 4.2.10 ([GR14, Lem. 8.5]). *Let $u \geq e^{1/2}$ and $v \geq 0$ be real numbers. Assume that $x > 0$ and $x \leq u(v + \log x)$. Then $x \leq 2u(\log u + v)$.*

4.2.3 The bound of isogeny degrees

This subsection includes some upper bounds of the minimal isogeny degree between B and any B' over k isogenous to B. Here we will obtain an upper bound depending on $h(B')$ and in the proof of main theorem in next subsection, we will use the properties of the Faltings height to obtain a bound only depending on $h(A)$ and $[k:\mathbb{Q}]$. This upper bound is a key input to obtain our effective Faltings theorem.

An explicit bound of minimal isogeny degrees is given for general abelian varieties in [GR14, Thm. 1.4] so readers may use their bound and Lemma 4.2.14 later to finish the proof of Theorem 4.2.13 when $\mathrm{End}_k(A) = \mathbb{Z}$. However, we give a proof here since the same technique is used to bound Λ, which in turn will be used to deduce the effective Faltings theorem from the upper bound of minimal isogeny degree when $\mathrm{End}_k(A) \neq \mathbb{Z}$.

PROPOSITION 4.2.11. *There exists an isogeny $B' \to B$ over k of degree at most $2^{48}(\Lambda')^{16}\Lambda^{16r}$, where Λ, Λ' are defined in §4.2.2 and r is the $\mathbb{Z}$-rank of* $\mathrm{End}_k(A)$.

Proof. This follows from [GR14, Prop. 6.2] by noticing that the $\widehat{W_i}$ term there is not needed since A is principally polarized and by the fact that $v(A) \leq \Lambda^r$. □

LEMMA 4.2.12. *Let m_A and $m_{A,B'}$ denote* $\max(1, h(A))$ *and respectively* $\max(1, h(A), h(B'))$. *We have*

$$\Lambda \leq \begin{cases} 2 & \text{if } \bar{r} = 1, \\ 4^5 \cdot 9^8 \Big[5.04 \cdot 10^{24} [k:\mathbb{Q}] m_A & \\ \quad \cdot \big(\frac{5}{4} m_A + \log[k:\mathbb{Q}] + \log m_A + 60 \big) \Big]^{8/\bar{r}} & \text{if } \bar{r} = 2 \text{ or } 4. \end{cases}$$

and

$$\Lambda_{B,B'} \leq 4^{11} \cdot 9^{12} \Big[(4.4 \cdot 10^{46} [k:\mathbb{Q}] m_{A,B'} \\ \big(9 m_{A,B'} + 8 \log m_{A,B'} + 8 \log[k:\mathbb{Q}] + 920 \big) \Big]^{16/\bar{r}}.$$

Proof. Recall that $\bar{r}$ denotes the $\mathbb{Z}$-rank of $\mathrm{End}_{\bar{k}}(A)$. To deduce the bound of Λ, we first study the case $\bar{r} = 1$. In this case, $\mathrm{End}_{\bar{k}}(A) = \mathbb{Z}$ and by definition the norm of the identity map is $\sqrt{\mathrm{Tr}(\mathrm{id})} = \sqrt{4} = 2$. In other words, $\Lambda = 2$.

We postpone the discussion of Λ for $\bar{r} = 2, 4$, since it is a simplified version of the following discussion on the bound of Λ'. The estimate of Λ' is essentially [GR14, Lem. 9.1]. We modify its proof here to obtain a sharper bound for this special case.

Let k_1 be the field where all the $\overline{k}$-endomorphisms of $A \times B'$ are defined. Then by Lemma 4.2.9, we have $[k_1 : k] \leq 4 \cdot 18^4 \cdot 36^8 = 4^{11} \cdot 9^{12}$. For any complex embedding $\sigma : k_1 \to \mathbb{C}$, we may view A and $Z(B')$ as abelian varieties over $\mathbb{C}$ and let $\Omega_{A,\sigma}$ and $\Omega_{Z(B'),\sigma}$ be the period lattices. The principal polarization induces a metric on $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$). More precisely, the polarization line bundle gives rise to the Riemann form (a Hermitian form) on the tangent space of A (resp. $Z(B)$) and its real part defines a norm on the real tangent space and hence on $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$). We use $\Lambda(\Omega_{A,\sigma})$ (resp. $\Lambda(\Omega_{Z(B'),\sigma})$) to denote the smallest real number which bounds from above the norms of all elements in some $\mathbb{Z}$-basis of some sublattice (of finite index) of $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$).

Let $\omega_1, \ldots, \omega_4$ (resp. $\chi_1, \ldots, \chi_{64}$) be a free family in $\Omega_{A,\sigma}$ (resp. $\Omega_{Z(B'),\sigma}$) such that $||\omega_i|| \leq \Lambda(\Omega_{A,\sigma})$ (resp.$||\chi_i|| \leq \Lambda(\Omega_{Z(B'),\sigma})$) hold. Let ω be $(\omega_1, \chi_1, \ldots, \chi_{64}) \in \Omega_{A,\sigma} \oplus (\Omega_{Z(B'),\sigma})^{64}$ and let H be the smallest abelian subvariety of $A \times (Z(B'))^{64}$ whose Lie algebra (over $\mathbb{C}$) contains ω. Since $\chi_1, \ldots, \chi_{64}$ generate a sublattice of finite index of $\Omega_{Z(B'),\sigma}$, then for any $\chi \in \Omega_{Z(B'),\sigma}$, there exist $\ell, m_1, \ldots, m_{64}$ such that $\ell\chi + \sum m_i\chi_i = 0$ and hence H satisfies the assumption of [GR14, Prop. 7.1]. Therefore

$$\Lambda'_{k_1} \leq (\deg H)^2.$$

Let $h = \dim H$. By [GR14, Lem. 8.1], we have $2 \leq h \leq 8/\bar{r} \leq 8$ and by Lemma 4.2.7,

$$(\deg H)^{1/h} \leq 50[k_1\mathbb{Q}]h^{2h+6} \max(1, h(H), \log \deg H)||\omega||^2.$$

Now we bound $||\omega||$. Notice that by definition, we have

$$||\omega||^2 = ||\omega_1||^2 + \sum_i ||\chi_i||^2 \leq \Lambda(\Omega_{A,\sigma})^2 + 64\Lambda(\Omega_{Z(B'),\sigma})^2.$$

From now on, we fix a σ such that $\Lambda(\Omega_{A,\sigma})^2 + 64\Lambda(\Omega_{Z(B'),\sigma})^2$ is the smallest.

Then by Lemma 4.2.8, we have that, for any $\epsilon \in (0, 1)$,

$$||\omega||^2 \leq \frac{6}{(1-\epsilon)\pi}\left(16h(A) + 8^7 h(B') + (16 + 16^4)\log\left(\frac{2\pi^2}{\epsilon}\right)\right).$$

By taking $\epsilon = \frac{1}{40}$, we have $||\omega||^2 \leq 5 \times 10^6 \max(1, h(A), h(B'))$. Combining the above inequalities, we have the bound

$$(\deg H)^{\bar{r}/8} \leq 1.85 \times 10^{28}[k_1 : \mathbb{Q}] \max(1, h(A), h(B')) \cdot \left(9 \max(1, h(A), h(B')) + \log \deg H + 48\right),$$

where we use Lemma 4.2.6 to obtain

$$h_F(H) \leq 9 \max(1, h(A), h(B')) + \log \deg H + 48.$$

Then by Lemma 4.2.10, we have

$$\deg H \leq \left[3.7 \cdot 10^{28}[k_1 : \mathbb{Q}] m_{A,B'} \cdot \left(9m_{A,B'} + 48 + \frac{8}{\bar{r}} \log\left(1.85 \cdot 10^{28}[k_1 : \mathbb{Q}] \frac{8m_{A,B'}}{\bar{r}}\right)\right)\right]^{8/\bar{r}}.$$

Then we have (by Lemma 4.2.3) that Λ' can be bounded from above by

$$[k_1 : k]\Lambda'_{k_1} \leq [k_1 : k](\deg H)^2$$

and subsequently by

$$[k_1 : k]\left[3.7 \cdot 10^{28}[k_1 : \mathbb{Q}] m_{A,B'} \cdot \left(9m_{A,B'} + 48 + \frac{8}{\bar{r}} \log\left(1.85 \cdot 10^{28}[k_1 : \mathbb{Q}] \frac{8m_{A,B'}}{\bar{r}}\right)\right)\right]^{16/\bar{r}}$$
$$\leq 4^{11} \cdot 9^{12}\left[4.4 \cdot 10^{46}[k : \mathbb{Q}] m_{A,B'} \cdot \left(9m_{A,B'} + 8 \log m_{A,B'} + 8 \log[k : \mathbb{Q}] + 920\right)\right]^{16/\bar{r}}.$$

Now we assume that $\bar{r} = 2$ or 4. In this case we cannot compute Λ so we apply the same strategy as for the bound on Λ'. The proof is practically identical, but the bounds are different. In this case we bound the degree $[k_1 : k] \leq 4 \cdot 18^8$ and there exists an abelian subvariety H of $A \times A^4$ over k_1 such that the bounds

$$\Lambda \leq [k_1 : k](\deg H)^2$$

and

$$\deg H \leq \left[100 \cdot 4^{19} \cdot 9^8 \cdot 1063 \cdot [k : \mathbb{Q}] m_A \cdot (5m_A + 4 \log[k : \mathbb{Q}] + 4 \log m_A + 240)\right]^{8/\bar{r}}$$

are satisfied. Combining these two inequalities together, we obtain the bound for Λ. $\square$

4.2.4 Effective Faltings' theorem in the geometrically simple case

We assume that A is geometrically simple. Equivalently, A is not isogenous to a product of two elliptic curves over $\bar{k}$. Let Γ be its absolute Galois group. For a positive integer m, let A_m be the $\mathbb{Z}[\Gamma]$-module of m-torsion points of $A(\bar{k})$.

THEOREM 4.2.13. *For any integer m, let M_m be the smallest positive integer such that the cokernel of the map $\mathrm{End}_k(A) \to \mathrm{End}_\Gamma(A_m)$ is killed by M_m.*[3] *There exists an upper bound $\widetilde{M}$ for M_m depending on $h(A)$ and $[k:\mathbb{Q}]$ which is independent of m. Explicitly, when $\bar{r}=1$, then $\widetilde{M}$ equals*

$$2^{4664} c_1^{16} c_2(k)^{256} \left(2h(A) + \tfrac{8}{17}\log[k:\mathbb{Q}] + 8\log c_1 + 128\log c_2(k) + 1503\right)^{512},$$

and when $\bar{r}=2$ or 4,

$$\widetilde{M} = (r/4)^{r/2} 2^{48} \cdot c_1^{16} c_2(k)^{256} c_8(A,k)^{17r} \cdot \Big(16\log c_1 + \frac{256}{\bar{r}}\log c_2(k) + 16r\log c_8(A,k) + 4h(A) + \tfrac{16}{17}\log[k:\mathbb{Q}] + 1400\Big)^{512/\bar{r}}.$$

Here r (resp. $\bar{r}$) is the $\mathbb{Z}$-rank of $\mathrm{End}_k(A)$ (resp. $\mathrm{End}_{\bar{k}}(A)$). We have that $r, \bar{r} \in \{1,2,4\}$ and $r \le \bar{r}$.

The constants c_1 and c_2 are $c_1 = 4^{11}\cdot 9^{12}$ and $c_2(k) = 7.5\cdot 10^{47}[k:\mathbb{Q}]$, and $c_8(A,k)$ is

$$4^5 \cdot 9^8 \left(5.04\cdot 10^{24}[k:\mathbb{Q}] m_A \left(\tfrac{5}{4} m_A + \log[k:\mathbb{Q}] + \log m_A + 60\right)\right)^{8/\bar{r}},$$

where m_A is $\max(1, h(A))$.

We denote by $b(B)$ the smallest integer such that for any abelian variety B' defined over k, if B' is isogenous to B over k, then there exists an isogeny $\phi : B' \to B$ over k of degree at most $b(B)$.

LEMMA 4.2.14. *With notation as above, $M_m \le (r/4)^{r/2}\Lambda^r b(B)$.*

[3] Such M_m exists since $\mathrm{End}_\Gamma(A_m)$ is a finite group.

Proof. By [MW95, Lem. 3.2], one bounds M_m by $i(A)b(B)$, where $i(A)$ is the class index of the order $\mathrm{End}_k(A)$. By [MW95, eqn. 2.2] we have $i(A) \leq d(A)^{1/2}$, where $d(A)$ is the discriminant of $\mathrm{End}_k(A)$ as a $\mathbb{Z}$-module. Finally, by definition, $d(A)^{1/2} = (r/4)^{r/2} v(A) \leq (r/4)^{r/2} \Lambda^r$. □

Proof of Theorem 4.2.13. We start by bounding the smallest degree of isogenies from B' to B, for which we have used the notation $b(B)$. Let $\phi : B' \to B$ be an isogeny of the smallest degree d. We want to bound d in terms of $h(A)$ and $[k : \mathbb{Q}]$. First, by Lemma 4.2.4, we have

$$h(B') \leq h(B) + \tfrac{1}{2}\log \deg(\phi) = 2h(A) + \tfrac{1}{2}\log \deg(\phi) = 2h(A) + \tfrac{1}{2}\log d.$$

Then $m_{A,B'} = \max(1, h(A), h(B')) \leq 2h(A) + \frac{1}{2}\log d + 7$, since $h(A) \geq -3$ by Lemma 4.2.5. Then by Lemma 4.2.12 and the fact $m_{A,B'} \geq \log m_{A,B'}$, we have

$$\Lambda' \leq c_1 \left(c_2(k) \left(c_3(A,k) + \tfrac{1}{2}\log d \right)^2 \right)^{\frac{16}{\bar{r}}}, \tag{4.2.1}$$

where $\bar{r} = 1, 2$ or 4 and the constants are defined as

$$\begin{cases} c_1 = 4^{11} \cdot 9^{12}, \\ c_2(k) = 7.5 \cdot 10^{47} [k : \mathbb{Q}], \\ c_3(A,k) = 2h(A) + \frac{8}{17}\log[k : \mathbb{Q}] + \frac{1039}{17}. \end{cases}$$

We furthermore introduce the constants

$$\begin{cases} c_4(A,k) = \sqrt{c_2(k)}\, c_3(A,k), \\ c_5(k) = \dfrac{\sqrt{c_2(k)}}{2}, \\ c_6(A,k) = 2^{48} \cdot c_1^{16} \cdot \Lambda^{16r}, \end{cases}$$

and we rewrite inequality (4.2.1) as:

$$\Lambda' \leq c_1 [c_4(A,k) + c_5(k)\log d]^{\frac{32}{\bar{r}}}.$$

Then by Lemma 4.2.11, we have

$$d = \deg \phi \leq 2^{48} (\Lambda')^{16} \Lambda^{16r} \leq c_6(A,k) \left[c_4(A,k) + c_5(k) \log d \right]^{\frac{32 \cdot 16}{\bar{r}}}. \tag{4.2.2}$$

We define $c_7(A,k) = 2^{48} \cdot c_1^{16} \cdot c_8(A,k)^{16r}$ with $c_8(A,k)$ defined as

$$c_8(A,k) = \begin{cases} 2 & \text{if } \bar{r} = 1, \\ 4^5 \cdot 9^8 \cdot \Big(5.04 \cdot 10^{24} [k : \mathbb{Q}] m_A & \\ \quad \cdot \left(\frac{5}{4} m_A + \log[k : \mathbb{Q}] + \log m_A + 60 \right) \Big)^{8/\bar{r}} & \text{if } \bar{r} = 2, 4. \end{cases}$$

Then by Lemma 4.2.12, $c_6(A,k) \le c_7(A,k)$. We rewrite inequality (4.2.2) as

$$d^{\frac{\bar{r}}{32\cdot 16}} \le u(A,k)\left(\tfrac{\bar{r}}{32\cdot 16}\log d + v(A,k)\right),$$

where

$$\begin{cases} u(A,k) = c_7(A,k)^{\frac{\bar{r}}{32\cdot 16}} c_5(A,k)\cdot \dfrac{32\cdot 16}{\bar{r}}, \\ v(A,k) = \dfrac{c_4(A,k)\bar{r}}{32\cdot 16 c_5(A,k)}. \end{cases}$$

Then by Lemma 4.2.10, we have

$$d^{\frac{\bar{r}}{32\cdot 16}} \le 2u(A,k)[\log u(A,k) + v(A,k)].$$

Define

$$C(A,k) = 2u(A,k)[\log u(A,k) + v(A,k)],$$

which only depends on $h(A)$ and $[k:\mathbb{Q}]$. Then we find

$$b(B) \le C(A,k)^{\frac{32\cdot 16}{\bar{r}}}.$$

By Lemmas 4.2.14, 4.2.12, we obtain:

$$M_m \le (r/4)^{r/2}\Lambda^r b(B) \le (r/4)^{r/2} c_8(A,k)^r C(A,k)^{\frac{32\cdot 16}{\bar{r}}}.$$

Using $r \le \bar{r}$, in the case $\bar{r} = 1$ we find

$$M_m \le 2^{4664} c_1^{16} c_2(k)^{256}\Big(2h(A) + \tfrac{8}{17}\log[k:\mathbb{Q}] + 8\log c_1 + 128\log c_2(k) + 1503\Big)^{512},$$

and in the case $\bar{r} = 2$ or 4 we find that M_m is bounded above by

$$\begin{aligned} &(r/4)^{r/2} 2^{48}\cdot c_1^{16} c_2(k)^{256} \\ &\quad\cdot \Big(4^5\cdot 9^8\big(5.04\cdot 10^{24}[k:\mathbb{Q}] m_A\big(\tfrac{5}{4}m_A + \log[k:\mathbb{Q}] + \log m_A + 60\big)\big)^{8/\bar{r}}\Big)^{17r} \\ &\quad\cdot \Big[16\log c_1 + \frac{256}{\bar{r}}\log c_2(k) + 16r\log c_8(A,k) \\ &\qquad + 4h(A) + \tfrac{16}{17}\log[k:\mathbb{Q}] + 1400\Big]^{512/\bar{r}}. \end{aligned}$$

The constants c_1, $c_2(k)$ and $c_8(A,k)$ only depend on the Faltings height and the degree of the field extension $[k:\mathbb{Q}]$. □

4.3 Effective computations of the Néron–Severi lattice as a Galois module

Our goal of this section is to prove the following theorem:

THEOREM 4.3.1. *There is an explicit algorithm that takes input a smooth projective curve C of genus 2 defined over a number field k, and outputs a bound of the algebraic Brauer group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ where X is the Kummer surface associated to the Jacobian $\mathrm{Jac}(C)$.*

A general algorithm to compute Néron–Severi groups for arbitrary projective varieties is developed in [PTvL15], so here we consider algorithms specialized to the Kummer surface X associated to a principally polarized abelian surface A.

4.3.1 The determination of the Néron–Severi rank of A

THEOREM 4.3.2. *The following is a complete list of possibilities for the rank ρ of $\mathrm{NS}(\overline{A})$. For any prime $\mathfrak{p}$ we denote by $\rho_{\mathfrak{p}}$ the reduction of ρ modulo $\mathfrak{p}$.*

1. *When A is geometrically simple, we consider $D = \mathrm{End}_{\bar{k}}(A) \otimes \mathbb{Q}$, which has the following possibilities:*
   (a) *$D = \mathbb{Q}$ and $\rho = 1$. There exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 2$.*
   (b) *D is a totally real quadratic field. Then $\rho = 2$ and there exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 2$.*
   (c) *D is a indefinite quaternion algebra over $\mathbb{Q}$. Then $\rho = 3$ and there exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 4$.*
   (d) *D is a degree 4 CM field. Then $\rho = 2$ and there exists a density one set of primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}} = 2$. In fact this holds for the set of $\mathfrak{p}$'s such that A has ordinary reduction at $\mathfrak{p}$.*
2. *When A is isogenous over $\bar{k}$ to $E_1 \times E_2$ for two elliptic curves. Then*
   (a) *if E_1 is isogenous to E_2 and CM, then $\rho = 4$ and $\rho_{\mathfrak{p}} = 4$ for all ordinary reduction places.*

(b) *if E_1 is isogenous to E_2 but not CM, then $\rho = 3$ and $\rho_{\mathfrak{p}} = 4$ for all ordinary reduction places.*

(c) *if E_1 is not isogenous to E_2, then $\rho = 2$ and there exists a density one set of primes $\mathfrak{p}$ such that $\rho_{\mathfrak{p}} = 2$.*

Notice that for all the above statements, by an abuse of language, being density one means there exists a finite extension of k such that the primes are of density one with respect to this finite extension.

Proof. We apply [Mum70, p. 201 Thm. 2 and p.208] (and the remark on p. 203 referring to the work of Shimura) to obtain the list of the rank ρ. When A is geometrically simple, we can only have A of type I, II, and IV (in the sense of the Albert's classification). In the case of Type I, the totally real field may be $\mathbb{Q}$ or quadratic. In this case, the Rosati involution is trivial. This gives case (1)-(a,b). By [Mum70, p. 196], the Rosati involution of Type II is the transpose and its invariants are symmetric 2-by-2 matrices, which proves case (1)-(c). In the case of Type IV, D is a degree 4 CM field. In this case, the Rosati involution is the complex conjugation and this gives case (1)-(d). When A is not geometrically simple, then A is isogenous to the product of two elliptic curves and all these cases are easy.

Notice that after a suitable field extension, there exists a density one set of primes such that A has ordinary reduction (due to Katz, see [Ogu82] Sec. 2). We first pass to such an extension and only focus on primes where A has ordinary reduction. Then $\rho_{\mathfrak{p}} = 2$ if $A \bmod \mathfrak{p}$ is geometrically simple and $\rho_{\mathfrak{p}} = 4$ if A is not. Since $\rho_{\mathfrak{p}} \geq \rho$, we see that $\rho_{\mathfrak{p}} = 4$ in (1)-(c), (2)-(a,b) for any $\mathfrak{p}$ where A has ordinary reduction. When $\rho = 2$ (case (1)-(b,d), (2)-(c)), the dimension over $\mathbb{Q}$ of the orthogonal complement T of $\mathrm{NS}(\overline{A})$ in the Betti cohomology $\mathrm{H}^2(A, \mathbb{Q})$ is 4. By [Cha14, Thm. 1], if $\rho_{\mathfrak{p}}$ were 4 for a density one set of primes, then the endomorphism algebra E of T as a Hodge structure would have been a totally real field of degree $\rho_{\mathfrak{p}} - \rho = 2$ over $\mathbb{Q}$. Then T would have been of dimension 2 over E, which contradicts the assumption of the second part of Charles' theorem. Now the remaining case is (1)-(a). By [Cha14], for a density one set of $\mathfrak{p}$, the rank $\rho_{\mathfrak{p}}$ only depends on the degree of the endomorphism algebra E of the transcendental part T of the $\mathrm{H}^2(A, \mathbb{Q})$. This degree is the same for all A in case (1)-(a) since $E = \mathrm{End}(T) \subset \mathrm{End}(\mathrm{H}^2(A, \mathbb{Q}))$ is a set of Hodge cycles of $A \times A$ and all A in this case have the same set of Hodge cycles. For more details we refer the reader to [CF16]. Hence we only need to study a generic abelian surface. For a generic abelian surface, its ordinary

reduction is a (geometrically) simple CM abelian surface and hence $\rho_{\mathfrak{p}}$ is 2. □

Algorithms to compute the geometric Néron–Severi rank of A

Here we discuss an algorithm provided by Charles in [Cha14]. Charles' algorithm is to compute the geometric Néron–Severi rank of any $K3$ surface X, and his algorithm relies on the Hodge conjecture for codimension 2 cycles in $X \times X$. However, the situation where the Hodge conjecture is needed does not occur for abelian surfaces, so his algorithm is unconditional for abelian surfaces.

Suppose that A is a principally polarized abelian surface and Θ its principal polarization. We run the following algorithms simultaneously:

1. Compute Hilbert schemes of curves on A with respect to Θ for each Hilbert polynomial, and find divisors on A. Compute its intersection matrix using the intersection theory, and determine the rank of lattices generated by divisors one finds. This gives a lower bound η for $\rho = \operatorname{rk} \mathrm{NS}(\overline{A})$.

2. For each finite place $\mathfrak{p}$ of good reduction for A, compute the geometric Néron–Severi rank $\rho_{\mathfrak{p}}$ for $A_{\mathfrak{p}}$ using explicit point counting on the curve C combined with the Weil conjecture and the Tate conjecture. Furthermore compute the square class $\delta(\mathfrak{p})$ of the discriminant of $\mathrm{NS}(A_{\mathfrak{p}})$ in $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$ using the Artin–Tate conjecture:

$$P_2(q^{-s}) \sim_{s \to 1} \left(\frac{\#\operatorname{Br}(A_{\mathfrak{p}}) \cdot |\operatorname{disc}(\mathrm{NS}(A_{\mathfrak{p}}))|}{q} (1 - q^{1-s})^{\rho(A_{\mathfrak{p}})} \right),$$

where P_2 is the characteristic polynomial of the Frobenius endomorphism on

$$\mathrm{H}^2_{\text{ét}}(\overline{A}_{\mathfrak{p}}, \mathbb{Q}_{\ell}),$$

and q is the size of the residue field of $\mathfrak{p}$. When the characteristic is not equal to 2, then the Artin-Tate conjecture follows from the Tate conjecture for divisors ([Mil75]), and the Tate conjecture for divisors in abelian varieties is known ([Tat66]). Note that as a result of [LLR05], the size of the Brauer group must be a square. This gives us an upper bound for ρ.

When ρ is even, there exists a prime $\mathfrak{p}$ such that $\rho = \rho_{\mathfrak{p}}$. Thus eventually we obtain $\rho_{\mathfrak{p}} = \eta$ and we compute ρ.

When ρ is odd, it is proved in [Cha14, Prop. 18] that there exist $\mathfrak{p}$ and $\mathfrak{q}$ such that $\rho_{\mathfrak{p}} = \rho_{\mathfrak{q}} = \eta + 1$, but $\delta(\mathfrak{p}) \neq \delta(\mathfrak{q})$ in $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$. If this happens, then we can conclude that $\rho = \rho_{\mathfrak{p}} - 1$.

REMARK 4.3.3. The algorithm (1) can be conducted explicitly in the following way: Suppose that our curve C of genus 2 is given as a subscheme in the weighted projective space $\mathbb{P}(1,1,3)$. Let $Y = \mathrm{Sym}^2(C)$ be the symmetric product of C. Then we have the following morphism

$$f : C \times C \to Y \to \mathrm{Jac}(C), \quad (P,Q) \mapsto [P + Q - K_C].$$

The first morphism $C \times C \to Y$ is the quotient map of degree 2, and the second morphism is a birational morphism contracting a smooth rational curve R over the identity of $\mathrm{Jac}(C)$. We denote the diagonal of $C \times C$ by Δ and the image of the morphism $C \ni P \mapsto (P, \iota(P)) \in C \times C$ by Δ' where ι is the involution associated to the degree 2 canonical linear system. Then we have

$$f^*\Theta \equiv 5p_1^*\{\mathrm{pt}\} + 5p_2^*\{\mathrm{pt}\} - \Delta.$$

Note that $f^*\Theta$ is big and nef, but not ample. If we have a curve D on $\mathrm{Jac}(C)$, then its pullback f^*D is a connected subscheme of $C \times C$ which is invariant under the symmetric involution and $f^*D.\Delta' = 0$, and vice verse. Hence instead of doing computations on $\mathrm{Jac}(C)$, we can do computations of Hilbert schemes and the intersection theory on $C \times C$. This may be a more effective way to find curves on $\mathrm{Jac}(C)$ and its intersection matrix.

REMARK 4.3.4. The algorithm (2) is implemented in the paper [EJ12a].

4.3.2 The computation of the Néron–Severi lattice and its Galois action

Here we discuss an algorithm to compute the Néron–Severi lattice and its Galois structure. We have an algorithm to compute the Néron–Severi rank of $\overline{A}$, so we may assume it to be given. First we record the following algorithm:

LEMMA 4.3.5. *Let S be a polarized abelian surface or a polarized K3 surface over k, with an ample divisor H. Suppose that we have computed a*

full rank sublattice $M \subset \mathrm{NS}(\overline{S})$ containing the class of H, i.e., we know its intersection matrix, the Galois structure on $M \otimes \mathbb{Q}$, and we know generators for M as divisors in S. Then there is an algorithm to compute $\mathrm{NS}(\overline{S})$ as a Galois module.

Proof. We fix a basis $B_1, \cdots, B_r$ for M which are divisors on S. First note that the Néron–Severi lattice $\mathrm{NS}(\overline{S})$ is an overlattice of M. By Nikulin [Nik79, Sec. 1-4], there are only finitely many overlattices, (they correspond to isotropic subgroups in $D(M) = M^\vee/M$), and moreover we can compute all possible overlattices of M explicitly. Let N be an overlattice of M. We can determine whether N is contained in $\mathrm{NS}(\overline{S})$ in the following way:

Let $D_1, \ldots, D_s$ be generators for N/M. The overlattice N is contained in $\mathrm{NS}(\overline{S})$ if and only if the classes D_i are represented by integral divisors. After replacing D_i by $D_i + mH$, we may assume $D_i^2 > 0$ and $(D_i \cdot H) > 0$. If D_i is represented by an integral divisor, then it follows from Riemann–Roch that D_i is actually represented by an effective divisor C_i. We define $k = (D_i \cdot H)$ and $c = -\frac{1}{2}D_i^2$. The Hilbert polynomial of C_i with respect to H is $P_i(t) = kt + c$. Now we compute the Hilbert scheme Hilb^{P_i} associated with $P_i(t)$. For each connected component of Hilb^{P_i}, we take a member E_i of the universal family and compute the intersection numbers $(B_1 \cdot E), \ldots, (B_r \cdot E)$. If these coincide with the intersection numbers of D_i, then that member E_i is an integral effective divisor representing D_i. If we cannot find such an integral effective divisor for any connected component of Hilb^{P_i}, then we conclude that N is not contained in $\mathrm{NS}(\overline{S})$.

In this way we can compute the maximal overlattice $N_{\max}$ all whose classes are represented by integral divisors. This lattice $N_{\max}$ must be $\mathrm{NS}(\overline{S})$. Since M is full rank, the Galois structure on M induces the Galois structure on $\mathrm{NS}(\overline{S})$. □

From now on we focus on the case where $\overline{A}$ is simple and has Néron–Severi rank $\rho = 1$.

PROPOSITION 4.3.6. *Let A be a principally polarized abelian surface defined over a number field k whose geometric Néron–Severi rank is 1. Let X be the Kummer surface associated to A. Then there is an explicit algorithm that computes $\mathrm{NS}(\overline{X})$ as a Galois module and furthermore computes the group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$.*

The abelian surface A is a principally polarized abelian surface, so the lattice $\mathrm{NS}(\overline{A})$ is isomorphic to the lattice $\langle 2\rangle$ with the trivial Galois action. We denote the blow up of 16 2-torsion points on A by $\widetilde{A}$ and the 16 exceptional curves on $\tilde{A}$ by E_i. There is an isometry

$$\mathrm{NS}(\widetilde{A}_{\overline{k}}) \cong \mathrm{NS}(\overline{A}) \oplus \bigoplus_{i=1}^{16} \mathbb{Z}E_i.$$

We want to determine the Galois structure of this lattice. To this end, one needs to understand the Galois action on the set of 2-torsion elements on $\overline{A}$. This can be done explicitly in the following way: Suppose that A is given as a Jacobian of a smooth projective curve C of genus 2. Then C is a hyperelliptic curve whose canonical linear series is a degree 2 morphism. We denote the ramification points (over $\overline{k}$) of this degree 2 map by $p_1, \cdots, p_6$. One can find the Galois action on these ramification points from the polynomial defining C. All non-trivial 2-torsion points of $\overline{A}$ are given by $p_i - p_j$ where $i < j$. Note that $p_i - p_j \sim p_j - p_i$ as classes in $\mathrm{Pic}(C)$. Thus, we can determine the Galois structure on the set of 2-torsion elements of $\overline{A}$.

Let X be the Kummer surface associated to A with the degree 2 finite morphism $\pi : \widetilde{A} \to X$. We take the pushforward of $\mathrm{NS}(\widetilde{A}_{\overline{k}})$ in $\mathrm{NS}(\overline{X})$:

$$\mathrm{NS}(\overline{X}) \supset \pi_* \mathrm{NS}(\widetilde{A}_{\overline{k}}) \cong \pi_* \mathrm{NS}(\overline{A}) \oplus \bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i.$$

This is a full rank sublattice. Thus the Galois representation for $\mathrm{NS}(\widetilde{A}_{\overline{k}})$ tells us the representation for $\mathrm{NS}(\overline{X})$. Hence we need to determine the lattice structure for $\mathrm{NS}(\overline{X})$. This is done in [LP80, Sec. 3]. Let us recall the description of the Néron–Severi lattice for any Kummer surface.

According to [LP80, Prop. 3.4] and [LP80, Prop. 3.5], the sublattice $\pi_* \mathrm{NS}(\widetilde{A}_{\overline{k}})$ is primitive in $\mathrm{NS}(\overline{X})$, and its intersection pairing is twice the intersection pairing of $\mathrm{NS}(\widetilde{A}_{\overline{k}})$. In particular, in our situation, we have $\pi_* \mathrm{NS}(\widetilde{A}_{\overline{k}}) \cong \langle 4\rangle$. Let K be the saturation of the sublattice generated by the $\pi_* E_i$'s. Nodal classes $\pi_* E_i$ have self intersection -2. We have the following inclusions:

$$\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i \subset K \subset K^\vee \subset \left(\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i \right)^\vee = \bigoplus_{i=1}^{16} \frac{1}{2}\mathbb{Z}\pi_* E_i$$

where $L^\vee$ denotes the dual abelian group of a given lattice L. We denote the set of 2-torsion elements of $\overline{A}$ by V. We can consider V as the 4 dimensional affine space over $\mathbb{F}_2$. Then we can interpret $\bigoplus_{i=1}^{16} \frac{1}{2}\mathbb{Z}\pi_* E_i/\mathbb{Z}\pi_* E_i$ as the space of $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$-valued functions on V. [LP80, Prop 3.6] shows that with this identification, the image of K (resp. $K^\vee$) in $\bigoplus_{i=1}^{16} \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ consists of polynomial functions $V \to \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of degree ≤ 1 (resp. ≤ 2.) Hence we have

$$\left[K : \bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i\right] = 2^5, \quad [K^\vee : K] = 2^6.$$

This description allows us to choose an explicit basis for K as well as to find its intersection matrix. The discriminant group of K is isomorphic to $\mathbb{F}_2^6$ whose discriminant form is given by

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

This discriminant form is isometric to the discriminant form of $\pi_* H^2(A, \mathbb{Z})$ which is isomorphic to

$$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$$

Now we have overlattices:

$$\pi_* \operatorname{NS}(\overline{A}) \oplus K \subset \operatorname{NS}(\overline{X}).$$

To identify $\operatorname{NS}(\overline{X})$, we consider the following overlattices:

$$\pi_* \operatorname{H}^2(A, \mathbb{Z}) \oplus K \subset \operatorname{H}^2(X, \mathbb{Z}).$$

One can describe $\operatorname{H}^2(X, \mathbb{Z})$ using techniques in [Nik79, Sec 1.1-1.5]. Since the second cohomology of any $K3$ surface is unimodular, we have the following inclusions:

$$\pi_* \operatorname{H}^2(A, \mathbb{Z}) \oplus K \subset \operatorname{H}^2(X, \mathbb{Z}) = \operatorname{H}^2(X, \mathbb{Z})^\vee \subset (\pi_* \operatorname{H}^2(A, \mathbb{Z}))^\vee \oplus K^\vee$$

This gives us the following isotropic subgroup in the direct sum of the discriminant forms:

$$H = \operatorname{H}^2(X, \mathbb{Z})/\pi_* \operatorname{H}^2(A, \mathbb{Z}) \oplus K \hookrightarrow D(\pi_* \operatorname{H}^2(A, \mathbb{Z})) \oplus D(K)$$

where $D(L)$ denotes the discriminant group of a given lattice L.

Since $\pi_* \mathrm{H}^2(A,\mathbb{Z})$ and K are primitive in $\mathrm{H}^2(X,\mathbb{Z})$, each of the projections $H \to D(\pi_* \mathrm{H}^2(A,\mathbb{Z}))$ and $H \to D(K)$ is injective. Moreover, since $\mathrm{H}^2(X,\mathbb{Z})$ is unimodular, the isotropic subgroup H must be maximal inside $D(\pi_* \mathrm{H}^2(A,\mathbb{Z})) \oplus D(K)$. This implies that both injections are in fact isomorphisms. Thus we determine $\mathrm{H}^2(X,\mathbb{Z})$ as an overlattice corresponding to H in $D(\pi_* \mathrm{H}^2(A,\mathbb{Z})) \oplus D(K)$. Note that we can apply the orthogonal group $O(K)$ to H so that H is unique up to this action. Namely if we fix an identification $q_K = -q_K \cong q_{\pi_* \mathrm{H}^2(A,\mathbb{Z})}$ and $D(K) \cong D(\pi_* \mathrm{H}^2(A,\mathbb{Z}))$, then we can think of H as the diagonal in $D(K) \oplus D(\pi_* \mathrm{H}^2(A,\mathbb{Z}))$.

We succeeded in expressing our embedding $\pi_* H^2(A,\mathbb{Z}) \oplus K \hookrightarrow H^2(X,\mathbb{Z})$, hence we can express $\mathrm{NS}(\overline{X})$ as

$$\mathrm{NS}(\overline{X}) = H^2(X,\mathbb{Z}) \cap (\pi_* \mathrm{NS}(\overline{A}) \oplus K) \otimes \mathbb{Q}.$$

Note that an embedding of $\mathrm{NS}(\overline{A})$ into $H^2(A,\mathbb{Z})$ is unique up to isometries because of [Nik79, Thm 1.1.2[4]], so we can map a generator of $\mathrm{NS}(\overline{A})$ to $e+f$ where e, f is a basis for the hyperbolic plane $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Thus we determine the lattice structure of $\mathrm{NS}(\overline{X})$.

Remark 4.3.7. In §4.5, we will in fact use a somewhat simpler argument in order to describe $\mathrm{NS}(\overline{X})$ as a Galois module. The advantage of the argument given in the current section is that it can be made applicable for higher rank cases.

4.4 Effective bounds for the transcendental part of Brauer groups

Let A be a principally polarized abelian surface defined over a number field k. Let $X = \mathrm{Kum}(A)$ be the Kummer surface associated to the abelian surface A. The goal of this section is to prove the following theorem:

Theorem 4.4.1. *There exists an effectively computable constant N_1 depending on the number field k, the Faltings height $h(A)$, and $\mathrm{NS}(\overline{A})$ satisfying*

$$\#\frac{\mathrm{Br}(X)}{\mathrm{Br}_1(X)} \leq N_1.$$

[4] attributed to D.G. James

Remark 4.4.2. In this section we focus on the proof of the method in the general case. In case that A is not geometrically simple, better bounds can be found based on recent work of Newton [New16].

First we use the following important theorem by Skorobogatov and Zarhin:

Theorem 4.4.3. [SZ12, Prop. 1.3] *Let A be an abelian surface defined over a number field k and $X = \mathrm{Kum}(A)$ the associated Kummer surface. Then there is a natural map*

$$\mathrm{Br}(\overline{X}) \cong \mathrm{Br}(\overline{A})$$

which is an isomorphism of Galois modules.

Hence there is an injection

$$\frac{\mathrm{Br}(X)}{\mathrm{Br}_1(X)} \hookrightarrow \mathrm{Br}(\overline{X})^{\Gamma} = \mathrm{Br}(\overline{A})^{\Gamma},$$

where $\Gamma = \mathrm{Gal}(\bar{k}/k)$. Thus, to bound $\frac{\mathrm{Br}(X)}{\mathrm{Br}_1(X)}$ in terms of k, the Faltings height $h(A)$, and $\delta = \det(\mathrm{NS}(\overline{A}))$, we only need to bound $\mathrm{Br}(\bar{A})^{\Gamma}$.

Also we would like to recall the following important result about the geometric Brauer groups:

Theorem 4.4.4. *As abelian groups, we have the following isomorphisms:*

$$\mathrm{Br}(\overline{X}) \cong \mathrm{Br}(\overline{A}) \cong (\mathbb{Q}/\mathbb{Z})^{6-\rho},$$

where $\rho = \rho(\overline{A})$ is the geometric Néron–Severi rank of A.

Proof. This follows from the remark before [SZ12, Lem. 1.1]. □

We discuss several lemmas to prove our main Theorem 4.4.1. Recall that $\widetilde{M}$ is the constant from Theorem 4.2.13.

Lemma 4.4.5. *Let $N_2 = \max\{\widetilde{M}, \delta\}$ where $\delta = \mathrm{disc}(\mathrm{NS}(\overline{A}))$. Then for any prime number $\ell > N_2$ we have*

$$\mathrm{Br}(\overline{A})^{\Gamma}_{\ell} = \{0\},$$

where $\mathrm{Br}(\overline{A})^{\Gamma}_{\ell}$ denotes the ℓ-torsion group of $\mathrm{Br}(\overline{A})^{\Gamma}$.

Proof. This essentially follows from results in [SZ08] combined with Theorem 4.2.13. The following exact sequence occurs as the $n = 1$ case of [SZ08, p. 486 (5)]:

$$0 \to \left(\mathrm{NS}(\overline{A})/\ell\right)^{\Gamma} \xrightarrow{f} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_\ell)^{\Gamma} \to \mathrm{Br}(\overline{A})^{\Gamma}_{\ell} \to$$
$$\to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell) \xrightarrow{g} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_\ell)).$$

The discussion in [SZ08, Prop. 2.5 (a)] shows that $\mathrm{NS}(\overline{A}) \otimes \mathbb{Z}_\ell$ is a direct summand of $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1))$ for any prime $\ell \nmid \delta$. For such ℓ, the homomorphism g in the above exact sequence is injective.

Next, Theorem 4.2.13 asserts that there exists an effectively computable integer $\widetilde{M} > 0$ depending on k and $h(A)$ such that for any prime $\ell > \widetilde{M}$, we have an isomorphism:

$$\mathrm{End}_k(A)/\ell \cong \mathrm{End}_\Gamma(A_\ell).$$

The discussion in [SZ08, Lem. 3.5] shows that for such ℓ, the homomorphism f is bijective. Thus our assertion follows. □

Thus, to prove our main theorem, we need to bound $\mathrm{Br}(\overline{A})^{\Gamma}(\ell)$ for each prime number ℓ where $\mathrm{Br}(\overline{A})^{\Gamma}(\ell)$ denotes the ℓ-primary subgroup of elements whose orders are powers of ℓ. To achieve this task, we employ techniques from [HKT13, §7 and 8].

We fix an embedding $k \hookrightarrow \mathbb{C}$ and consider the following lattice:

$$\mathrm{H}^2(A(\mathbb{C}), \mathbb{Z}).$$

It contains $\mathrm{NS}(\overline{A})$ as a primitive sublattice and we denote its orthogonal complement by $T_A = \langle \mathrm{NS}(\overline{A}) \rangle^{\perp}_{\mathrm{H}^2(A(\mathbb{C}),\mathbb{Z})}$ and call it the transcendental lattice of A. The direct sum $\mathrm{NS}(\overline{A}) \oplus T_A$ is a full rank sublattice of $\mathrm{H}^2(A(\mathbb{C}), \mathbb{Z})$ and we can put it into the exact sequence:

$$0 \to \mathrm{NS}(\overline{A}) \oplus T_A \to \mathrm{H}^2(A(\mathbb{C}), \mathbb{Z}) \to K \to 0,$$

where K is a finite abelian group of order $\delta = \mathrm{disc}(\mathrm{NS}(\overline{A}))$. Tensoring with $\mathbb{Z}_\ell$ and using a comparison theorem for the different cohomologies, we have

$$0 \to \mathrm{NS}(\overline{A})_\ell \oplus T_{A,\ell} \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \to K_\ell \to 0,$$

where $\mathrm{NS}(\overline{A})_\ell = \mathrm{NS}(\overline{A}) \otimes \mathbb{Z}_\ell$, $T_{A,\ell} = T_A \otimes \mathbb{Z}_\ell$, and K_ℓ is the ℓ-primary part of K. The second étale cohomology $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1))$ comes with a natural pairing which is compatible with Γ-action, and $T_{S,\ell}$ is the orthogonal complement of $\mathrm{NS}(\overline{A})_\ell$. In particular, $T_{A,\ell}$ has a natural structure as a Galois module.

LEMMA 4.4.6. *Fix a prime number ℓ. Let $N_{3,\ell} = (6-\rho)\log_\ell \widetilde{M}$. Then for each integer $n \geq 1$ the bound*

$$\#(T_A/\ell^n)^\Gamma \leq \ell^{N_{3,\ell}}$$

is satisfied.

Proof. Since A is principally polarized, we have a natural isomorphism of Galois modules:

$$\mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \cong (\mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)))^* \cong T_\ell(A),$$

where $T_\ell(A)$ is the Tate module of A. Hence we have

$$\begin{aligned} T_{A,\ell} &\hookrightarrow \mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) = \textstyle\bigwedge^2 \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \\ &\hookrightarrow \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \otimes \mathrm{H}^1_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \cong \mathrm{End}(T_\ell(A)). \end{aligned}$$

Thus we have

$$(T_A/\ell^n) = (T_{A,\ell}/\ell^n) \hookrightarrow \mathrm{End}(T_\ell(A))/\ell^n = \mathrm{End}(\overline{A}[\ell^n]).$$

Hence we obtain a homomorphism

$$\Phi : (T_A/\ell^n)^\Gamma \hookrightarrow \mathrm{End}_\Gamma(\overline{A}[\ell^n]) \to \mathrm{End}_\Gamma(\overline{A}[\ell^n])/\mathrm{End}(A).$$

This composite homomorphism Φ must be injective because T_A is the transcendental lattice which does not meet the algebraic part $\mathrm{End}(A)$. The order of this quotient is bounded by Theorem 4.2.13. □

Taking a finite extension of k only increases the size of $\mathrm{Br}(\overline{A})^{\mathrm{Gal}(\bar{k}/k')}$, so from now on we assume that the Galois action on the Néron–Severi space $\mathrm{NS}(\overline{A})$ is trivial. This is automatically true when the geometric Néron–Severi rank of A is 1.

LEMMA 4.4.7. *Suppose that the Galois action on $\mathrm{NS}(\overline{A})$ is trivial. Write*

$$N_{4,\ell} = (2v_\ell(\delta) + 10\log_\ell \widetilde{M})(6-\rho)$$

where v_ℓ is the valuation at ℓ. Then for each prime ℓ, we have

$$\#\,\mathrm{Br}(\overline{A})^\Gamma(\ell) \leq \ell^{N_{4,\ell}}.$$

Proof. Recall the exact sequence of [SZ08, p. 486 (5)]:

$$\begin{aligned} 0 \to \left(\mathrm{NS}(\overline{A})/\ell^n\right)^\Gamma \xrightarrow{f_n} \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma \to \mathrm{Br}(\overline{A})^\Gamma_{\ell^n} \to \\ \to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \xrightarrow{g_n} \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})), \end{aligned}$$

so we need to bound the cokernel of f_n and the kernel of g_n independent of n. By Theorem 4.4.4, it is enough to bound the orders of elements in $\mathrm{coker}(f_n)$ as well as $\ker(g_n)$ independently of n.

Let ℓ^m be the order of K_ℓ and we assume that $n \geq m$. We have the following exact sequence:

$$0 \to \mathrm{NS}(\overline{A})_\ell \oplus T_{A,\ell} \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1)) \to K_\ell \to 0.$$

Tensoring by $\mathbb{Z}/\ell^n\mathbb{Z}$ (as $\mathbb{Z}_\ell$-modules) and using Tor functors, we obtain a four term exact sequence:

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus T_A/\ell^n \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \to K_\ell \to 0, \tag{4.4.1}$$

where we've used that the middle term $\mathrm{H}^2_{\text{ét}}(\overline{A}, \mathbb{Z}_\ell(1))$ is a free (and hence flat) $\mathbb{Z}_\ell$-module.

Note that the projection

$$K_\ell \to \mathrm{NS}(\overline{A})/\ell^n$$

is injective because $T_A/\ell^n \to \mathrm{H}^2(\overline{A}, \mu_{\ell^n})$ is injective. In particular, the Galois action on K_ℓ is trivial. We split the exact sequence (4.4.1) as

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus T_A/\ell^n \to D \to 0,$$

and

$$0 \to D \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}) \to K_\ell \to 0.$$

These gives us the long exact sequences

$$\begin{aligned} 0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus (T_A/\ell^n)^\Gamma \to D^\Gamma \to \\ \to \mathrm{Hom}(\Gamma, K_\ell) \to \mathrm{Hom}(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \oplus \mathrm{H}^1(\Gamma, T_A/\ell^n), \end{aligned}$$

and

$$0 \to D^\Gamma \to \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma \to K_\ell \to \mathrm{H}^1(\Gamma, D) \to \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})).$$

The map $\mathrm{Hom}(\Gamma, K_\ell) \to \mathrm{Hom}(\Gamma, \mathrm{NS}(\overline{A})/\ell^n)$ is injective, so the sequence

$$0 \to K_\ell \to \mathrm{NS}(\overline{A})/\ell^n \oplus (T_A/\ell^n)^\Gamma \to D^\Gamma \to 0,$$

is exact. We conclude that

$$\#\operatorname{coker}(f_n) = \frac{\#\,\mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})^\Gamma}{\#\,\mathrm{NS}(\overline{A})/\ell^n} \leq \frac{\#K_\ell \cdot \#D^\Gamma}{\#\,\mathrm{NS}(\overline{A})/\ell^n} = \#(T_A/\ell^n)^\Gamma$$

is bounded independent of n by application of Lemma 4.4.6.

Next we discuss a uniform bound on the maximum order of elements in $\ker(g_n)$. The homomorphism g_n is a composition of two homomorphisms:

$$\mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \to \mathrm{H}^1(\Gamma, D) \to \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n})).$$

The kernel of $\mathrm{H}^1(\Gamma, D) \to \mathrm{H}^1(\Gamma, \mathrm{H}^2_{\text{ét}}(\overline{A}, \mu_{\ell^n}))$ is bounded by K_ℓ. We have the exact sequence

$$0 \to \mathrm{NS}(\overline{A})/\ell^n \to D \to D/\,\mathrm{NS}(\overline{A}) \to 0,$$

which gives the long exact sequence

$$0 \to \mathrm{NS}(\overline{A})/\ell^n \to D^\Gamma \to (D/\,\mathrm{NS}(\overline{A}))^\Gamma \to \mathrm{H}^1(\Gamma, \mathrm{NS}(\overline{A})/\ell^n) \to \mathrm{H}^1(\Gamma, D).$$

Thus to finish the proof we need to find an uniform bound for the maximum order of elements in $(D/\,\mathrm{NS}(\overline{A}))^\Gamma$. To obtain this, we look at the exact sequence

$$0 \to K_\ell \to T_A/\ell^n \to D/\,\mathrm{NS}(\overline{A}) \to 0.$$

This gives us the long exact sequence

$$0 \to K_\ell \to (T_A/\ell^n)^\Gamma \to (D/\,\mathrm{NS}(\overline{A}))^\Gamma \to \mathrm{Hom}(\Gamma, K_\ell).$$

Note that the group $\mathrm{Hom}(\Gamma, K_\ell)$ is killed by $\#K_\ell$. Finally, $\#(T_A/\ell^n)^\Gamma$ is uniformly bounded by the result of Lemma 4.4.6. Therefore the maximum order of elements in $(D/\,\mathrm{NS}(\overline{A}))^\Gamma$ is uniformly bounded and our assertion follows. □

Proof of Theorem 4.4.1. It follows from Lemma 4.4.5 and 4.4.7 that we can take N_1 as

$$\delta^{10} \prod_{\ell \leq N_2} \widetilde{M}^{50}.$$

□

4.5 Computations on rank 17

In this section we discuss some computations in order to determine the group $\mathrm{Br}_1(X)/\mathrm{Br}_0(X)$ through $\mathrm{H}^1(k, \mathrm{NS}(\overline{X}))$ using Magma, where the geometric Néron–Severi rank of X is 17.[5] Recall that the Néron–Severi lattice of a Kummer surface is determined by the sixteen 2-torsion points on the associated abelian surface and its Néron–Severi lattice. A principally polarized abelian surface is the Jacobian of a genus 2 curve C and its 2-torsion points correspond to the classes $p_i - p_j$ of differences of the six ramification points of $C \to \mathbb{P}^1$.

First we need to fix some ordering. Let $\{p_1, \ldots, p_6\}$ be the ramification points of C. Then on $\mathrm{Jac}(C)[2] = \{0, p_i - p_j : i < j\}$ the following additive rule holds

$$p_i - p_j = p_k - p_l + p_n - p_m$$

where $\{i, j\}$ and $\{k, l, m, n\}$ are two complementary subsets of $\{1, \ldots, 6\}$.

Lemma 4.5.1. *The set*

$$\{p_1 - p_2 =: v_1, p_1 - p_3 =: v_2, p_1 - p_4 =: v_3, p_1 - p_5 =: v_4\}$$

forms a basis of $\mathrm{Jac}(C)[2] \cong \mathbb{F}_2^4$.

Proof. In order to write 0 as a linear combination of these elements (over $\mathbb{F}_2$), we need to use an even number. Since any two of these are different, this may only be done using all four of them. However, the sum of these four elements is $p_2 - p_3 + p_4 - p_5 = p_1 - p_6 \neq 0$. □

We order the 2-torsion elements in terms of $p_i - p_j$ and in terms of v_i in Table 4.1.

The Galois action is defined by a subgroup of S_6, acting on the six ramification points p_i and hence on the set of e_i. This action defines S_6 as a subgroup of S_{16}. We know that S_6 is generated by the two elements $(1, 2)$ and $(1, 2, 3, 4, 5, 6)$, so to determine the map $S_6 \to S_{16}$ we need only specify the images of $(1, 2)$ and $(1, 2, 3, 4, 5, 6)$.

[5] In the published paper there is a typo: this rank is said to be assumed to be 1 instead. In the case we are considering, this does hold for the associated abelian surface.

LEMMA 4.5.2. *Let $\rho\colon S_6 \to S_{16}$ be the map that represents the action of S_6 on the sixteen 2-torsion points e_i. Then*

$$\rho((1,2)) = (3,4)(5,6)(9,10)(15,16)$$

and

$$\rho((1,2,3,4,5,6)) = (2,4,7,13,8,16)(3,6,11,12,9,15)(5,10,14)$$

hold.

Proof. Direct computation on the elements in Table 4.1, e.g. $\rho((1,2))$ maps $e_3 = p_1 - p_3$ to $p_2 - p_3 = e_4$. □

$e_1 = 0$	$e_9 = p_1 - p_5 = v_4$
$e_2 = p_1 - p_2 = v_1$	$e_{10} = p_2 - p_5 = v_1 + v_4$
$e_3 = p_1 - p_3 = v_2$	$e_{11} = p_3 - p_5 = v_2 + v_4$
$e_4 = p_2 - p_3 = v_1 + v_2$	$e_{12} = p_4 - p_6 = v_1 + v_2 + v_4$
$e_5 = p_1 - p_4 = v_3$	$e_{13} = p_4 - p_5 = v_3 + v_4$
$e_6 = p_2 - p_4 = v_1 + v_3$	$e_{14} = p_3 - p_6 = v_1 + v_3 + v_4$
$e_7 = p_3 - p_4 = v_2 + v_3$	$e_{15} = p_2 - p_6 = v_2 + v_2 + v_4$
$e_8 = p_5 - p_6 = v_1 + v_2 + v_3$	$e_{16} = p_1 - p_6 = v_1 + v_2 + v_3 + v_4$

Table 4.1: Chosen ordering of 2-torsion elements in both descriptions.

Using the description from [LP80, Prop. 3.4 and 3.5] as explained in §4.3.2, the lattice K is generated by $\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i$ together with lifts from polynomials in four variables with values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ of degree at most 1. These are generated as an abelian group by $x_1, x_2, x_3, x_4, 1$, where the set of x_i's is dual to the set of v_j's in the sense $x_i(v_j) = \delta_{ij}$. We identify the set of exceptional curves with the set of 2-torsion points in the natural way by identifying E_i and e_i for each $i = 1, \ldots, 16$.

From a theoretical perspective, one could use the approach as laid out in §4.3.2 in order to calculate $\mathrm{NS}(X)$, but for the case $\operatorname{rk}\mathrm{NS}(\overline{A}) = 1$, it turns out that there is an easier approach which involves knowing the index of $\pi_* \mathrm{NS}(A) \oplus K$ in $\mathrm{NS}(X)$.

LEMMA 4.5.3. *Let A be an abelian surface of Néron–Severi rank ρ, write $X = \mathrm{Kum}(A)$ and let K be the saturation of $\bigoplus_{i=1}^{16} \mathbb{Z}\pi_* E_i$ inside $\mathrm{NS}(X)$. Then the index of $\pi_* \mathrm{NS}(A) \oplus K$ inside $\mathrm{NS}(X)$ is 2^ρ.*

Proof. Write $t = |\operatorname{disc} \mathrm{NS}(A)|$, then also $t = |\operatorname{disc} T(A)|$ holds, where $T(A)$ is the transcendental lattice of A, since $\mathrm{H}^2(A, \mathbb{Z})$ is unimodular. We have equality of ranks

$$\operatorname{rk} T(X) = \operatorname{rk} T(A) = 6 - \rho,$$

and hence $|\operatorname{disc} T(X)| = t \cdot 2^{6-\rho}$ from which follows $|\operatorname{disc} \mathrm{NS}(X)| = t \cdot 2^{6-\rho}$ since $\mathrm{H}^2(X, \mathbb{Z})$ is unimodular.

Let $L = \pi_* \mathrm{NS}(A)$. Then $\operatorname{rk} L = \rho$ and $|\operatorname{disc} L| = 2^\rho t$ hold.

We use the chain of inclusions

$$L \oplus K \subset \mathrm{NS}(X) \subset \mathrm{NS}(X)^\vee \subset L^\vee \oplus K^\vee$$

The index of $L \oplus K \subset L^\vee \oplus K^\vee$ is $2^\rho t \cdot 2^6$ (see §4.3.2 for the discriminant of K) and combining with the discriminants above, we find the statement of the lemma. □

From now on, assume $\rho = 1$, i.e. the geometric Néron–Severi rank of X is 17. Let l be the push-forward of the theta-divisor on A. Then $l^2 = 4$ and by Lemma 4.5.3, the index of $\Lambda := \langle l \rangle \oplus K$ in $\mathrm{NS}(\overline{X})$ is 2. It therefore suffices to find a single element $D \in \mathrm{NS}(\overline{X})$ such that $2D$ is an element of Λ but D itself is not. Then Λ and D together span $\mathrm{NS}(\overline{X})$.

Lemma 4.5.4. *Up to isomorphism there is only one index 2 even overlattice of* Λ.

Proof. Even overlattices of index 2 correspond to isotropic subgroups of the discriminant group $D(\Lambda) = D(\pi_* \mathrm{NS}(\overline{A})) \oplus D(K)$ of order 2. Since K is saturated, a generating element of such a subgroup projects to an element of $D(\pi_* \mathrm{NS}(\overline{A}))$ which has order exactly 2. Since $D(\pi_* \mathrm{NS}(\overline{A}))$ is isomorphic to $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$, there is only one such element, which has square $1 \pmod 2$. We therefore need to consider order 2 elements of square $1 \pmod 2$ in $D(K)$. Since we remember the intersection form on $D(K)$ from section 4.3.2, we easily see that there are four such elements, with coordinates $(1,0,0,0,0,1)$, $(0,1,0,0,1,0)$, $(0,0,1,1,0,0)$ and $(1,1,1,1,1,1)$. By calculating the centralizer of the intersection matrix of $D(K)$ inside $\mathrm{GL}_6(\mathbb{F}_2)$, that is $\mathcal{O}(D(K))$, it is easily found that each of these lie in the same orbit under the action of $\mathcal{O}(D(K))$. □

It is worthwhile to remark that the Galois action on the 2-torsion points of A induces an action on $D(K)$ and only one of the four elements in the

previous proof is invariant under the action of the full symmetric group S_6, which in our chosen basis is $(1,1,1,1,1,1)$.

LEMMA 4.5.5. *The element*

$$D = \frac{1}{2}(\pi_* E_1 + \pi_* E_8 + \pi_* E_{12} + \pi_* E_{14} + \pi_* E_{15} + \pi_* E_{16} + l)$$

together with Λ *spans* $\mathrm{NS}(\overline{X})$.

Proof. We already know that the coefficient of l is non-zero since K is saturated in $\mathrm{NS}(\overline{X})$, and by adding a suitable element of 2Λ to D, we can write $D = \frac{1}{2}l + \frac{1}{2}\sum_{i=1}^{16} a_i \pi_* E_i$, where for each i we take $a_i \in \{0, \frac{1}{2}, 1, \frac{3}{2}\}$.

By intersecting D with any of the $\pi_* E_i$, we find $a_i \in \{0, 1\}$ since the intersection needs to be integral. From $D^2 \in 2\mathbb{Z}$ we deduce the congruence $\sum_{i=1}^{16} a_i \equiv 2 \pmod 4$. Furthermore, the projection of D to $D(K)$ needs to be one of the four elements from the proof of Lemma 4.5.4. In order to ensure that the lattice we generate is a Galois module for any subgroup of S_6, the element D from the statement is chosen so that it projects to the unique S_6-invariant one. □

Now that we have computed $\mathrm{NS}(\overline{X})$, we can have MAGMA take Galois cohomology by applying the action from Lemma 4.5.2 and we find

$$\mathrm{H}^1(k, \mathrm{NS}(\overline{X})) = 1.$$

We can furthermore consider the case where the Galois group is not the full S_6. The MAGMA computations also yield the following:

PROPOSITION 4.5.6. *Up to conjugation there are only three subgroups* H *of* S_6 *for which* $\mathrm{H}^1(H, \mathrm{NS}(\overline{X}))$ *is non-trivial: one of order 4 (isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*), one of order 12 (isomorphic to* A_4*) and one of order 60 (isomorphic to* A_5*). In each of these cases we find* $\mathrm{H}^1(H, \mathrm{NS}(\overline{X})) \cong \mathbb{Z}/2\mathbb{Z}$.

4.6 An example

In this section we compute a concrete bound as stated in Theorem 4.2.13. Let us consider the genus 2 curve defined over $\mathbb{Q}$ by:

$$C : y^2 = x^6 + x^3 + x + 1.$$

Let A denote the Jacobian of C. Thanks to the algorithm provided by Elsenhans and Jahnel in [EJ12a] we compute the Néron–Severi rank of A and we obtain that its geometric Néron–Severi rank is 1. By Theorem 4.3.2 we know $\mathrm{End}(A) = \mathbb{Z}$.

Since $x^6 + x^3 + x + 1 = (x+1)(x^2+1)(x^3 - x^2 + 1)$, the splitting field F of $x^6 + x^3 + x + 1$ is the composite field of $\mathbb{Q}(\sqrt{-1})$ and the splitting field F_1 of $x^3 - x^2 + 1$. The Galois group $\mathrm{Gal}(F/\mathbb{Q})$ has 12 elements and two normal subgroups: $\mathbb{Z}/2\mathbb{Z}$ and S_3. By Proposition 4.5.6, the only exceptional subgroup with 12 elements is A_4. Since the only nontrivial normal subgroup of A_4 has 4 elements, $\mathrm{Gal}(F/\mathbb{Q})$ cannot be one of the exceptional subgroups of S_6. Therefore the algebraic Brauer group is trivial.

To compute the bound of Theorem 4.2.13 we need to compute the Faltings height of the abelian surface A. By Proposition 4.2.1, $h(A)$ is bounded above by

$$\begin{aligned} &-\log(2\pi^2) + \tfrac{1}{10}\log\left(2^{-12}\,\mathrm{Disc}_6\left(4(x^6+x^3+x+1)\right)\right) \\ &\qquad - \log\left(2^{-1/5}|J_{10}|^{1/10}\det(\Im\tau)^{1/2}\right), \end{aligned}$$

with $2^{-12}\,\mathrm{Disc}_6\left(4(x^6+x^3+x+1)\right) = 2^{12}\cdot 25\cdot 23$, $|J_{10}| = 0.001921635$ and

$$\tau = \begin{pmatrix} -1.49097 + 1.64505i & -0.50000 + 0.98058i \\ -0.50000 + 0.98058i & -1.50903 + 1.64505i \end{pmatrix}.$$

Hence $h(A) \leq -0.79581$. In our situation we have $k = \mathbb{Q}$, so we can bound M by plugging these into

$$\begin{aligned} M \leq 2^{4664} c_1^{16} c_2(k)^{256} \Big(&2h(A) + \tfrac{8}{17}\log[k:\mathbb{Q}] + 8\log c_1 \\ &+ 128\log c_2(k) + 1503 \Big)^{512} \end{aligned}$$

with $c_1 = 4^{11}\cdot 9^{12}$ and $c_2(k) = 7.5\cdot 10^{47}[k:\mathbb{Q}]$.

Using Magma we get

$$M \leq \widetilde{M} = 8.7 \times 10^{16100}.$$

Let $X = \mathrm{Kum}(A)$. We may apply Theorem 4.4.1 directly to obtain an explicit bound. However, since the curve C is defined over $\mathbb{Q}$, we will combine our bound in Lemma 4.4.7 with the results of Dieulefait and Skorobogatov–Zarhin to obtain a sharper bound as pointed out by one of the referees.

PROPOSITION 4.6.1 (Dieulefait[6].). *For $\ell \geq 3$, the image of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *in* $\mathrm{Aut}(A[\ell])$ *is* $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

Proof. Note that C is isomorphic to the curve defined by $y^2 = x^6 - x^3 - x + 1$ and hence by [Die02, Thm. 4.2], the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell \neq 2, 3, 5, 23$. By [BLR90, Ex.9.2.8][7], one finds that [Die02 Prop 5.4] applies. The order of the component group of the Néron-model is $\mathrm{ord}_p(n)$ where n is the resultant of $f(x)$ and $f'(x)$. For $p = 5$ (resp. $p = 23$) this order is 2 (resp. 1). Now we apply [Die02, Thm. 5.4] and we use MAGMA to compute characteristic polynomials of Frobenii for hyperelliptic curves over $\mathbb{Q}$. We first take $p = 5$ and $q = 11$ (resp. $q = 19$). Since the characteristic polynomial of $Frob_q$ is irreducible modulo 3 (resp. 23), we conclude that the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell = 3, 23$. We then take $p = 23$ and $q = 29$ to conclude that the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell = 5$. □

PROPOSITION 4.6.2 (Skorobogatov–Zarhin). *For $\ell \geq 3$, we have*

$$\mathrm{Br}(\overline{A})^\Gamma(\ell) = 0.$$

Proof. It suffices to show that the assumptions of [Sko17, Prop. 4.2] are satisfied when image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$. This follows from $\mathrm{PSp}_4(\mathbb{F}_\ell)$ being a simple non-abelian group of order $> \ell$ as in the argument in Example 1 in *loc. cit.*. □

COROLLARY 4.6.3. *For the Kummer surface $X = \mathrm{Kum}(\mathrm{Jac}(C))$ with C defined by $y^2 = x^6 + x^3 + x + 1$, we have*

$$|\mathrm{Br}(X)/\mathrm{Br}_0(X)| < 2^{10} \cdot 10^{805050}.$$

Proof. By Propositions 4.6.1 and 4.6.2, we have $|\mathrm{Br}(\overline{X})^\Gamma| = |\mathrm{Br}(\overline{A})^\Gamma(2)|$. By Lemma 4.4.7, we have

$$|\mathrm{Br}(\overline{A})^\Gamma(2)| < \prod \ell^{10 v_\ell(\delta)} \cdot (8.7 \times 10^{16100})^{50} < 2^{10} \cdot 10^{805050}.$$

Since $\mathrm{Br}_1(X)/\mathrm{Br}_0(X) = 0$, we conclude that

$$|\mathrm{Br}(X)/\mathrm{Br}_0(X)| \leq |\mathrm{Br}(\overline{X})^\Gamma| < 2^{10} \cdot 10^{805050}.$$

□

[6]The results in [Die02] are stated as conditional upon Serre's modularity conjecture, which is now proved by Khare and Wintenberger [KW09a, KW09b]

[7]Alternatively one may use the SAGE function *genus2reduction*.

REMARK 4.6.4. The above algorithm works for any genus 2 (hyperelliptic) curve over $\mathbb{Q}$. More precisely, we may use Dieulefait's algorithm in [Die02] to find a finite set S such that for any $\ell \notin S$, the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(\mathrm{Jac}(C)[\ell])$ is $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and hence by [Sko17, Prop. 4.2], we conclude that $\mathrm{Br}(\overline{A})^\Gamma(\ell) = 0$ for $\ell \notin S$. Then by Lemma 4.4.7, we have

$$|\operatorname{Br}(X)/\operatorname{Br}_1(X)| < \delta^{2(6-\rho)} \cdot \widetilde{M}^{10(6-\rho)|S|}.$$

Bibliography

[And96] Yves André, *On the Shafarevich and Tate conjectures for hyper-Kähler varieties*, Math. Ann. **305** (1996), no. 2, 205–248. ↑15

[Apo76] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics. ↑16

[Aut13] Pascal Autissier, *Un lemme matriciel effectif*, Math. Z. **273** (2013), no. 1-2, 355–361. ↑123

[AVA18] Dan Abramovich and Anthony Várilly-Alvarado, *Level structures on Abelian varieties, Kodaira dimensions, and Lang's conjecture*, Adv. Math. **329** (2018), 523–540. ↑118

[BBFL07] M. J. Bright, N. Bruin, E. V. Flynn, and A. Logan, *The Brauer-Manin obstruction and Sha[2]*, LMS J. Comput. Math. **10** (2007), 354–377. ↑116

[BHB17] Tim Browning and Roger Heath-Brown, *Forms in many variables and differing degrees*, J. Eur. Math. Soc. (JEMS) **19** (2017), no. 2, 357–394. ↑53, 55

[Bir62] B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. Ser. A **265** (1962), 245–263. ↑27, 28, 29, 30, 52, 53, 54, 76, 90, 91, 93, 110, 111

[BL17] T. D. Browning and D. Loughran, *Sieving rational points on varieties* (2017). preprint available at `https://arxiv.org/abs/1705.01999`. ↑51, 54, 55

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. ↑148

[BM90] V. V. Batyrev and Yu. I. Manin, *Sur le nombre des points rationnels de hauteur borné des variétés algébriques*, Math. Ann. **286** (1990), no. 1-3, 27–43. ↑9

[Bos96] Jean-Benoît Bost, *Périodes et isogenies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz)*, Astérisque **237** (1996), Exp. No. 795, 4, 115–161. Séminaire Bourbaki, Vol. 1994/95. ↑120

[Bou06] N. Bourbaki, *Algèbre commutative Chapitres 1 à 4*, Second, Éléments de mathématique, Springer-Verlag, Berlin Heidelberg, 2006. ↑26

[Bri06] Martin Bright, *Brauer groups of diagonal quartic surfaces*, J. Symbolic Comput. **41** (2006), no. 5, 544–558. ↑34, 116

[Bro09] Timothy D. Browning, *Quantitative arithmetic of projective varieties*, Progress in Mathematics, vol. 277, Birkhäuser Verlag, Basel, 2009. ↑17, 19, 25, 50

[BSD75] B. J. Birch and H. P. F. Swinnerton-Dyer, *The Hasse problem for rational surfaces*, J. Reine Angew. Math. **274/275** (1975), 164–174. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, III. ↑116

[BT95] Victor V. Batyrev and Yuri Tschinkel, *Rational points of bounded height on compactifications of anisotropic tori*, Internat. Math. Res. Notices **12** (1995), 591–635. ↑10

[BT96] ———, *Rational points on some Fano cubic bundles*, C. R. Acad. Sci. Paris Sér. I Math. **323** (1996), no. 1, 41–46. ↑10

[CF16] V. Cantoral-Farfán, *A survey around the Hodge, Tate and Mumford-Tate conjectures for abelian varieties* (2016). preprint available at `https://arxiv.org/abs/1602.08354`. ↑131

[CFTTV16] Victoria Cantoral-Farfán, Yunqing Tang, Sho Tanimoto, and Erik Visse, *Effective bounds for Brauer groups of Kummer surfaces over number fields* (2016). preprint available at `https://arxiv.org/abs/1606.06074`. ↑119

[CFTTV18] ———, *Effective bounds for Brauer groups of Kummer surfaces over number fields*, Journal of the London Mathematical Society **97** (2018), no. 3, 353–376. ↑115

[Cha13] François Charles, *The Tate conjecture for K3 surfaces over finite fields*, Invent. Math. **194** (2013), no. 1, 119–145. ↑15

[Cha14] ———, *On the Picard number of K3 surfaces over number fields*, Algebra Number Theory **8** (2014), no. 1, 1–17. ↑118, 131, 132, 133

[Con16] Brian Conrey, *Statistics of L-functions*, 2016. Analytic Number Theory, Oberwolfach. ↑50

[CTCS80] Jean-Louis Colliot-Thélène, Daniel Coray, and Jean-Jacques Sansuc, *Descente et principe de Hasse pour certaines variétés rationnelles*, J. Reine Angew. Math. **320** (1980), 150–191. ↑116

[CTKS87] Jean-Louis Colliot-Thélène, Dimitri Kanevsky, and Jean-Jacques Sansuc, *Arithmétique des surfaces cubiques diagonales*, Diophantine approximation and transcendence theory (Bonn, 1985), 1987, pp. 1–108. ↑116

[CTS13] Jean-Louis Colliot-Thélène and Alexei N. Skorobogatov, *Good reduction of the Brauer-Manin obstruction*, Trans. Amer. Math. Soc. **365** (2013), no. 2, 579–590. ↑116

[CTSSD87] Jean-Louis Colliot-Thélène, Jean-Jacques Sansuc, and Peter Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces. I*, J. Reine Angew. Math. **373** (1987), 37–107. ↑116

[Dav05] H. Davenport, *Analytic methods for Diophantine equations and Diophantine inequalities*, Second, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2005. With a foreword by R. C. Vaughan, D. R. Heath-Brown and D. E. Freeman, Edited and prepared for publication by T. D. Browning. ↑17, 21

[Die02] Luis V. Dieulefait, *Explicit determination of the images of the Galois representations attached to abelian surfaces with* $\mathrm{End}(A) = \mathbb{Z}$, Experiment. Math. **11** (2002), no. 4, 503–512 (2003). ↑118, 119, 148, 149

[DS18] Kevin Destagnol and Efthymios Sofos, *Prime and square-free values of polynomials in moderately many variables* (2018). preprint available at `https://arxiv.org/abs/1801.03082`. ↑76

[EJ10] Andreas-Stephan Elsenhans and Jörg Jahnel, *On the Brauer-Manin obstruction for cubic surfaces*, J. Comb. Number Theory **2** (2010), no. 2, 107–128. ↑116

[EJ12a] ———, *Kummer surfaces and the computation of the Picard group*, LMS J. Comput. Math. **15** (2012), 84–100. ↑119, 133, 147

[EJ12b] ———, *On the order three Brauer classes for cubic surfaces*, Cent. Eur. J. Math. **10** (2012), no. 3, 903–926. ↑116

[Fal86] Gerd Faltings, *Finiteness theorems for abelian varieties over number fields*, Arithmetic geometry (Storrs, Conn., 1984), 1986, pp. 9–27. Translated from the German original [Invent. Math. **7**3 (1983), no. 3, 349–366; ibid. **7**5 (1984), no. 2, 381; MR 85g:11026ab] by Edward Shipz. ↑120

[FI10] John Friedlander and Henryk Iwaniec, *Opera de cribro*, American Mathematical Society Colloquium Publications, vol. 57, American Mathematical Society, Providence, RI, 2010. ↑66

[FLS18] C. Frei, D. Loughran, and E. Sofos, *Rational points of bounded height on general conic bundle surfaces*, Proc. Lond. Math. Soc. (2018). to appear. ↑53

[FMT89] Jens Franke, Yuri I. Manin, and Yuri Tschinkel, *Rational points of bounded height on Fano varieties*, Invent. Math. **95** (1989), no. 2, 421–435. ↑9

[FS97] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus* 2 *and the infinite descent*, Acta Arith. **79** (1997), no. 4, 333–352. ↑117

[GK17] Andrew Granville and Dimitris Koukoulopoulos, *Beyond the LSD method for the partial sums of multiplicative functions* (2017). preprint available at `https://arxiv.org/abs/1710.01389`. ↑34, 35

[GR14] Éric Gaudron and Gaël Rémond, *Polarisations et isogénies*, Duke Math. J. **163** (2014), no. 11, 2057–2108. ↑120, 122, 123, 124, 125

[HB98] D. R. Heath-Brown, *The circle method and diagonal cubic forms*, R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci. **356** (1998), no. 1738, 673–699. ↑50

[HKT13] Brendan Hassett, Andrew Kresch, and Yuri Tschinkel, *Effective computation of Picard groups and Brauer-Manin obstructions of degree two K3 surfaces over number fields*, Rend. Circ. Mat. Palermo (2) **62** (2013), no. 1, 137–151. ↑116, 117, 118, 139

[Hoo07] Christopher Hooley, *On ternary quadratic forms that represent zero. II*, J. Reine Angew. Math. **602** (2007), 179–225. ↑51

[Hoo93] C. Hooley, *On ternary quadratic forms that represent zero*, Glasgow Math. J. **35** (1993), no. 1, 13–23. ↑51, 93

[HS16] Yonatan Harpaz and Alexei N. Skorobogatov, *Hasse principle for Kummer varieties*, Algebra Number Theory **10** (2016), no. 4, 813–841. ↑116

[Huy16] Daniel Huybrechts, *Lectures on K3 surfaces*, Cambridge Studies in Advanced Mathematics, vol. 158, Cambridge University Press, Cambridge, 2016. ↑8

[HVA13] Brendan Hassett and Anthony Várilly-Alvarado, *Failure of the Hasse principle on general K3 surfaces*, J. Inst. Math. Jussieu **12** (2013), no. 4, 853–877. ↑116

[HVAV11] Brendan Hassett, Anthony Várilly-Alvarado, and Patrick Varilly, *Transcendental obstructions to weak approximation on general K3 surfaces*, Adv. Math. **228** (2011), no. 3, 1377–1404. ↑116

[IK04] Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. ↑6, 15, 16, 17, 38, 40

[IS15] Evis Ieronymou and Alexei N. Skorobogatov, *Odd order Brauer-Manin obstruction on diagonal quartic surfaces*, Adv. Math. **270** (2015), 181–205. ↑116

[ISZ11] Evis Ieronymou, Alexei N. Skorobogatov, and Yuri G. Zarhin, *On the Brauer group of diagonal quartic surfaces*, J. Lond. Math. Soc. (2) **83** (2011), no. 3, 659–672. With an appendix by Peter Swinnerton-Dyer. ↑116

[Kau99] Ivan Kausz, *A discriminant and an upper bound for ω^2 for hyperelliptic arithmetic surfaces*, Compositio Math. **115** (1999), no. 1, 37–69. ↑121

[KMP16] Wansu Kim and Keerthi Madapusi Pera, *2-adic integral canonical models*, Forum Math. Sigma **4** (2016), e28, 34. ↑15

[KT04] Andrew Kresch and Yuri Tschinkel, *On the arithmetic of del Pezzo surfaces of degree 2*, Proc. London Math. Soc. (3) **89** (2004), no. 3, 545–569. ↑116

[KT08] ———, *Effectivity of Brauer-Manin obstructions*, Adv. Math. **218** (2008), no. 1, 1–27. ↑116

[KT11] ———, *Effectivity of Brauer-Manin obstructions on surfaces*, Adv. Math. **226** (2011), no. 5, 4131–4144. ↑116

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. ↑148

[KW09b] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586. ↑148

[Liv95] Ron Livné, *Motivic orthogonal two-dimensional representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Israel J. Math. **92** (1995), no. 1-3, 149–156. ↑14

[LLR05] Qing Liu, Dino Lorenzini, and Michel Raynaud, *On the Brauer group of a surface*, Invent. Math. **159** (2005), no. 3, 673–676. ↑132

[Log08] Adam Logan, *The Brauer-Manin obstruction on del Pezzo surfaces of degree 2 branched along a plane section of a Kummer surface*, Math. Proc. Cambridge Philos. Soc. **144** (2008), no. 3, 603–622. ↑116

[Lou13] D. Loughran, *The number of varieties in a family which contain a rational point*, J. Eur. Math. Soc. (2013). to appear, preprint available at `https://arxiv.org/abs/1310.6219`. ↑11, 51, 52, 108, 109

[LP80] Eduard Looijenga and Chris Peters, *Torelli theorems for Kähler K3 surfaces*, Compositio Math. **42** (1980/81), no. 2, 145–186. ↑135, 136, 144

[LS16] D. Loughran and A. Smeets, *Fibrations with few rational points*, Geom. Funct. Anal. **26** (2016), no. 5, 1449–1482. ↑51, 52, 55

[LST18] Brian Lehmann, Akash Kumar Sengupta, and Sho Tanimoto, *Geometric consistency of Manin's Conjecture* (2018). preprint available at `https://arxiv.org/abs/1805.10580`. ↑10

[LT18] Brian Lehmann and Sho Tanimoto, *On exceptinal sets in Manin's Conjecture* (2018). preprint available at `https://arxiv.org/abs/1807.07995`. ↑10

[LTBT17] D. Loughran, R. Takloo-Bighash, and S. Tanimoto, *Zero-loci of Brauer group elements on semi-simple algebraic groups* (2017). preprint available at `https://arxiv.org/abs/1705.09244`. ↑51, 52

[Lui] R.M. van Luijk. data available at `http://pub.math.leidenuniv.nl/~luijkrmvan/maninK3/`. ↑9, 34

[LvL09] Adam Logan and Ronald van Luijk, *Nontrivial elements of Sha explained through K3 surfaces*, Math. Comp. **78** (2009), no. 265, 441–483. ↑116

[Man71] Y. I. Manin, *Le groupe de Brauer-Grothendieck en géométrie diophantienne* (1971), 401–411. ↑116

[Man86] Yu. I. Manin, *Cubic forms*, Second, North-Holland Mathematical Library, vol. 4, North-Holland Publishing Co., Amsterdam, 1986. Algebra, geometry, arithmetic, Translated from the Russian by M. Hazewinkel. ↑116

[Mau14] Davesh Maulik, *Supersingular K3 surfaces for large primes*, Duke Math. J. **163** (2014), no. 13, 2357–2425. With an appendix by Andrew Snowden. ↑15

[McK11] David McKinnon, *Vojta's conjecture implies the Batyrev-Manin conjecture for K3 surfaces*, Bull. Lond. Math. Soc. **43** (2011), no. 6, 1111–1118. ↑9

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533. ↑132

[MP15] Keerthi Madapusi Pera, *The Tate conjecture for K3 surfaces in odd characteristic*, Invent. Math. **201** (2015), no. 2, 625–668. ↑15

[MSTVA17] Kelly McKinnie, Justin Sawon, Sho Tanimoto, and Anthony Várilly-Alvarado, *Brauer groups on K3 surfaces and arithmetic applications*, Brauer groups and obstruction problems, 2017, pp. 177–218. ↑116

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970. ↑122, 131

[MV07] Hugh L. Montgomery and Robert C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007. ↑6, 16, 31

[MW95] D. W. Masser and G. Wüstholz, *Refinements of the Tate conjecture for abelian varieties*, Abelian varieties (Egloffstein, 1993), 1995, pp. 211–223. ↑120, 128

[New16] Rachel Newton, *Transcendental Brauer groups of products of CM elliptic curves*, J. Lond. Math. Soc. (2) **93** (2016), no. 2, 397–419. ↑138

[Nik79] V. V. Nikulin, *Integer symmetric bilinear forms and some of their geometric applications*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 1, 111–177, 238. ↑134, 136, 137

[NO85] Niels Nygaard and Arthur Ogus, *Tate's conjecture for $K3$ surfaces of finite height*, Ann. of Math. (2) **122** (1985), no. 3, 461–507. ↑15

[Odo73] R. W. K. Odoni, *The Farey density of norm subgroups of global fields. I*, Mathematika **20** (1973), 155–169. ↑55

[Ogu82] A. Ogus, *Hodge cycles and crystalline cohomology*, Hodge cycles, motives, and Shimura varieties, 1982. ↑131

[Paz12] Fabien Pazuki, *Theta height and Faltings height*, Bull. Soc. Math. France **140** (2012), no. 1, 19–49. ↑120

[Paz14] F. Pazuki, *Décompositions en hauteurs locales* (2014). preprint available at `https://arxiv.org/abs/1205.4525`. ↑120, 121

[Pey17] Emmanuel Peyre, *Liberté et accumulation*, Doc. Math. **22** (2017), 1615–1659. ↑10

[Pey18] ———, *Beyond heights: slopes and distribution of rational points* (2018). preprint available at `https://arxiv.org/abs/1806.11437`. ↑10

[Pey95] ———, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), no. 1, 101–218. ↑9, 10

[PSD91] R. G. E. Pinch and H. P. F. Swinnerton-Dyer, *Arithmetic of diagonal quartic surfaces. I*, L-functions and arithmetic (Durham, 1989), 1991, pp. 317–338. ↑14

[PT01] Emmanuel Peyre and Yuri Tschinkel, *Tamagawa numbers of diagonal cubic surfaces, numerical evidence*, Math. Comp. **70** (2001), no. 233, 367–387. ↑109

[PTvL15] Bjorn Poonen, Damiano Testa, and Ronald van Luijk, *Computing Néron-Severi groups and cycle class groups*, Compos. Math. **151** (2015), no. 4, 713–734. ↑116, 118, 130

[PV04] Bjorn Poonen and José Felipe Voloch, *Random Diophantine equations*, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), 2004, pp. 175–184. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz. ↑51

[Rie65] G. J. Rieger, *über die Anzahl der als Summe von zwei Quadraten darstellbaren und in einer primen Restklasse gelegenen Zahlen unterhalb einer positiven Schranke. II*, J. Reine Angew. Math. **217** (1965), 200–216. ↑63

[Rud14] Céline Le Rudulier, *Point algébriques de hauteur bornée*, 2014. PhD thesis, Université de Rennes 1. ↑10

[Sal98] Per Salberger, *Tamagawa measures on universal torsors and points of bounded height on Fano varieties*, Astérisque **251** (1998), 91–258. Nombre et répartition de points de hauteur bornée (Paris, 1996). ↑11

[SD00] Peter Swinnerton-Dyer, *Arithmetic of diagonal quartic surfaces. II*, Proc. London Math. Soc. (3) **80** (2000), no. 3, 513–544. ↑34

[SD93] ———, *The Brauer group of cubic surfaces*, Math. Proc. Cambridge Philos. Soc. **113** (1993), no. 3, 449–460. ↑116

[SD99] ———, *Brauer-Manin obstructions on some Del Pezzo surfaces*, Math. Proc. Cambridge Philos. Soc. **125** (1999), no. 2, 193–198. ↑116

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7. ↑62, 108

[Ser90] Jean-Pierre Serre, *Spécialisation des éléments de* $\mathrm{Br}_2(\mathbf{Q}(T_1, \cdots, T_n))$, C. R. Acad. Sci. Paris Sér. I Math. **311** (1990), no. 7, 397–402. ↑51

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, Third, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre. ↑10

[Sha08] William Shakespeare, *Complete works*, The RSC Shakespeare, Red Globe Press, Basingstoke, 2008. Edited by Jonathan Bate and Eric Rasmussen. ↑

[Sil92] A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, J. Pure Appl. Algebra **77** (1992), no. 3, 253–262. ↑123

[Sko17] A. N. Skorobogatov, *Kummer varieties and their Brauer groups* (2017). preprint available at `https://arxiv.org/abs/1612.05993`. ↑118, 119, 148, 149

[Sof16] E. Sofos, *Serre's problem on the density of isotropic fibres in conic bundles*, Proc. Lond. Math. Soc. (3) **113** (2016), no. 2, 261–288. ↑51

[SVM18] Efthymios Sofos and Erik Visse-Martindale, *The density of fibres with a rational point for a fibration over hypersurfaces of low degree* (2018). preprint available at `https://arxiv.org/abs/1804.05768`. ↑51

[SZ08] Alexei N. Skorobogatov and Yuri G. Zarhin, *A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces*, J. Algebraic Geom. **17** (2008), no. 3, 481–502. ↑11, 116, 118, 139, 141

[SZ12] ———, *The Brauer group of Kummer surfaces and torsion of elliptic curves*, J. Reine Angew. Math. **666** (2012), 115–140. ↑117, 118, 138

[SZ14] ———, *The Brauer group and the Brauer-Manin set of products of varieties*, J. Eur. Math. Soc. (JEMS) **16** (2014), no. 4, 749–768. MR3191975 ↑116

[Tan88] S. G. Tankeev, *Surfaces of type K3 over number fields, and l-adic representations*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6, 1252–1271, 1328. ↑15

[Tat65] John T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 1965, pp. 93–110. ↑15

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. ↑132

[Ten95] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995. Translated from the second French edition (1995) by C. B. Thomas. ↑56, 62

[TVA16] S. Tanimoto and A. Várilly-Alvarado, *Kodaira dimension of moduli of special cubic fourfolds*, J. Reine Angew. Math. (2016). to appear. ↑118

[VA08] Anthony Várilly-Alvarado, *Weak approximation on del Pezzo surfaces of degree 1*, Adv. Math. **219** (2008), no. 6, 2123–2145. ↑116

[VA17] ———, *Arithmetic of K3 surfaces*, Geometry over nonclosed fields, 2017, pp. 197–248. ↑118

[VAV17] Anthony Várilly-Alvarado and Bianca Viray, *Abelian n-division fields of elliptic curves and Brauer groups of product Kummer & abelian surfaces*, Forum Math. Sigma **5** (2017), e26, 42. ↑119

[VW95] R. C. Vaughan and T. D. Wooley, *On a certain nonary cubic form and related equations*, Duke Math. J. **80** (1995), no. 3, 669–735. ↑50

[Wir61] Eduard Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102. ↑34

[Wit16] Olivier Wittenberg, *Rational points and zero-cycles on rationally connected varieties over number fields* (2016). preprint available at `https://arxiv.org/abs/1604.08543`. ↑116

Summary

Here's the scroll,
The continent and summary of my fortune

Bassanio, The Merchant of Venice, Scene 3.2, lines 132-133

This PhD thesis concerns the topic of 'arithmetic geometry', that is, the interplay between arithmetic on the one hand – integer numbers, their addition and multiplication, and their fractions – and geometry on the other – shapes and their intersections. We address three different questions and each of the questions in some way is about counting how big some set is or can be.

In arithmetic geometry we are interested in so called *polynomial* equations: we restrict ourselves to only use fractions of integers and any number of indeterminates – sometimes also called variables – and the rules we may use are just addition, multiplication, and exponentiation with positive integer powers. That means no square roots, logarithms, or trigonometric functions for example. That may feel like a relief (we may forget half of our secondary school mathematics), but the questions that arise turn out to be surprisingly difficult. Some of them date back at least to the ancient Greeks, if not further!

So what *are* the questions that we want to study? Take for example the equation

$$x^2 + y^2 = 1. \tag{5.1}$$

You may remember from that half of secondary school mathematics that we did not forget in the last paragraph that this is the equation of a circle in a plane. In other words: if we label our axes x and y and we draw all the points in the plane that have x- and y-coordinates which satisfy the equation, our drawing will take the shape of a circle. This is where we see the geometry appear naturally. How about the arithmetic? Well, we cannot individually draw *all* the points on a circle – there are simply too many of them. Let us separate them into two sets. One set, which we will

call S, will contain all those points whose coordinates x and y are fractions of integer numbers, for example $(1, 0)$ lies in S, and so does $(\frac{3}{5}, \frac{4}{5})$. The other set will contain all the other points, for example $(\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{2})$, and we will ignore it. Now the set S is still infinite, but let us impose a further restriction on its elements. What if we don't take all possible fractions, but we only use those whose numerator and denominator are small, let's say less than some number B that we may freely choose? This set is finite so we can count the number N of elements of this set, which depends on what we choose for B.

Question 1: How exactly does this number N depend on B?

In this case the answer is not too difficult to find and it turns out to be a linear function in B. But if we replace equation (5.1) by a more difficult equation, say

$$x^4 + y^4 - 3z^4 = 1, \tag{5.2}$$

then the question has become a whole lot more difficult. With the extra variable z, the dimension of the corresponding geometric object is raised to two (whereas the circle has dimension one), and with the higher exponent 4, the shapes get more complicated. For equations of this new shape, no definitive answer has been proven to date. In Chapter 2 we give evidence (which is not synonymous to 'proof') that the answer should be some explicit power of $\log B$. Indeed, to understand the answer, we need to relearn about logarithms!

Chapter 3 deals with a similar question, and to explain this question, we need to learn about modular arithmetic. In essence, this is arithmetic like on a clock: every 12 hours the time on the clock is repeated. How can we phrase this in mathematics? On the clock we know that 13 equals 1, 14 equals 2 and so on. Mathematically we equate a number with its remainder upon division by 12. Indeed, we have $13 = 1 \times 12 + 1$, and $14 = 1 \times 12 + 2$, and so on. There is no need to stop at 24: we also have $35 = 2 \times 12 + 11$, so we equate 35 with 11. Moreover, mathematically there is nothing special about the number 12. We could imagine a clock with any number of 'hours'.

We now replace (5.1) by a different equation than before. For example we may also look at the ellipse whose equation is

$$x^2 + 3y^2 = 2. \tag{5.3}$$

Using the modular arithmetic just introduced, it is not hard to prove that

this equation has no solutions where x and y are fractions of integers. Equations (5.1) and (5.3) are very similar, in fact we can write down a *family* of equations of which both are a member. In this case, equations (5.1) and (5.3) are both members of the family defined by

$$x^2 + (1 + 2t)y^2 = 1 + t. \tag{5.4}$$

We get members of this family when we choose values for the parameter t. For example, if we set $t = 0$ then we recover equation (5.1), and for $t = 1$ we obtain equation (5.3).

Question 2: Given some family, can we count how many of its members have fractional solutions?

This number could be infinite, so we need our question to be phrased more carefully. For example, we may restrict ourselves to members with a t that is a fraction of integers not exceeding some number B. Again we are confronted with a question that can be described in simple terms, and again the answer is quite difficult to prove. In fact, there are reasons to believe that there exists some deeper meaning that covers the answers to Questions 1 and 2, but we seem quite far from understanding this meaning. In Chapter 3 we look at families of some prescribed shape and we answer this counting question in full. Like in Chapter 2, the answer depends on B and we find a formula for the number that we wanted to count. There are two noteworthy observations about this: in the literature such formulas are quite rare – normally one is only able to give upper bounds – and the formula involves a complicated constant that we have unravelled. The way that this constant is built up provides further evidence for the deeper meaning that we alluded to above.

Equation (5.3) has no fractional solutions because of problems arising from modular arithmetic. One may wonder if these are the only problems that may occur, and this is exactly what Yuri Manin did in the 1970's. He gave a construction that may explain the existence of *obstructions* to fractional solutions; this construction involves a set that we call the *Brauer group*. For many simple geometric objects, Manin's construction accounts for all obstructions, but this need not always be the case. Recall the equations of the shape (5.2) that we studied in Chapter 2. Their geometric objects are examples of what we call K3 surfaces. In recent years people have started to wonder if Manin's construction is strong enough to explain all obstructions to fractional solutions for K3 surfaces, and this question remains open. In order to work towards an answer, we studied these

Brauer groups for some type of K3 surfaces in Chapter 4. It is known for K3 surfaces that Brauer groups only have finitely many elements, but the theorem that shows this does not tell us how many.

Question 3: How big can a Brauer group of a K3 surface get?

Our result gives a recipe that takes as ingredients only a few basic numerical values attached to the surface whose Brauer group one wants to study. However, our method does not give the exact answer but only an upper bound. We were not the first ones to give such upper bounds, but our result has the benefit of being easy to compute. There is, however, no reason to assume that our upper bounds are in any way *sharp*, which means that these upper bounds may be far above the actual size.

In conclusion, the title of this thesis goes against the main strength of mathematics: to describe complex phenomena with no room for ambiguity. The title can be separated in two different ways. Reading it as "Counting points on (K3 surfaces and other arithmetic-geometric objects)" emphasizes that in each chapter we focus on counting some quantities, while reading it as "(Counting points on K3 surfaces) and other arithmetic-geometric objects" shows that we are mainly interested in K3 surfaces, but that the thesis also contains other results. In this case the ambiguity does not hurt: both readings are correct.

Nederlandse samenvatting

Hier is de rol papier,
de inhoud en de optelsom van mijn fortuin

Bassanio, De Koopman van Venetië, Scene 3.2, regels 132-133

Dit proefschrift valt in het vakgebied van de 'aritmetische meetkunde', dat is het samenspel van aritmetiek, in het Nederlands ookwel rekenkunde, aan de ene kant – gehele getallen, hun optelling en vermenigvuldiging, en hun breuken – en meetkunde aan de andere – vormen en hun doorsnijdingen. We beschouwen drie verschillende vragen en in elk van deze vragen zijn we op enige manier geïnteresseerd in het tellen van hoe groot een zekere verzameling kan zijn.

In de aritmetische meetkunde zijn we geïnteresseerd in zogenaamde *polynomiale* vergelijkingen: we beperken onszelf tot breuken van gehele getallen en een willekeurig aantal variabelen. De operaties die we mogen toepassen zijn slechts optelling, vermenigvuldiging, en machtsverheffen met positieve gehele machten. Dat betekent dus geen vierkantswortels, logaritmes, of trigonometrische functies. Dat voelt misschien als een opluchting (we mogen immers de helft van onze schoolwiskunde vergeten), maar de vragen die opkomen blijken verrassend moeilijk te zijn. Sommige daarvan dateren in ieder geval terug tot de oude Grieken, zo niet verder!

Wat zijn dan de vragen die we willen bestuderen? Neem bijvoorbeeld de vergelijking

$$x^2 + y^2 = 1. \tag{5.1}$$

Misschien weet u nog wel van dat deel van de schoolwiskunde dat we niet zojuist vergeten zijn dat dit de vergelijking is van een cirkel in het platte vlak. In andere woorden: als we onze assen x en y noemen, en we tekenen alle punten in het vlak die x- en y-coördinaten hebben die aan de vergelijking voldoen, dan neemt onze tekening de vorm van een cirkel aan. Dit is waar de meetkunde natuurlijkerwijs naar voren komt. Hoe zit dat met de rekenkunde? Nou, we kunnen niet *alle* punten van de cirkel

individueel tekenen – dat zijn er simpelweg te veel. Laten we ze in twee verzamelingen opsplitsen. Een verzameling, die we S zullen noemen, geven we alle punten waarvan de coördinaten x en y breuken van gehele getallen zijn. Bijvoorbeeld $(0, 1)$ ligt in S en zo ook $(\frac{3}{5}, \frac{4}{5})$. De andere verzameling geven we alle andere punten, bijvoorbeeld $(\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{2})$; deze zullen we negeren. De verzameling S is nog steeds oneindig groot, dus laten we ons verder beperken. Wat als we niet alle mogelijke breuken toelaten, maar alleen die waarvan de teller en de noemer klein zijn, zeg kleiner dan een getal B dat we vrij mogen kiezen? Deze nieuwe verzameling is wel eindig, dus we kunnen het aantal elementen N tellen, welke zal afhangen van wat we kiezen voor B.

Vraag 1: Hoe hangt dit getal N precies van B af?

In dit geval is het niet al te ingewikkeld om het antwoord te vinden en het blijkt een lineaire functie in B te zijn. Maar als we vergelijking (5.1) vervangen door een ingewikkeldere vergelijking, zeg

$$x^4 + y^4 - 3z^4 = 1, \tag{5.2}$$

dan wordt de vraag een stuk moeilijker. Met de extra variabele z wordt de dimensie van het corresponderende meetkundige object verhoogd naar twee (terwijl de cirkel dimensie één heeft), en met de hogere exponent 4 worden de vormen ingewikkelder. Voor vergelijkingen van deze vorm bestaat er tot nog toe geen bewezen antwoord. In Hoofdstuk 2 geven we bewijsmateriaal (hetgeen niet synoniem is aan 'bewijs') dat laat zien dat het antwoord een zekere expliciete macht van $\log B$ zou moeten zijn. Dus om het antwoord te begrijpen, moeten we opnieuw over logaritmes leren!

Hoofdstuk 3 behandelt een gelijksoortige vraag, en om deze vraag te begrijpen, moeten we iets leren over modulaire rekenkunde. In essentie is dat rekenkunde zoals op een klok: iedere 12 uur wordt de tijd op de klok herhaald. Hoe kunnen we dit in wiskunde vertalen? Op de klok weten we dat 13 gelijk is aan 1, 14 aan 2, enzovoorts. Wiskundig gezien stellen we een getal gelijk aan zijn rest bij deling door 12. We hebben $13 = 1 \times 12 + 1$, en $14 = 1 \times 12 + 2$ en zo verder. Er is geen reden om te stoppen bij 24: we hebben ook $35 = 2 \times 12 + 11$, dus we stellen 35 en 11 gelijk. Bovendien is er wiskundig niets speciaals aan het getal 12. We zouden ons een klok kunnen voorstellen met ieder willekeurig aantal 'uren'.

Nu vervangen we (5.1) door een andere vergelijking dan eerst. Bijvoor-

beeld kunnen we ook kijken naar de ellips met de vergelijking

$$x^2 + 3y^2 = 2. \tag{5.3}$$

Met behulp van de modulaire rekenkunde die we zojuist geïntroduceerd hebben, is het niet zo moeilijk om aan te tonen dat deze vergelijking geen oplossingen heeft waarbij x en y breuken zijn. Vergelijkingen (5.1) en (5.3) lijken heel veel op elkaar, en we kunnen een *familie* van vergelijkingen opschrijven waarvan beide lid zijn. In dit geval zijn beide vergelijkingen lid van de familie die gedefinieerd wordt door

$$x^2 + (1 + 2t)y^2 = 1 + t. \tag{5.4}$$

Wanneer we waarden voor de parameter t kiezen, krijgen we de leden van deze familie. Als we bijvoorbeeld $t = 0$ kiezen, dan herontdekken we vergelijking (5.1), en voor $t = 1$ vinden we vergelijking (5.3) terug.

Vraag 2: Gegeven een zekere familie, kunnen we het aantal leden tellen dat een oplossing in breuken heeft?

Dit aantal zou oneindig kunnen zijn, dus we moeten onze vraag voorzichtiger stellen. Bijvoorbeeld kunnen we ons beperken tot alleen die leden die horen bij een t die zelf een breuk is waarvan de teller en de noemer niet groter zijn dan een zekere grenswaarde B. Nu worden we weer geconfronteerd met een vraag die in eenvoudige termen te beschrijven is, en weer blijkt het antwoord lastig te bewijzen. Er zijn zelfs goede redenen om te geloven dat er een onderliggend dieper verband is tussen de antwoorden van Vragen 1 en 2, maar begrip hiervan lijkt nog vrij ver weg te zijn. In Hoofdstuk 3 kijken we naar families van een zekere voorgeschreven vorm en beantwoorden we deze telvraag in zijn geheel: we geven een formule voor het aantal dat we wilden tellen. Er zijn twee belangrijke observaties hierbij: in de literatuur zijn zulke formules zeldzaam – normaal kan men slechts bovengrenzen geven – en de formule omvat een ingewikkelde constante die we hebben ontrafeld. De wijze waarop deze constante is opgebouwd voorziet ons van verder bewijsmateriaal voor het diepere verband waarop we hierboven al zinspeelden.

Vergelijking (5.3) heeft geen oplossingen in breuken wegens problemen die uit de modulaire rekenkunde komen. Men zou zich kunnen afvragen of dit de enige problemen zijn die kunnen voorkomen, en dit is precies wat Yuri Manin deed in de jaren '70 van de vorige eeuw. Hij beschreef een constructie die het bestaan van *obstructies* tot oplossingen in breuken kan

verklaren; deze constructie maakt gebruik van een verzameling die we de *Brauergroep* noemen. Voor veel simpele meetkundige objecten worden al zulke obstructies verklaard door de constructie van Manin, maar dit hoeft niet altijd het geval te zijn. Laten we terugkijken naar vergelijkingen van de vorm (5.2) die we in Hoofdstuk 2 bestudeerd hebben. Hun meetkundige objecten zijn voorbeelden van wat we K3-oppervlakken noemen. Recent zijn onderzoekers begonnen zich af te vragen of de constructie van Manin sterk genoeg is om alle obstructies tot oplossingen in breuken voor K3-oppervlakken te verklaren, en deze vraag is nog onbeantwoord. Om richting een antwoord te werken, bestuderen we deze Brauergroepen voor een bepaald type K3-oppervlakken in Hoofdstuk 4. Het is bekend dat Brauergroepen van K3-oppervlakken slechts eindig veel elementen kunnen hebben, maar de stelling die dit laat zien zegt niets over het precieze aantal.

Vraag 3: Hoe groot kan de Brauergroep van een K3-oppervlak zijn?

Ons resultaat geeft een recept dat als ingrediënten slechts een aantal basale waardes heeft die gemoeid zijn met het oppervlak waarvan men de Brauergroep wil bestuderen. Onze methode geeft desalniettemin geen exact antwoord, maar slechts een bovengrens. Wij zijn niet de eersten die zo'n bovengrens geven, maar ons resultaat heeft het voordeel dat het gemakkelijk is uit te rekenen. Er is daarentegen geen enkele reden om aan te nemen dat onze bovengrens op enige wijze *scherp* is, hetgeen betekent dat deze bovengrenzen ver boven de werkelijke waarde kunnen liggen.

Ter afsluiting, de titel van dit proefschrift gaat in tegen de grootste kracht van de wiskunde: het beschrijven van complexe fenomenen zonder ruimte voor dubbelzinnigheid. De titel, vertaald naar het Nederlands, kan op twee manieren opgedeeld worden. Een lezing als "Het tellen van punten op (K3-oppervlakken en andere rekenkundig-meetkundige objecten)" benadrukt dat we in elk hoofdstuk ons richten op het tellen van zekere hoeveelheden, terwijl een lezing als "(Het tellen van punten op K3-oppervlakken) en andere rekenkundig-meetkundige objecten" juist naar voren brengt dat we in eerste instantie geïnteresseerd zijn in K3-oppervlakken, maar dat dit proefschrift ook andere resultaten bevat. In dit geval schaadt de dubbelzinnigheid niet: beide manieren van lezen zijn correct.

Acknowledgements

I thank thee, gentle Percy; and be sure
I count myself in nothing else so happy
As in a soul rememb'ring my good friends

Bullingbrook, RICHARD II, Scene 2.3, lines 46-48

First of all, I want to thank Ronald for his excellent guidance and supervision over the past few years. Your constant positive outlook is greatly appreciated, and our heart to heart conversations during my moments of doubt have been, and still are, very valuable to me. I am happy that we were able to disagree sometimes. I vividly remember when I laid out my very optimistic plans for a difficult talk, that you only told me: "I guess this can only be done by someone who assisted in a presentation course for three years." This is only one example of how you have always trusted my abilities, and that trust is highly valued.

I also want to thank Peter for his help, in particular for reminding me how to write Dutch properly, and for de-Anglicizing attached propositions.

I appreciate the effort that the members of the thesis committee have taken. Not every line in the thesis is insightful, and not every calculation interesting. I am glad that you soldiered on and offered some helpful suggestions for improvement.

I would like to thank my wife, former colleague, and former office mate for supporting me every step of the way, and for finding the right words in which to express this thought. Since I have known you, you have inspired me personally and scientifically. I am a more complete person with you beside me.

I believe the mathematical department contains (now and in the past) a lot of wonderful people, of whom I would like to mention a few in particular. Thanks to Owen for making sure that we really taught the course on commutative algebra together, and for probing my understanding of my native language. Ik mis de lunchgesprekken over moeilijke Nederlandse

woorden nog vaak. Thanks to Martin for your patient help with lots of little questions, both of a mathematical and a linguistic nature. Thank you – and the other organizers – for the conference on Schiermonnikoog; that week has a special place in my academic career. Thanks to Bas for your help in setting up the Shimura varieties course and for having the Friday afternoon wine meetings in your office. Thanks to Hans for helping me take some of my first mathematical steps and for encouraging me to look past the course material. Thanks to David for continuing to be one of the young people, even though your job title says that you could easily be one of the grown ups now. Thanks to Rachel for keeping a close interest in my progress even after you left Leiden. Thanks to Efthymios for not only teaching me so very much, but also for your, let's say, lively contributions to the culture in the department. Moreover, I feel privileged for having been able to also have serious non-mathematical conversations with you. Thanks to Lenny for being an alround inspiring mathematician and for teaching me how to think throughout several amazing courses.

Over the years, my journey of working towards a PhD knew many people who partook in the same quest. I would like to especially acknowledge the contributions of joy made by Abtien, Anna, Christophe, Djordjo, Garnet, Giulio, Julian, Mima, Raymond, Richard, Rosa, Steven, and Wouter. To Wouter also thanks for the extended journey that started all the way back in 2007 when we were just fresh out of secondary school. Julian and Rosa, our small mathematical family sometimes almost feels like a real one.

Thanks to Hanneke, Kathelijne, Laura en Marianne for their valuable help with all kinds of practicalities.

Also thanks to Nel for the little conversations in the cafetaria. A human touch is vital for a place where people mostly work behind their computers.

Of my non-mathematical friends I want to mention Jens especially, who has always been an examplary scientist to me: you have phenomenal passion for your subject, but you also go actively out of your way to help people in need and to remove prejudice.

Of course, I cannot write this thesis without thanking my family for supporting my every decision leading up to this point.

Curriculum Vitae

> All the world's a stage,
> And all the men and women merely players
>
> Jaques, As You Like It, Scene 2.7, lines 142-143

Erik Visse was born in Zoetermeer on 2nd August 1989. In 2007 he obtained his secondary school gymnasium level diploma at Erasmus College Zoetermeer. Afterwards, he started studying physics at Leiden University. Here he was active in the Rino foundation, giving physics demonstrations at secondary schools. In his first year, he realized the joy that mathematics can bring and he decided to pursue a degree in mathematics to accompany the one in physics. Before he obtained both bachelor degrees in 2012, it had become apparent that mathematics surpassed his initial field of study in his level of interest. In 2014 he obtained his masters degree in mathematics, also in Leiden, having written a thesis in number theory under the supervision of Rachel Newton and David Holmes. Soon after, he started the PhD project that culminated in this thesis.

In recent years, Erik discovered the joy of theatre when he joined the student theatre society Cuculum, and afterwards the theatre society Solon in Utrecht. The works of Shakespeare in particular are of great interest to him.

In 2018, in the midst of finishing this PhD thesis, Erik got married to Chloe Martindale whom he had met through mathematics. He adopted her surname which now proudly and justly features on the cover of this thesis.