Universiteit
Leiden
The Netherlands

Counting points on K3 surfaces and other arithmetic-geometric objects

Visse, H.D.

Citation

Visse, H. D. (2018, December 18). *Counting points on K3 surfaces and other arithmetic-geometric objects*. Retrieved from https://hdl.handle.net/1887/67532

Version:	Not Applicable (or Unknown)
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/67532

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

The handle http://hdl.handle.net/1887/67532 holds various files of this Leiden University dissertation.

Author: Visse, H.D.
Title: Counting points on K3 surfaces and other arithmetic-geometric objects
Issue Date: 2018-12-18

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.

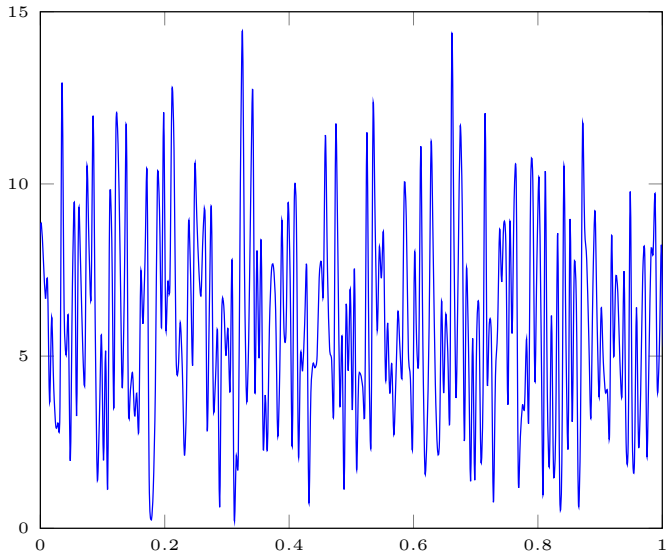

Figure 1.1: Plot of the modulus $\left|\sum_{x\in\mathbb{Z}\cap[-10,10]} e(\alpha x^4)\right|$ for $\alpha \in [0,1]$.

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]. □