Thesis for the degree of Doctor of Philosophy

Counting solutions to Diophantine equations

Oscar Marmon

Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg
Gothenburg, Sweden 2010

Counting solutions to Diophantine equations
OSCAR MARMON
ISBN 978-91-7385-402-3

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr 3083
ISSN 0346-718X

Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Sweden
Telephone: +46 (0)31-772 1000

Printed in Gothenburg, Sweden 2010

Counting solutions to Diophantine equations

OSCAR MARMON
Department of Mathematical Sciences
Chalmers University of Technology and University of Gothenburg

Abstract

This thesis presents various results concerning the density of rational and integral points on algebraic varieties. These results are proven with methods from analytic number theory as well as algebraic geometry.

Using exponential sums in several variables over finite fields, we prove upper bounds for the number of integral points of bounded height on an affine variety. More precisely, our method is a generalization of a technique due to Heath-Brown — a multi-dimensional version of van der Corput's *AB*-process. It yields new estimates for complete intersections of r hypersurfaces of degree at least three in $\mathbb{A}^n$, as well as for hypersurfaces in $\mathbb{A}^n$ of degree at least four.

We also study the so called determinant method, introduced by Bombieri and Pila to count integral points on curves. We show how their approach may be extended to higher-dimensional varieties to yield an alternative proof of Heath-Brown's Theorem 14, avoiding p-adic considerations.

Moreover, we use the determinant method to study the number of representations of integers by diagonal forms in four variables. Heath-Brown recently developed a new variant of the determinant method, adapted to counting points *near* algebraic varieties. Extending his ideas, we prove new upper bounds for the number of representations of an integer by a diagonal form in four variables of degree $k \geq 8$. Furthermore, we use a refined version of the determinant method for affine surfaces, due to Salberger, to derive new estimates for the number of representations of a positive integer as a sum of four k-th powers of positive integers, improving upon estimates by Wisdom.

Keywords. Integral points, rational points, counting function, exponential sums, Weyl differencing, van der Corput's method, determinant method, sum of k-th powers.

Papers in this thesis

Paper I

Oscar Marmon. The density of integral points on complete intersections. *Q. J. Math.* **59** (2008), 29–53. With an appendix by Per Salberger.

Paper II

Oscar Marmon. The density of integral points on hypersurfaces of degree at least four. *Acta Arith.* **141** (2010), 211–240.

Paper III

Oscar Marmon. A generalization of the Bombieri-Pila determinant method. To appear in *Proceedings of the HIM Trimester Program on Diophantine Equations, Bonn 2009*.

Paper IV

Oscar Marmon. Sums and differences of four k-th powers. *Preprint.*

Acknowledgements

I wish to thank my supervisor Per Salberger, who found a good starting point for my research, and who has provided invaluable help and insightful guidance during these five years. I am also grateful to Pär Kurlberg, my co-supervisor, for introducing me to analytic number theory.

I am grateful to the Department of Mathematical Sciences at Chalmers University of Technology and University of Gothenburg — it has been a privilege to conduct doctoral studies here. I also want to thank my (former and present) fellow doctoral students, whose company I have enjoyed during this time: Leif, Kenny, Elizabeth, Jonas, Micke P, Blojne, David, Fredrik, Karin, Jacob, Magnus, Ragnar, Ida and many others.

In 2009, I visited the HIM in Bonn, during the trimester program *Diophantine Equations*. I am deeply grateful to the organizers for providing that opportunity. Thanks also to all friends I have met at conferences and summer schools.

I have benefited greatly from discussions with Tim Browning and Jonathan Pila. I also wish to thank Roger Heath-Brown for showing interest in my research, as well as providing inspiration for a major part of it.

I thank my family for always supporting me. Especially, I thank Sofia for her love, thoughtfulness and generosity and for inspiring me, supporting me and believing in me during times of doubt. And I thank our ε, whom I can't wait to meet.

Oscar Marmon
Gothenburg April 2010

Till morfar

Counting solutions to Diophantine equations

Oscar Marmon

1 Introduction

The study of Diophantine equations is among the oldest branches of mathematics, and also one of the most intriguing. By a Diophantine equation, we mean a polynomial equation in several variables defined over the integers. The term *Diophantine* refers to the Greek mathematician Diophantus of Alexandria, who studied such equations in the 3rd century A.D.

Thus, let $f(x_1, \ldots, x_n)$ be a polynomial with integer coefficients. We then wish to study the set of solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ to the equation

$$f(x_1, \ldots, x_n) = 0. \tag{1}$$

This may be done from several different perspectives. The first question one may ask is perhaps whether or not the Diophantine equation (1) has any solutions at all. Indeed, one of the most famous theorems in mathematics, Fermat's Last Theorem, proven by Wiles in 1995, states that for $f(x, y, z) = x^n + y^n - z^n$, where $n \geq 3$, there are no solutions in positive integers x, y, z. Qualitative questions of this type are often studied using algebraic methods.

Secondly, one may adapt an algorithmic perspective. To give another famous example, the tenth problem in Hilbert's famous list from 1900 asked for a general algorithm to determine, in a finite number of steps, the solvability of any given Diophantine equation. It was proven by Matiyasevich in 1970 that this problem is unsolvable.

In this thesis, we shall focus on a third problem - that of estimating the number of solutions to Diophantine equations. Our methods are both analytic and algebraic in nature. Much attention has been given to cases where the set of solutions to (1) is finite. Thus, for example, if $f(x, y, z)$ is a homogeneous polynomial, the equation $f = 0$ defines an algebraic curve in the projective plane. The celebrated theorem of Faltings states that there are only finitely many rational points on such a curve if its genus is at least 2. In other words, there are only finitely many solutions, with x, y, z relatively prime, to the Diophantine equation (1) in this case.

When the number of variables is larger, however, we often expect there to be infinitely many solutions. Still, we want to measure the size of the solution set in some way. One convenient way of expressing such quantitative information is through the *counting function*

$$N(f,B) = \#\{\mathbf{x} \in \mathbb{Z}^n; f(x_1,\dots,x_n) = 0, \max_i |x_i| \le B\}.$$

Estimates for such counting functions shall occur frequently throughout this thesis. In order to express these estimates, it is convenient at this point to introduce some notation.

Notation. We shall interchangeably use the notations $\Phi(B) \ll \Psi(B)$, $\Phi(B) = O(\Psi(B))$ to express the fact that there is a constant c such that $\Phi(B) \le c\Psi(B)$ for B large enough. If c is allowed to depend on certain parameters, this is indicated by subscripts. The notation $\Phi(B) \sim \Psi(B)$ shall mean that

$$\lim_{B\to\infty} \Phi(B)/\Psi(B) = 1,$$

and $\Phi(B) \approx \Psi(B)$ means that $\Phi(B) \sim c\Psi(B)$ for some constant c.

1.1 A simple heuristic

Suppose that $f \in \mathbb{Z}[x_1,\dots,x_n]$ is a polynomial of degree $d \le n$. Then we can argue as follows to guess the order of magnitude of $N(f,B)$. The values $f(\mathbf{x})$, where $\mathbf{x} \in [-B,B]^n$, will be of order B^d. Thus, we might expect the probability that $f(\mathbf{x})$ vanishes for a randomly chosen $\mathbf{x} \in [-B,B]^n$ to be of order B^{-d}. As the cube $[-B,B]^n$ contains $\approx B^n$ integral points, we are led to expect that

$$B^{n-d} \ll N(f,B) \ll B^{n-d}. \tag{2}$$

In some cases, this heuristic can be shown to give the correct answer. In particular, the Hardy-Littlewood circle method yields accurate bounds when n is large enough compared to d. Thus, Birch [3] has proved that for a non-singular homogeneous polynomial f of degree d in $n > (d-1)2^d$ variables, we have

$$N(f,B) \sim c_f B^{n-d}$$

as $B \to \infty$, where the constant c_f is positive if the equation $f = 0$ has a non-trivial solution in $\mathbb{R}$ and in each p-adic field $\mathbb{Q}_p$.

One may apply the same heuristic arguments to systems of equations. Let us denote the maximum norm of a point $\mathbf{x} \in \mathbb{C}^n$ by $|\mathbf{x}| = \max_i |x_i|$. In analogy

with the definition of $N(f,B)$, we define a counting function for systems of equations:

$$N(f_1,\dots,f_r,B) = \#\{\mathbf{x}\in\mathbb{Z}^n; f_1(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0, |\mathbf{x}| \le B\}.$$

Given polynomials $f_1,\dots,f_r \in \mathbb{Z}[x_1,\dots,x_r]$ of degree $d_1,\dots,d_r$, respectively, the naïve reasoning above would lead us to expect that

$$B^{n-(d_1+\cdots+d_r)} \ll N(f_1,\dots,f_r,B) \ll B^{n-(d_1+\cdots+d_r)} \tag{3}$$

if $d_1+\cdots+d_r \le n$.

In Section 2 we will discuss results of this thesis, providing estimates that come quite close to the heuristic upper bounds in (2) and (3), for n of more moderate size than required in the Hardy-Littlewood circle method.

1.2 Integral and rational points on algebraic varieties

In the language of algebraic geometry, the equation (1) defines a hypersurface X in affine space $\mathbb{A}^n$. The set of integral solutions to (1) may then be seen as the intersection of X with the integral lattice $\mathbb{Z}^n$. In general, given any locally closed subvariety $X \subset \mathbb{A}^n$, we can study the set of integral points $X(\mathbb{Z}) = X \cap \mathbb{Z}^n$.

In this thesis, we investigate the *quantitative arithmetic* of algebraic varieties, to use a term introduced by Browning [8]. This involves understanding the behaviour of counting functions similar to the function $N(f,B)$ introduced above. Thus, let

$$X(\mathbb{Z},B) := X(\mathbb{Z}) \cap [-B,B]^n$$

for any positive real number B, and define the counting function

$$N(X,B) := \#X(\mathbb{Z},B).$$

The first simple observation one can make about the growth of $N(X,B)$ is the following standard result.

Proposition 1.1. *Let $X \subset \mathbb{A}^n$ be a closed subvariety of dimension m and degree d. Then*

$$N(X,B) = O_{n,d}(B^m). \tag{4}$$

Proof. We shall prove (4) by induction on m. If $m = 0$, then X consists of at most d points, so the estimate follows. Thus, suppose that $m > 0$. Since X decomposes into at most d irreducible components by Bézout's theorem, we may assume that X is in fact irreducible.

Then, for some $i \in \{1, \dots, n\}$, X intersects any hyperplane $H_a = \{x_i = a\}$, for $a \in \bar{\mathbb{Q}}$, properly. Thus we have

$$X(\mathbb{Z}, B) \subseteq \bigcup_{a \in \mathbb{Z},\ |a| \leq B} (X \cap H_a)(\mathbb{Z}, B),$$

where $\dim(X \cap H_a) \leq m - 1$ and $\deg(X \cap H_a) \leq d$ for all a. Thus we may conclude by induction that $N(X \cap H_a, B) = O_{n,d}(B^{m-1})$, so that

$$N(X, B) = \sum_{|a| \leq B} N(X \cap H_a, B) \ll_{n,d} B^m.$$

□

We shall refer to the bound given by Proposition 1.1 as the *trivial* estimate.

If the polynomial f is homogeneous, any multiple of a solution to (1) is again a solution, so it is more natural to study the set of solutions $(x_1, \dots, x_n) \in \mathbb{Z}^n$ with $\gcd(x_1, \dots, x_n) = 1$. We call these solutions *primitive*. The primitive solutions correspond to rational points on the projective variety $X \subset \mathbb{P}^{n-1}$ defined by (1).

More precisely, consider projective space $\mathbb{P}^n$ over $\bar{\mathbb{Q}}$, defined as the set of equivalence classes $[\mathbf{x}]$ of non-zero elements $\mathbf{x} = (x_0, \dots, x_n) \in \bar{\mathbb{Q}}^{n+1}$ under the equivalence relation $\sim$ given by

$$(x_0, \dots, x_n) \sim (\lambda x_0, \dots, \lambda x_n) \quad \text{for all} \quad \lambda \in \bar{\mathbb{Q}} \setminus \{0\}.$$

Let $\mathbb{P}^n(\mathbb{Q})$ be the set of points $x \in \mathbb{P}^n$ for which we can find a representative $\mathbf{x} \in \mathbb{Q}^{n+1}$ such that $[\mathbf{x}] = x$. If $X \subset \mathbb{P}^n$ is a locally closed subvariety, we define $X(\mathbb{Q}) = X \cap \mathbb{P}^n(\mathbb{Q})$. For each rational point $x \in X(\mathbb{Q})$, one can find a representative $\mathbf{x} \in \mathbb{Z}^{n+1}$ for x such that $\gcd(x_0, \dots, x_n) = 1$. Moreover, $\mathbf{x}$ is uniquely determine up to a choice of sign. We then define the *height* of the rational point $x \in \mathbb{P}^n(\mathbb{Q})$ as

$$H(x) = \max\{|x_0|, \dots, |x_n|\}.$$

The density of rational points on X is measured by the counting function

$$N(X, B) := \{x \in X(\mathbb{Q}), H(x) \leq B\}.$$

For any positive real number B, we also define the set

$$S(X, B) := \{\mathbf{x} \in \mathbb{Z}^{n+1}; [\mathbf{x}] \in X(\mathbb{Q}), H([\mathbf{x}]) \leq B\}.$$

Remark 1.1. The Möbius function μ may be used to single out the primitive points in $S(X,B)$, as explained in [8, §1.2]. Thus we have

$$N(X,B) = \frac{1}{2}\sum_{k=1}^{\infty}\mu(k)\#S(X,k^{-1}B) \tag{5}$$

and

$$\#S(X,B) = 2\sum_{k=1}^{\infty}N(X,k^{-1}B). \tag{6}$$

In particular, it is easy to see that if $\theta > 1$, then $N(X,B) \ll B^{\theta}$ if and only if $\#S(X,B) \ll B^{\theta}$.

More generally, one may impose individual restrictions on the coordinates $x_0,\dots,x_n$. Let $\mathbf{B} = (B_0,\dots,B_n)$ be an $(n+1)$-tuple of positive real numbers. Then we define

$$S(X,\mathbf{B}) = \{\mathbf{x}\in\mathbb{Z}^{n+1}; [\mathbf{x}]\in X(\mathbb{Q}), |x_i|\le B_i, i=0,\dots,n\}.$$

Remark 1.2. If K is a number field, one may define the height of a point $x\in\mathbb{P}^n(K)$ represented by $(x_0,\dots,x_n)\in K^{n+1}$ as

$$H_K(x) = \prod_{v\in M_K}\max\{\|x_0\|_v,\dots,\|x_n\|_v\},$$

where M_K is the set of standard absolute values on K (see [18, B.1]). It follows from the product formula [18, B.1.2] that $H_K(x)$ is independent of the choice of representative for x. Consequently, we may define a counting function

$$N_K(X,B) = \#\{x\in X(K); H_K(x)\le B\}.$$

We shall mostly be interested in the case $K=\mathbb{Q}$, but the conjectures we shall describe shortly, relating geometry and arithmetic, are most conveniently formulated over general number fields.

Example 1.1. It is easy to see that $N(\mathbb{A}^n,B) = (2\lfloor B\rfloor+1)^n$. Counting rational points in projective space is already more subtle. By a theorem of Schanuel [31], we have

$$N(\mathbb{P}^n,B) = \frac{2^{n-2}}{\zeta(n+1)}B^{n+1} + O(B^n(\log B)^{b_n}),$$

where $b_1 = 1$, $b_n = 0$ for $n\ge 2$.

For projective varieties, the trivial estimate is given by the following proposition.

Proposition 1.2. *Let $X \subset \mathbb{P}^n$ be a closed subvariety of dimension m and degree d. Then*

$$N(X,B) = O_{n,d}(B^{m+1}).$$

Proof. This follows from Proposition 1.1 by considering the affine cone $C(X) \subset \mathbb{A}^{n+1}$ over X. This is a variety of dimension $m+1$ and degree d, so

$$N(X,B) \leq N(C(X),B) = O_{n,d}(B^{m+1}).$$

□

The trivial estimate is obviously best possible for varieties containing a linear component defined over $\mathbb{Q}$. For any irreducible variety of degree at least 2, however, it can be improved upon. The most general result is due to Pila [26], who proves that

$$N(X,B) = O_{n,d,\varepsilon}(B^{m-1+1/d+\varepsilon}) \tag{7}$$

in the affine case, and

$$N(X,B) = O_{n,d,\varepsilon}(B^{m+1/d+\varepsilon}) \tag{8}$$

in the projective case.

1.3 The relation between geometry and arithmetic

There is a general philosophy in Diophantine geometry that "geometry governs arithmetic". For curves, one has a very satisfactory characterization of the density of rational points in terms of the genus, as explained in [18, Thm. B.6.2].

Let $C \subset \mathbb{P}^n$ be a smooth curve over a number field K. If $g(C) = 0$ and $C(K) \neq \emptyset$, then C is isomorphic to $\mathbb{P}^1$ over K, which implies that $N_K(C,B) \approx B^{2/d}$, where d is the degree of C. If $g(C) = 1$, then C is an elliptic curve, and by the Mordell-Weil theorem, $C(K)$ is a finitely generated abelian group. Then $N_K(C,B) \approx (\log B)^{r/2}$, where r is the rank of $C(K)$. Finally, if $g(C) \geq 2$, then Faltings' Theorem states that $C(K)$ is a finite set. In other words, $N_K(C,B) = O(1)$.

A similar characterization for higher-dimensional varieties is yet to be discovered, but there are conjectures inspired by the one-dimensional case. If X is a smooth projective variety over K, let K_X be a divisor in the canonical class (see [32, III.6.3]). The variety X is said to be of *general type* if K_X is ample, i.e. if some multiple nK_X defines an embedding of X into some projective space. A curve is of general type if and only if $g \geq 2$ [13, Prop. IV.5.2]. Thus, in

analogy with the case of curves, it is expected that rational points are scarce on such varieties. Indeed the Bombieri-Lang Conjecture [18, Conj. F.5.2.1] states that $X(K)$ is not Zariski dense in X if X is of general type.

At the opposite end of the spectrum, a variety X is called a *Fano variety* if $-K_X$ is ample. Such varieties are believed to possess "many" rational points. Batyrev and Manin [1] have formulated very general conjectures relating the density of rational points on a variety X to certain geometric invariants. They are most precise in the case of Fano varieties. For simplicity, suppose that we have an embedding $X \subset \mathbb{P}^n$. If X is Fano, then it is predicted that there is a non-empty open subset $U \subseteq X$ such that

$$N_K(U,B) \sim c_X B^{\alpha} (\log B)^{t-1} \tag{9}$$

for a certain $\alpha > 0$ and a certain integer $t \geq 1$, possibly after replacing K by a finite extension $K \subseteq K'$. For the precise definition of α and t we refer to [1], although a counterexample due to Batyrev and Tschinkel [2] shows that the suggested interpretation of t is not always correct. For a further discussion of this counterexample and its consequences, as well as the many cases for which the conjectural asymptotic formula has been verified, one may consult Peyre's survey article [25]. In the following important example, however, the invariants α and t have simple interpretations.

Example 1.2. Suppose that $X = V_1 \cap \cdots \cap V_r$ is an intersection of hypersurfaces $V_i \subset \mathbb{P}^{n-1}$ of degrees d_i, respectively, and that $\dim X = n-1-r$. In this case, we call X a *complete intersection of multidegree* $\mathbf{d} = (d_1, \ldots, d_r)$. If X is non-singular, then

$$K_X = -(n - (d_1 + \cdots + d_r))H,$$

where H is a hyperplane section. Therefore X is Fano if and only if $n > d_1 + \cdots + d_r$, and in this case, $\alpha = n - (d_1 + \cdots + d_r)$. Then [1, Conj. B'] states that

$$N_{K'}(U,B) \sim c B^{n-(d_1+\cdots+d_r)} (\log B)^{t-1}, \tag{10}$$

provided $U \subset X$ is a sufficiently small dense open subset, and $K' \supseteq K$ is sufficiently large. Moreover, it is conjectured that the integer t in (10) equals the rank of the Picard group of X. By [12, Cor. IV.3.2], $\mathrm{Pic}(X) \cong \mathbb{Z}$ if X is a complete intersection of dimension at least 3, and thus the log-factor in (10) vanishes in this case. In particular, for a hypersurface of degree d, the conjectural asymptotic formula (10) is in accordance with the heuristic (2) and Birch's theorem.

1.4 The dimension growth conjecture

One may also ask for a very general upper bound for the growth rate of $N(X,B)$, requiring as little information as possible about the variety X. In this direction, Heath-Brown has made the following conjecture ([15] or [16, Conj. 2]).

Conjecture 1. *Let $F \in \mathbb{Z}[x_1,\dots,x_n]$ be an irreducible homogeneous polynomial of degree d. Then*

$$N(F,B) \ll_{n,d,\varepsilon} B^{n-2+\varepsilon}.$$

Using birational projections, one can show that Conjecture 1 implies the following more general statement ([7, Conj. 2]):

Conjecture 2. *Let $X \subset \mathbb{P}^n$ be an irreducible closed subvariety of dimension m and degree $d \geq 2$. Then*

$$N(X,B) \ll_{n,d,\varepsilon} B^{m+\varepsilon}. \tag{11}$$

We refer to this statement, or a weaker version of it where the implied constant is allowed to depend on X, as the *dimension growth conjecture*.

Conjecture 2 has now been established in many cases, mainly due to Heath-Brown, Browning and Salberger. A table summarizing the progress may be found in Browning [8, Table 3.1]. Several different methods have been employed to treat different cases, including the approach with exponential sums introduced in Section 2 and the determinant method of Section 3, as well as the Hardy-Littlewood circle method. The case of cubic hypersurfaces has turned out to be the most difficult one [8]. More precisely, the remaining open case of the dimension growth conjecture is that of a singular hypersurface $X \subset \mathbb{P}^n$ of degree $d = 3$, where

$$5 \leq n \leq 5 + \dim \operatorname{Sing} X.$$

Example 1.3. Consider the surface $X \subset \mathbb{P}^3$ given by

$$x_1^3 - x_2^3 + x_3^3 - x_4^3 = 0.$$

Although X is irreducible, and even non-singular, it obviously contains the line given by $x_1 = x_2$ and $x_3 = x_4$. The contribution from this line alone shows that $N(X,B) \gg B^2$, so this provides an example where the bound (11) is best possible. On the other hand, the heuristic (2) suggests an estimate of order B. Thus, we might be tempted to pursue a better bound for the dense open subset $U \subset X$ obtained by deleting all lines on X. By a recent result of Salberger [28, Cor. 6.5], one obtains

$$N(U,B) \ll B^{\sqrt{3}} (\log B)^4.$$

In this case, the only lines on X are those given by

$$x_{\sigma(1)} - x_{\sigma(2)} = x_{\sigma(3)} - x_{\sigma(4)} = 0$$

for some permutation $\sigma \in S_4$.

In general, rational points on a variety X may accumulate along a certain algebraic subset A, and it makes sense to study the density of rational points on the open subset $U = X \setminus A$ rather than on X.

1.5 Counting representations of integers as sums or differences of powers (Paper IV)

Now we shall consider a particularly well studied Diophantine equation. The classical *Waring's problem* asks for the least integer $s = g(k)$ such that the equation

$$x_1^k + \cdots + x_s^k = N, \tag{12}$$

has a solution $(x_1, \ldots, x_s) \in \mathbb{N}^s$ for any $N \in \mathbb{N}$. In other words, we ask for the smallest integer s such that any natural number can be represented as a sum of s k-th powers of natural numbers.

A related question concerns the *number* of representations of N on the form (12), denoted $R_{k,s}(N)$. One easily deduces the bound

$$R_{k,s}(N) = O_\varepsilon(N^{(s-2)/k+\varepsilon}). \tag{13}$$

Indeed, the case $s = 2$, from which the general case is easily obtained by induction, follows from well-known estimates for the divisor function.

Remark 1.3. Moreover, we trivially have

$$\sum_{n=1}^{N} R_{k,s}(n) \ll N^{s/k},$$

so one might heuristically expect that $R_{k,s}(N) = O_\varepsilon(N^\varepsilon)$ if $s \leq k$ and $R_{k,s}(N) = O_\varepsilon(N^{s/k-1+\varepsilon})$ if $s > k$. The former bound would follow from the so called Hypothesis K of Hardy and Littlewood, stating that $R_{k,k}(N) = O(N^\varepsilon)$ for any natural number k. For $k = 3$, Hypothesis K was proven to be false for $k = 3$ by Mahler [24], but it remains open for larger k.

In Paper IV of this thesis, we study the case $s = 4$. Thus, let $R_k(N) := R_{k,4}(N)$. For sums of four cubes, Hooley [19] has proved the remarkable estimate $R_3(N) = O_\varepsilon(N^{11/18+\varepsilon})$, using sieve methods. Wisdom [36, 37] extended Hooley's methods to prove that $R_k(N) = O_\varepsilon(N^{11/(6k)+\varepsilon})$ for odd integers $k \geq 3$. In Paper IV, the following result is proven.

Theorem 1.1 (Paper IV, Thm. 1.3)**.**

$$R_k(N) \ll_{k,\varepsilon} N^{1/k+2/k^{3/2}+\varepsilon}$$

for any $\varepsilon > 0$.

More generally, we consider sums of three k-th powers and an l-th power. The results follow rather easily from recent work of Salberger [28], discussed further in Section 3.

The main part of Paper IV is devoted to another variant of the same problem, where some of the $+$ signs in (12) are replaced by $-$, and the variables x_i are allowed to be arbitrary integers. This problem was recently studied by Heath-Brown [17] in the case $s = 3$. Now there may well be infinitely many solutions, so it makes sense to study the density of solutions. Thus, for $k \geq 3$ and $\varepsilon_2, \varepsilon_3 \in \{\pm 1\}$, let $\mathscr{R}(N,B)$ be the number of solutions $\mathbf{x} \in \mathbb{Z}^3$ to

$$x_1^k + \varepsilon_2 x_2^k + \varepsilon_3 x_3^k = N, \tag{14}$$

satisfying $\max|x_i| \leq B$. Here we have the trivial estimate (cf. (13))

$$\mathscr{R}(N,B) = O_\varepsilon(B^{1+\varepsilon}).$$

Call a solution *special* if one of the terms $\pm x_i^k$ equals N. It may happen that the contribution to $\mathscr{R}(N,B)$ of the special solutions is of order B. If $\mathscr{R}_0(N,B)$ denotes the number of non-special solutions to the equation (14) satisfying $\max|x_i| \leq B$, then Heath-Brown proves that

$$\mathscr{R}_0(N,B) = O_k(B^{10/k})$$

if $N \ll B$, and that

$$\mathscr{R}_0(N,B) = O_\varepsilon(B^{9/10+\varepsilon} N^{1/10})$$

if $N \ll B^{3/13}$.

In Paper IV, we consider the case $s = 4$, in the following more general setting. For a quadruple of non-zero integers (a_1, a_2, a_3, a_4) and a positive integer N, we consider the equation

$$a_1 x_1^k + a_2 x_2^k + a_3 x_3^k + a_4 x_4^k = N, \tag{15}$$

where $x_i \in \mathbb{Z}$. Reusing the notation above, let $\mathscr{R}(N,B)$ be the number of solutions $\mathbf{x} \in \mathbb{Z}^4$ to (15) satisfying $\max|x_i| \leq B$. We think of N as being considerably smaller than B^k, as opposed to in Theorem 1.1, where we had a natural bound $B = N^{1/k}$ for the height of the solutions. In this case, the "trivial" estimate

$$\mathscr{R}(N,B) = O_\varepsilon(B^{2+\varepsilon}) \tag{16}$$

may be deduced from known bounds for the number of solutions to Thue equations.

As above, call a solution $\mathbf{x}$ to *special* if either $a_i x_i^k = N$ for some index i or $a_i x_i^k + a_j x_j^k = N$ for some pair of indices i, j. Again, the contribution of the special solutions to $\mathscr{R}(N,B)$ may be of order B, as the example $N = 1$, $\mathbf{a} = (1,-1,1,1)$, $\mathbf{x} = (t,t,0,1)$ shows. However, one can show that the contribution is at most $O_\varepsilon(BN^\varepsilon)$.

If $\mathscr{R}_0(N,B)$ denotes the number of non-special solutions to (15) with $|x_i| \leq B$ for all i, then the main result of Paper IV is the following.

Theorem 1.2 (Paper IV, Thm. 1.1)**.** *For any $\varepsilon > 0$ we have*

$$\mathscr{R}_0(N,B) \ll_{a_i,N,\varepsilon} B^{16/(3\sqrt{3k})+\varepsilon}(B^{2/\sqrt{k}} + B^{1/\sqrt{k}+6/(k+3)}). \tag{17}$$

In particular, $\mathscr{R}(N,B) \ll_{a_i,N} B$ for $k \geq 27$.

This estimate improves upon the trivial estimate (16) as soon as $k \geq 8$. There is also a version of Theorem 1.2 where the dependence on N is explicit. The method of proof is discussed in further detail in Section 3.

Remark 1.4. In the notation used earlier, we have $\mathscr{R}(N,B) = N(X,B)$, where $X \subset \mathbb{A}^n$ is the hypersurface given by (15), and $\mathscr{R}_0(N,B) = N(U,B)$, where the open subset $U \subset X$ is the complement of all lines contained in X (cf. Example 1.3).

2 The method of exponential sums

As mentioned above, the Hardy-Littlewood circle method may be used to prove asymptotic formulae for the density of solutions to Diophantine equations, provided the number of variables is large enough. The method described in this section gives slightly weaker bounds, but is useful when the number of variables is smaller. We begin by stating a result of Heath-Brown [15] that has provided the inspiration for the first two papers in this thesis. By the *leading form* of a polynomial, we shall mean its homogeneous part of maximal degree.

Theorem 2.1 (Heath-Brown [15, Thm. 2])**.** *Let $f \in \mathbb{Z}[x_1,\dots,x_n]$, where $n \geq 5$, be a polynomial of degree at least 3, with leading form F. Suppose that F defines a non-singular hypersurface in $\mathbb{P}^{n-1}_{\mathbb{Q}}$. Then*

$$N(f,B) \ll_f B^{n-3+15/(n+5)}.$$

Note that for cubic polynomials, this estimate approaches the upper bound predicted by our heuristic consideration (2) and the Batyrev-Manin conjectures, as $n \to \infty$. In Paper I, we prove the following generalization of Theorem 2.1 to varieties defined by several equations. Here we denote the *height* of a polynomial $F \in \mathbb{C}[x_1, \dots, x_n]$, defined as the maximum of the absolute values of the coefficients of F, by $\|F\|$.

Theorem 2.2 (Paper I, Thm. 1.1)**.** *Let $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$ be polynomials of degree at least 3 and at most d, with leading forms $F_1, \dots, F_r$, respectively. Suppose that $F_1, \dots, F_r$ define a non-singular complete intersection of codimension r in $\mathbb{P}^{n-1}_{\mathbb{Q}}$. Then*

$$N(f_1, \dots, f_r, B) \ll_{n,d} B^{n-3r+r^2\frac{13n-5-3r}{n^2+4nr-n-r-r^2}} (\log B)^{n/2} \left(\sum_{i=1}^{r} \log \left\| F_i \right\| \right)^{2r+1}.$$

Again, if $d = 3$, this estimate approaches the conjectural one as $n \to \infty$. In the case $r = 1$, the exponent

$$n - 3 + \frac{13n - 8}{n^2 + 3n - 2}$$

offers a slight improvement upon the exponent of Theorem 2.1, the nature of which will be explained in §2.7. Unfortunately, this is not enough to extend the range $n \geq 10$ in which Theorem 2.1 validates Conjecture 1. In Paper II, the aim is to improve upon the estimate in Theorem 2.1 for polynomials of higher degree. The following is our main result.

Theorem 2.3 (Paper II, Thm. 1.2)**.** *Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be a polynomial of degree $d \geq 4$ with leading form F. Suppose that F defines a non-singular hypersurface in $\mathbb{P}^{n-1}_{\mathbb{Q}}$. Then*

$$N(f, B) \ll_{n,d,\varepsilon} B^{n-4+(37n-18)/(n^2+8n-4)} + B^{n-3+\varepsilon}.$$

This estimate improves upon Theorem 2.1 as soon as $d \geq 4$ and $n \geq 11$. For very large n, the results above fall in importance, in favour of the Hardy-Littlewood circle method, at least for forms. Indeed, recall that Birch's work yields the bound $N(f, B) \ll B^{n-4}$ if $d = 4$ and $n \geq 49$. This has recently been improved to $n \geq 41$ by Browning and Heath-Brown [6]. The proofs of Theorems 2.2 and 2.10 are discussed in §2.7-2.8.

2.1 Counting solutions to congruences

The method used to prove the above results starts with the trivial observation that a solution $\mathbf{x} \in \mathbb{Z}^n$ to the equation $f(x_1, \dots, x_n) = 0$ is a fortiori a solution to the congruence

$$f(x_1, \dots, x_n) \equiv 0 \pmod{q} \tag{18}$$

for any integer q.

To count solutions to a polynomial congruence (18), one may use exponential sums. We adopt the standard notation $e(x) := e^{2\pi i x}$ and $e_q(x) := e(x/q)$. If t is an integer, then we have the following identity:

$$\sum_{a=1}^{q} e_q(at) = \begin{cases} q & \text{if } q \mid t, \\ 0 & \text{otherwise.} \end{cases} \tag{19}$$

Let $R = \mathbb{Z}/q\mathbb{Z}$, and let $f \in R[x_1, \dots, x_n]$ be a polynomial. If $N(f)$ denotes the number of solutions $\mathbf{x} \in R^n$ to the equation $f(\mathbf{x}) = 0$, then we may use (19) to obtain the formula

$$N(f) = \frac{1}{q} \sum_{a=1}^{q} \sum_{\mathbf{x} \in R^n} e_q(af(\mathbf{x})).$$

For $a = q$, the inner sum equals q^n, so we get

$$N(f) - q^{n-1} = \frac{1}{q} \sum_{a=1}^{q-1} \sum_{\mathbf{x} \in R^n} e_q(af(\mathbf{x})). \tag{20}$$

Thus, we can get a bound for the deviation of $N(f)$ from its expected value q^{n-1} by estimating the exponential sums $\sum_{\mathbf{x}} e_q(af(\mathbf{x}))$.

Suppose now that $q = p$ is a prime. Let $f \in \mathbb{F}_p[x_1, \dots, x_n]$ be a polynomial of degree d, where $(d, p) = 1$. Suppose that the leading form F of f defines a non-singular hypersurface in $\mathbb{P}^{n-1}$ over $\mathbb{F}_p$. Then we have Deligne's estimate [9, Thm. 8.4]

$$\sum_{\mathbf{x} \in \mathbb{F}_p^n} e_p(f(\mathbf{x})) \ll_{n,d} p^{n/2}. \tag{21}$$

An immediate corollary of (21) is that

$$N(f) = p^{n-1} + O_{n,d}(p^{n/2}).$$

More generally, Deligne proves the following result.

Theorem 2.4 (Deligne [9, Thm. 8.1])**.** *Let $X \subset \mathbb{P}^n_{\mathbb{F}_p}$ be a non-singular complete intersection of dimension $m = n - r$ and multidegree $\mathbf{d} = (d_1, \dots, d_r)$. Then*

$$\#X(\mathbb{F}_p) = \#\mathbb{P}^m(\mathbb{F}_p) + O_{n,\mathbf{d}}(p^{m/2}).$$

Remark 2.1. We have $\#\mathbb{P}^m(\mathbb{F}_p) = p^m + p^{m-1} + \cdots + 1$.

Theorem 2.4 and the estimate (21) are both consequences of the Weil conjectures, in particular the Riemann hypothesis for varieties over finite fields, proven by Deligne in [9].

2.2 Counting solutions of bounded height to congruences

It seems desirable to extend the above results in two directions. First, one may ask what happens for singular varieties. This question is addressed by Hooley [20], who proves the following generalization of Theorem 2.4.

Theorem 2.5 (Hooley [20, Thm. 2])**.** *Let X be a complete intersection in $\mathbb{P}^n_{\mathbb{F}_p}$ of dimension $m = n - r$ and multidegree $\mathbf{d}$, and let s be the dimension of the singular locus of X. Then*

$$\#X(\mathbb{F}_p) = \#\mathbb{P}^m(\mathbb{F}_p) + O_{n,\mathbf{d}}(p^{(m+s+1)/2}).$$

Secondly, we are interested in counting solutions of bounded height to congruences, rather than all solutions. Indeed, if we define

$$N(f_1, \ldots, f_r, B, q) = \#\{\mathbf{x} \in \mathbb{Z}^n; f_i(\mathbf{x}) \equiv 0 \,(\mathrm{mod}\, q), 1 \le i \le r, |\mathbf{x}| \le B\},$$

then we have

$$N(f_1, \ldots, f_r, B) \le N(f_1, \ldots, f_r, B, q)$$

for any integer q. If $B \ll q$, we may identify $\mathbb{Z} \cap [-B, B]^n$ with a subset of $(\mathbb{Z}/q\mathbb{Z})^n$. It is sometimes convenient to replace the characteristic function of the box $[-B, B]^n$ by a smooth weight function. More precisely, let $W : \mathbb{R}^n \to [0, 1]$ be an infinitely differentiable function, supported on $[-2, 2]^n$. Then we define a weighted counting function

$$N_W(f_1, \ldots, f_r, B, q) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ q | f_1(\mathbf{x}), \ldots, f_r(\mathbf{x})}} W\left(\frac{1}{B}\mathbf{x}\right).$$

We may for example take W to be the function defined by

$$W(\mathbf{t}) = \prod_{i=1}^{n} w(t_i/2), \text{ where } w(t) = \begin{cases} \exp(-1/(1-t^2)), & |t| < 1, \\ 0, & |t| \ge 1. \end{cases} \tag{22}$$

It is then clear that

$$N(f_1, \ldots, f_r, B, q) \ll N_W(f_1, \ldots, f_r, B, q).$$

In the hypersurface case, Heath-Brown proves the following asymptotic formula.

Theorem 2.6 (Heath-Brown [15, Thm. 3]). *Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be a polynomial of degree $d \geq 2$. Let q be a prime and $B \ll q$ a real number. Let Z_q the hypersurface in $\mathbb{P}^n_{\mathbb{F}_q}$ defined by the leading form F of f. Then*

$$N_W(f, B, q) = q^{-1} \sum_{\mathbf{x} \in \mathbb{Z}^n} W\left(\frac{1}{B}\mathbf{x}\right) + O_{n,d,W}\left(B^{s+1} q^{(n-s-1)/2}\right),$$

where s is the dimension of the singular locus of Z_q.

The following result of Paper I extends Theorem 2.6, and improves slightly upon its error term. It may be viewed as a weighted, affine version of Theorem 2.5.

Theorem 2.7 (Paper I, Thm. 3.3). *Let $f_1, \dots, f_r \in \mathbb{Z}[x_1, \dots, x_n]$ be polynomials of degree at least 2 and at most d, with leading forms $F_1, \dots, F_r$, respectively. Let q be a prime and B a real number with $1 \leq B \ll q$. Suppose that $F_1, \dots, F_r$ define a closed subscheme $Z_q \subset \mathbb{P}^{n-1}_{\mathbb{F}_q}$ of codimension r. Then*

$$N_W(f_1, \dots, f_r, B, q) = q^{-r} \sum_{\mathbf{x} \in \mathbb{Z}^n} W\left(\frac{1}{B}\mathbf{x}\right) + O_{n,d,W}\left(B^{s+2} q^{(n-r-s-2)/2}\right),$$

where s is the dimension of the singular locus of Z_q.

Remark 2.2. We have simplified the error term somewhat, by noting that the theorem is trivially true if $B \ll q^{1/2}$ (cf. Remark 3.1 in Paper II).

We shall discuss the proof of Theorem 2.7 in §2.7. In the appendix to Paper I, Salberger proves a version of Theorem 2.7 without the smooth weight function W, but with a slightly larger error term. To state it, we need to define counting functions for general boxes. By a *box* B in $\mathbb{R}^n$, we mean a product of closed intervals. If q is a positive integer, we define

$$N(f_1, \dots, f_r, \mathsf{B}, q) = \#\{\mathbf{x} \in \mathsf{B} \cap \mathbb{Z}^n; f_1(\mathbf{x}) \equiv \cdots \equiv f_r(\mathbf{x}) \equiv 0 \,(\mathrm{mod}\, q)\}.$$

Theorem 2.8 (Salberger). *Let $f_1, \dots, f_r$ be $r < n$ polynomials in $\mathbb{Z}[x_1, \dots, x_n]$ with leading forms $F_1, \dots, F_r$, respectively, of degree at least 2 and at most d. Let q be a prime and B be a box in $\mathbb{R}^n$ such that each side has length at most $2B < q$. Suppose that $F_1, \dots, F_r$ define a closed subscheme $Z_q \subset \mathbb{P}^{n-1}_{\mathbb{F}_q}$ of codimension r. Then*

$$N(f_1, \dots, f_r, \mathsf{B}, q) = q^{-r} \#(\mathsf{B} \cap \mathbb{Z}^n) + O_{n,d}(B^{s+2} q^{(n-r-s-2)/2} (\log q)^n),$$

where s is the dimension of the singular locus of Z_q.

2.3 Weyl differencing

The method used by Heath-Brown to derive the estimate in Theorem 2.1 has its roots in classical techniques for exponential sums in one variable. In its original form, the idea is due to Hermann Weyl, who pioneered the use of exponential sums in number theory, in his paper *Über die Gleichverteilung von Zahlen mod. Eins* from 1916 [35]. One of the fundamental tools in this paper is a procedure now known as "Weyl differencing". If $f : \mathbb{Z} \to \mathbb{R}$ is any function, the idea is to bound the size of the exponential sum

$$S = \sum_{x=1}^{B} e(f(x))$$

from above by a mean value of exponential sums involving differenced functions $f_h(x) = f(x+h) - f(x)$. In case f is a polynomial, the differenced function will be a polynomial of lower degree. To achieve this, one writes

$$\begin{aligned} |S|^2 &= \sum_{x=1}^{B} e(-f(x)) \sum_{x'=1}^{B} e(f(x')) \\ &= \sum_{|h|<B} \sum_{\substack{1\le x\le B \\ 1\le x+h\le B}} e(f(x+h)-f(x)) \\ &= \sum_{|h|<B} \sum_{\substack{1\le x\le B \\ 1\le x+h\le B}} e(f_h(x)). \end{aligned}$$

If f is a polynomial of degree d, one can iterate this procedure $d-1$ times, using Cauchy's inequality, until one has exponential sums involving linear polynomials. These are sums over geometric progressions, and are thus easily estimated. For a more precise account of Weyl's method, and applications to the Riemann zeta function, one may consult Iwaniec & Kowalski [21, Ch. 8].

2.4 Van der Corput's method

A refinement of Weyl's method was devised by van der Corput [33, 34]. His method involves two processes, now known as A and B, that may be iterated alternatingly to produce increasingly sharper bounds for certain exponential sums. The A-process is a refinement of the Weyl differencing described above. Changing notation slightly, we consider a function $F : \mathbb{Z} \to \mathbb{C}$ and let

$$S = \sum_{x=1}^{B} F(x).$$

Let χ be the characteristic function of the interval $[1,B]$. One then introduces a parameter $H \leq B$, and writes

$$HS = \sum_{h=1}^{H} \sum_{x \in \mathbb{Z}} \chi(x+h)F(x+h) = \sum_{x \in \mathbb{Z}} \sum_{h=1}^{H} \chi(x+h)F(x+h).$$

By Cauchy's inequality we have

$$\begin{aligned} H^2|S|^2 &\leq \left(\sum_{x=1-H}^{B-1} 1 \right) \sum_{x \in \mathbb{Z}} \left| \sum_{h=1}^{H} \chi(x+h)F(x+h) \right|^2 \\ &\leq (2B) \sum_{x \in \mathbb{Z}} \sum_{1 \leq h_1, h_2 \leq H} \chi(x+h_1)\chi(x+h_2)F(x+h_1)\overline{F(x+h_2)}. \end{aligned}$$

A variable change furnishes

$$\begin{aligned} |S|^2 &\ll BH^{-2} \sum_{|h|<H} \#\{(h_1,h_2); h_1 - h_2 = h\} \sum_{\substack{1 \leq x \leq B \\ 1 \leq x+h \leq B}} F(x+h)\overline{F(x)} \\ &\ll BH^{-1} \sum_{|h|<H} \sum_{\substack{1 \leq x \leq B \\ 1 \leq x+h \leq B}} F(x+h)\overline{F(x)}. \end{aligned}$$

If $F(x) = e(f(x))$, then $F(x+h)\overline{F(x)} = e(f_h(x))$ as defined above. The introduction of the parameter H adds a new level of flexibility compared to Weyl's method.

Loosely speaking, the B-process in van der Corput's method uses Poisson's summation formula to transform our exponential sum into another one of shorter length, under suitable smoothness assumptions on the function f. A thorough treatment of van der Corput's method is given in [10].

2.5 Heath-Brown's q-analogue

In [14] Heath-Brown introduced a q-analogue of van der Corput's method, applicable in the case where F is a periodic function, say $F(x) = e_q(f(x))$ for some function $f : \mathbb{Z} \to \mathbb{Z}$. For a suitable divisor q_0 of q, we take as our starting point the formula

$$HS = \sum_{h=1}^{H} \sum_{x \in \mathbb{Z}} \chi(x+hq_0)F(x+hq_0).$$

In the resulting estimate

$$|S|^2 \ll BH^{-1} \sum_{|h|<H} \sum_{\substack{1 \leq x \leq B \\ 1 \leq x+hq_0 \leq B}} F(x+hq_0)\overline{F(x)},$$

we have then also achieved a shortening of the period of the summand to q/q_0, which is often favourable.

2.6 A multi-dimensional q-analogue

The method developed by Heath-Brown to prove Theorem 2.1 may be viewed as an extension of his q-analogue of van der Corput's method to exponential sums in several variables. The idea is to bound $N(f,B)$ from above by $N_W(f,B,m)$, where W is the weight function defined in (22) and m is a composite number. More precisely, one chooses two primes p,q satisfying $p \leq B \leq q$ and puts $m = pq$. Here, p will play the role of the integer q_0 above. Thus, one divides the sum

$$N_W(f,B,pq) = \sum_{\substack{\mathbf{x}\in\mathbb{Z}^n \\ pq|f(\mathbf{x})}} W\left(\frac{1}{B}\mathbf{x}\right)$$

into congruence classes (mod p);

$$N_W(f,B,pq) = \sum_{\substack{\mathbf{u}\in\mathbb{F}_p^n \\ p|f(\mathbf{u})}} \sum_{\substack{\mathbf{x}\equiv\mathbf{u}(p) \\ q|f(\mathbf{x})}} W\left(\frac{1}{B}\mathbf{x}\right).$$

The expected value of the inner sum is

$$K := p^{-n}q^{-1}\sum_{\mathbf{x}\in\mathbb{Z}^n} W\left(\frac{1}{B}\mathbf{x}\right),$$

so one writes

$$\begin{aligned} N_W(f,B,pq) &= K\sum_{\substack{\mathbf{u}\in\mathbb{F}_p^n \\ p|f(\mathbf{u})}} 1 + \sum_{\substack{\mathbf{u}\in\mathbb{F}_p^n \\ p|f(\mathbf{u})}} \left(\sum_{\substack{\mathbf{x}\equiv\mathbf{u}(p) \\ q|f(\mathbf{x})}} W\left(\frac{1}{B}\mathbf{x}\right) - K\right) \\ &\ll B^n p^{-1}q^{-1} + \left|\sum_{\substack{\mathbf{u}\in\mathbb{F}_p^n \\ p|f(\mathbf{u})}} \left(\sum_{\substack{\mathbf{x}\equiv\mathbf{u}(p) \\ q|f(\mathbf{x})}} W\left(\frac{1}{B}\mathbf{x}\right) - K\right)\right|. \end{aligned} \tag{23}$$

Van der Corput differencing is then applied to the rightmost sum, which leads one to estimate counting functions for the hypersurfaces in $\mathbb{A}^n_{\mathbb{F}_q}$ defined by differenced polynomials

$$f^{\mathbf{y}}(\mathbf{x}) := f(\mathbf{x}+p\mathbf{y}) - f(\mathbf{x}).$$

To this end, one uses Theorem 2.6. Thus, geometric arguments are needed to keep track of the quantity s appearing in Theorem 2.6, or, in other words, to determine how singular the "differenced" hypersurfaces are.

2.7 Generalization to complete intersections (Paper I)

Let $f_1, \dots, f_r$ and $F_1, \dots, F_r$ be as in the hypotheses of Theorem 2.2. As in Heath-Brown's proof of Theorem 2.1, we shall work with a modulus that is a product of two primes. More precisely, if

$$Z = \operatorname{Proj} \mathbb{Z}[x_1, \dots, x_n]/(F_1, \dots, F_r),$$

then the primes p and q are chosen so that $2p < 2B + 1 < q - p$, and both $Z_{\mathbb{F}_p}$ and $Z_{\mathbb{F}_q}$ are non-singular of codimension r. The differencing procedure that lies at the heart of the proof of Theorem 2.2 is a rather straightforward extension of that in [15], one major difference being that we avoid the use of a smooth weight function. Thus, let χ_{B} be the characteristic function of the box $\mathsf{B} = [-B, B]^n$. Writing

$$N := N(f_1, \dots, f_r, B, pq)$$

we have

$$N = K \sum_{\substack{\mathbf{u} \in \mathbb{F}_p^n \\ p \mid f_1(\mathbf{u}), \dots, f_r(\mathbf{u})}} 1 + \sum_{\substack{\mathbf{u} \in \mathbb{F}_p^n \\ p \mid f_1(\mathbf{u}), \dots, f_r(\mathbf{u})}} \left(\sum_{\substack{\mathbf{x} \equiv \mathbf{u} (p) \\ q \mid f_1(\mathbf{x}), \dots, f_r(\mathbf{x})}} \chi_{\mathsf{B}}(\mathbf{x}) - K \right), \tag{24}$$

where

$$K = p^{-n} q^{-r} (2B + 1)^n.$$

As in (23), van der Corput differencing is applied to the rightmost sum in (24). This procedure introduces differenced polynomials $f_1^{\mathbf{y}}, \dots, f_r^{\mathbf{y}}$, for $\mathbf{y} \in \mathbb{F}_q^n$, defined by

$$f_i^{\mathbf{y}}(\mathbf{x}) := f_i(\mathbf{x} + p\mathbf{y}) - f_i(\mathbf{x}).$$

Defining the boxes

$$\mathsf{B}_{\mathbf{y}} := \left\{ \mathbf{x} \in \mathbb{Z}^n ; \mathbf{x} \in \mathsf{B}, \mathbf{x} + p\mathbf{y} \in \mathsf{B} \right\},$$

we are then required to estimate the sum $\sum_{\mathbf{y} \in \mathbb{Z}^n} \Delta(\mathbf{y})$, where

$$\Delta(\mathbf{y}) = N(f_1^{\mathbf{y}}, \dots, f_r^{\mathbf{y}}, \mathsf{B}_{\mathbf{y}}, q) - q^{-r} \#(\mathsf{B}_{\mathbf{y}} \cap \mathbb{Z}^n).$$

If the leading form of $f_i^{\mathbf{y}}$ is denoted $F_i^{\mathbf{y}}$ for $1 \le i \le r$, let

$$Z_{\mathbf{y}} = \operatorname{Proj} \mathbb{F}_q[x_1, \dots, x_n]/(F_1^{\mathbf{y}}, \dots, F_r^{\mathbf{y}}).$$

(In fact, $F_i^{\mathbf{y}} = p\mathbf{y}\cdot\nabla F_i$ for all i, unless $\mathbf{y} = \mathbf{0}$.) Then the estimation of $\sum \Delta(\mathbf{y})$ by means of Theorem 2.8 requires uniform bounds for the dimension and degree of the closed subset of $\mathbf{y} \in \mathbb{A}^n$ such that $\dim \operatorname{Sing}(Z_{\mathbf{y}}) \ge s$, for all possible values of $s \ge -1$. This problem is addressed in the geometric part of the paper.

The output of the method just described is the following asymptotic formula (Paper I, Theorem 1.4):

$$\begin{aligned} N(f_1, \dots, f_r, B, pq) = \frac{(2B+1)^n}{p^r q^r} + O_{n,d}\Big(\Big(&B^{(n+1)/2}p^{-r/2}q^{(n-r-1)/4} \\ &+ B^{(n+1)/2}p^{(n-2r)/2}q^{-1/4} + B^{n/2}p^{-r/2}q^{(n-r)/4} \\ &+ B^{n/2}p^{(n-r)/2} + B^n p^{-(n+r-1)/2}q^{-r} + B^{n-1}p^{-r+1}q^{-r})(\log q)^{n/2}\Big). \end{aligned} \tag{25}$$

To deduce Theorem 2.2 from the asymptotic formula (25), we try to find primes p and q optimizing the expression on the right hand side, and at the same time satisfying the hypotheses that $Z_{\mathbb{F}_p}$ and $Z_{\mathbb{F}_q}$ be non-singular. It is only at this point that a dependence on the height of the polynomials is introduced into our estimates. A careful analysis using universal forms allows us to state this dependence explicitly in Theorem 2.2.

Now we turn to Theorem 2.7. The main part of the proof concerns the non-singular case $s = -1$. As in [15], we apply Poisson's summation formula to the counting function $N(f_1, \dots, f_r, B, q)$, in a q-analogue of van der Corput's B-process. One is then lead to estimate exponential sums

$$\sum_{\substack{\mathbf{x} \in \mathbb{F}_q^n \\ q \mid f_1(\mathbf{x}), \dots, f_r(\mathbf{x})}} e_q(\mathbf{a}\cdot\mathbf{x}),$$

where $\mathbf{a} \in \mathbb{F}_q^n$. Following Luo [23], we use estimates due to Katz [22] to bound these exponential sums. Already for hypersurfaces, this yields an improvement upon Heath-Brown's approach using Deligne's bounds. The general case is proven by induction on s. Part of the paper is devoted to geometric considerations needed in order to carry out this induction in a uniform manner.

At the end of Paper I, we sketch a proof of the following weighted version of the asymptotic formula (25), using Theorem 2.7 in place of Theorem 2.8.

Theorem 2.9. *Let $W : \mathbb{R}^n \to [0,1]$ be an infinitely differentiable function supported on $[-2,2]^n$. Let $f_1, \dots, f_r$ be polynomials in $\mathbb{Z}[x_1, \dots, x_n]$ of degree at least 3 and at most d, with leading forms $F_1, \dots, F_r$. Let*

$$Z = \operatorname{Proj} \mathbb{Z}[x_1, \dots, x_n]/(F_1, \dots, F_r)$$

and suppose that p and q are primes, with $p \leq B \leq q$, such that both $Z_{\mathbb{F}_p}$ and $Z_{\mathbb{F}_q}$ are non-singular subvarieties of codimension r in $\mathbb{P}^{n-1}$. Then we have

$$\begin{aligned} N_W(f_1,\dots,f_r,B,pq) - p^{-r}q^{-r}\sum_{\mathbf{x}\in\mathbb{Z}^n} W\left(\frac{1}{B}\mathbf{x}\right) \\ \ll_{D,n,d,C} B^{(n+1)/2}p^{-r/2}q^{(n-r-1)/4} + B^{(n+1)/2}p^{(n-2r)/2}q^{-1/4} \\ + B^n p^{-(n+r-1)/2}q^{-r} + B^{n-C/2}p^{(C-r)/2}q^{-r/2} \end{aligned}$$

for any $C > 0$, where $D = D_{n+1}$ is the maximum over $\mathbb{R}^n$ of all partial derivatives of W of order $n+1$.

2.8 Iteration of the Heath-Brown-van der Corput method (Paper II)

The idea behind the proof of Theorem 2.3 is to perform two iterations of the differencing procedure introduced in [15]. To this end, we use a modulus that is a product of three primes, $m = \pi pq$, where $\pi, p \leq B \leq q$. Moreover, we revert to the use of a smooth weight function. Thus, with W the function defined in (22), the heart of the proof of Theorem 2.10 is an asymptotic formula of the type

$$N_W(f,B,\pi pq) = (\pi pq)^{-1}\sum_{\mathbf{x}\in\mathbb{Z}^n} W\left(\frac{1}{B}\mathbf{x}\right) + \text{error terms}. \tag{26}$$

The primes π and p are used as parameters in the two differencing steps. In the differencing procedure, we incorporate a refinement of Heath-Brown's method due to Salberger [29], allowing us to retain, throughout the differencing step, congruence conditions that were discarded in the original approach.

For any $\mathbf{y} \in \mathbb{Z}^n$, we define the polynomial $f^{\mathbf{y}} \in \mathbb{Z}[x_1,\dots,x_n]$ by

$$f^{\mathbf{y}}(\mathbf{x}) = f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x}).$$

For any pair $(\mathbf{y},\mathbf{z}) \in \mathbb{Z}^n \times \mathbb{Z}^n$, we define the twice differenced polynomial

$$f^{\mathbf{y},\mathbf{z}}(\mathbf{x}) = f(\mathbf{x}+\mathbf{y}+\mathbf{z}) - f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x}+\mathbf{z}) + f(\mathbf{x}).$$

Furthermore, let

$$F^{\mathbf{y}}(\mathbf{x}) = \mathbf{y}\cdot\nabla F(\mathbf{x}) = y_1\frac{\partial F}{\partial x_1} + \cdots + y_n\frac{\partial F}{\partial x_n},$$

$$F^{\mathbf{y},\mathbf{z}}(\mathbf{x}) = (\mathrm{Hess}(F))\mathbf{y}\cdot\mathbf{z} = \sum_{1\leq i,j\leq n}\frac{\partial^2 F}{\partial x_i \partial x_j}y_i z_j.$$

Note how this notation differs from that of §2.7. Ignoring the technicalities of the differencing procedure itself, the main issue is now to estimate counting functions for the family of "differenced" varieties defined by

$$f(\mathbf{x}) = f^{p\mathbf{z}}(\mathbf{x}) = f^{\pi\mathbf{y},p\mathbf{z}}(\mathbf{x}) = 0.$$

Once more, these estimates are supplied by Theorem 2.7, successful application of which requires knowledge of the dimension of the singular loci of the projective subschemes

$$Z_{q,\mathbf{z},\mathbf{y}} = \operatorname{Proj} \mathbb{F}_q[x_1, \dots, x_n]/(F, F^{\mathbf{z}}, F^{\mathbf{y},\mathbf{z}})$$

for different determinations of $\mathbf{y}, \mathbf{z}$. This turns out to require considerable geometric machinery. In particular, although the asymptotic formula (26) holds uniformly in f, the conditions that have to be imposed on the primes π, p, q in order for the method to work go beyond mere good reduction of the hypersurface $f = 0$. A thorough investigation is made in order to ensure that such primes may always be found, of a prescribed order of magnitude in relation to B. At this point, a dependence on the height of F is unavoidable. We get the following result.

Theorem 2.10 (Paper II, Thm. 1.1)**.** *Let $f \in \mathbb{Z}[x_1, \dots, x_n]$ be a polynomial of degree $d \geq 4$ with leading form F. Suppose that F defines a non-singular hypersurface in $\mathbb{P}^{n-1}_{\mathbb{Q}}$. Then*

$$N(f, B) \ll_F B^{n-4+(37n-18)/(n^2+8n-4)}.$$

The uniform version, Theorem 2.3, is derived using a version of Siegel's lemma due to Heath-Brown [16], combined with an application of the determinant method in §3, due to Browning, Heath-Brown and Salberger [7].

3 The determinant method

In this section we shall discuss another method for counting solutions to Diophantine equations, investigated in Papers III and IV in this thesis. Quite contrary to the methods discussed above, the determinant method is most powerful when the number of variables is small compared to the degree of the equation. The method has its origins in a paper by Bombieri and Pila [4] from 1989.

3.1 Uniform bounds for affine curves

Bombieri and Pila proved upper bounds for the number of integral points on plane curves. If $C \subset \mathbb{A}^2$ is an irreducible algebraic curve of degree d, defined over the integers, then their bound has the shape

$$N(C,B) = O_{d,\varepsilon}(B^{1/d+\varepsilon}) \tag{27}$$

for any $\varepsilon > 0$.

The key part of the proof of (27) is the construction of a number of auxiliary curves of low degree. Thus, it is proven that every point in $C(\mathbb{Z},B)$ resides on one of $O_{d,\varepsilon}(B^{1/d+\varepsilon})$ algebraic curves of degree $O_d(1)$. To achieve this, one divides the curve C into small arcs, where it is sufficiently smooth, and for each such arc Γ one exhibits an algebraic curve meeting C in all the integral points of Γ. The number of integral points on the intersection of C with this curve is then $O_d(1)$ by Bézout's Theorem. The existence of the auxiliary curves is established by examining a generalized Vandermonde determinant involving monomials evaluated at integral points, a procedure similar to techniques used in the theory of Diophantine approximation.

A notable feature of the estimate (27), which makes it useful in several contexts, is that the bound does not depend on the coefficients of the defining equation. Thus, for example, Pila [26] uses (27) as base for an induction argument to prove the estimates (7) and (8) above.

3.2 Heath-Brown's p-adic determinant method

An important milestone in the subject of quantitative arithmetic of algebraic varieties is Heath-Brown's paper [16] from 2002, in which the key result is a vast generalization of the one in [4]. It is a sign of its significance that the theorem is often referred to simply as "Theorem 14".

Theorem 3.1 ([16, Thm. 14])**.** *Let $F \in \mathbb{Z}[x_1,\dots,x_n]$ be an absolutely irreducible homogeneous polynomial of degree d, defining a hypersurface $X \subset \mathbb{P}^{n-1}$. Then, for any $\varepsilon > 0$, there is a homogeneous polynomial $G \in \mathbb{Z}[x_1,\dots,x_n] \setminus (F)$ of degree*

$$k \ll_{n,d,\varepsilon} B^{(n-1)d^{-1/(n-2)}+\varepsilon}(\log \|F\|)^{2n-3},$$

all of whose irreducible factors have degree $O_{n,d,\varepsilon}(1)$, such that $G(\mathbf{x}) = 0$ for every $\mathbf{x} \in S(X,B)$.

Remark 3.1. Heath-Brown actually proves a more general statement, for boxes of possibly unequal sidelength. If $\mathbf{B} = (B_1,\dots,B_n)$, then he defines

$$V = B_1 \cdots B_n, \quad T = \max(B_1^{f_1} \cdots B_n^{f_n})$$

where the maximum is taken over all monomials $x_1^{f_1} \cdots x_n^{f_n}$ that occur in F with non-zero coefficient. The statement of the theorem above then holds with $S(X,B)$ replaced by $S(X,\mathbf{B})$ and

$$k \ll_{n,d,\varepsilon} \left(V^d/T\right)^{d^{-(n-1)/(n-2)}} V^{\varepsilon} (\log \|F\|)^{2n-3}.$$

Remark 3.2. The mild dependence on the coefficients of F in the above theorem may in fact be eliminated by appealing to an argument in the spirit of Siegel's lemma [16, Theorem 4]. The same argument appears in our Paper II (Lemma 5.1).

Heath-Brown's version of the determinant method is quite different from that of Bombieri and Pila, but is based upon a variant of the same idea. Let F be as in Theorem 3.1. We may certainly assume that F is primitive, i.e. has coprime coefficients, so that for each prime p, the equation $F(x_1,\dots,x_n) \equiv 0 \pmod{p}$ defines a hypersurface $X_p \subset \mathbb{P}^{n-1}_{\mathbb{F}_p}$. For a prime p one then considers a partition of $S(X,B)$ into subsets $S(X,B,\xi)$, where $S(X,B,\xi)$ is the set of $\mathbf{x} \in S(X,B)$ such that $[\mathbf{x}]$ reduces (mod p) to $\xi \in X_p(\mathbb{F}_p)$. For each *non-singular* $\mathbb{F}_p$-point ξ one gets an auxiliary polynomial, vanishing at every point of $S(X,B,\xi)$, by proving the vanishing of a certain determinant. In other words, integral points are grouped together based on their p-adic distance to each other, whereas Bombieri and Pila considered a covering of small patches defined in the Euclidean metric. Thus we may distinguish between the "real" determinant method of [4], and the "p-adic" determinant method developed by Heath-Brown.

3.3 Further refinements

Several refinements of Heath-Brown's determinant method have appeared. Broberg [5] generalizes Theorem 14 to the case of an irreducible projective variety of any codimension. Broberg uses graded monomial orderings to formulate his result. This notion is elaborated in Paper III, Section 3. In particular, given a monomial ordering $<$ and an irreducible projective variety $X \subseteq \mathbb{P}^n$, we associate to the pair $(<,X)$ an $(n+1)$-tuple $(a_0,\dots,a_n)$ of real numbers satisfying $0 \le a_i \le 1$ and $a_0 + \cdots + a_n = 1$. Broberg considers varieties over an arbitrary number field K, but for simplicity we shall only state the case $K = \mathbb{Q}$ here.

Theorem 3.2 ([5, Thm. 1])**.** *Let $X \subset \mathbb{P}^n$ be an irreducible closed subvariety of dimension m and degree d. Suppose that the ideal $I \subset \mathbb{Q}[x_0,\dots,x_n]$ of X is generated by forms of degree at most δ. Let $\mathbf{B} = (B_0,\dots,B_n)$ be an $(n+1)$-tuple of positive real numbers, and let $<$ be a graded monomial ordering on*

$\mathbb{Q}[x_0,\dots,x_n]$. *Then, for any* $\varepsilon > 0$*, there is a homogeneous polynomial* $G \in \mathbb{Z}[x_0,\dots,x_n] \setminus I$ *of degree*

$$k \ll_{n,\delta,\varepsilon} (B_0^{a_0} \cdots B_n^{a_n})^{(m+1)d^{-1/m}+\varepsilon},$$

all of whose irreducible factors have degree $O_{n,\delta,\varepsilon}(1)$*, such that* $G(\mathbf{x}) = 0$ *for all* $\mathbf{x} \in S(X,\mathbf{B})$.

Remark 3.3. The dependence on δ in the implied constants in Theorem 3.2 may be replaced by a dependence on the degree d of X, by Lemmata 1.3 and 1.4 in Salberger [30].

To understand some of the further developments, we shall have to look a bit closer on the proof of Theorem 14. Thus, let X be a hypersurface as in the theorem. First we note that we can easily dispose of those $\mathbf{x} \in S(X,B)$ that correspond to singular points $[\mathbf{x}] \in X$, incorporating among our auxiliary forms one of the equations defining the singular locus of X. Thus it suffices to count non-singular points. For any given prime p, however, it may happen that a point that is non-singular over $\mathbb{Q}$ still reduces to a singular point on X_p. But it is possible to find a finite set of primes $\mathscr{P}$ with the property that any non-singular point $x \in X(\mathbb{Q})$ reduces to a non-singular point $\xi \in X_p(\mathbb{F}_p)$ for some prime $p \in \mathscr{P}$. Heath-Brown then uses a p-adic Implicit Function Theorem to parameterize the elements of $S(X,B,\xi)$.

Salberger [30] endeavours to count integral points on an affine surface X by a procedure that may be roughly described as follows. First the p-adic determinant method is applied once to obtain a number of curves of bounded degree on X. Then one repeats this a second time with a new prime q, to count integral points on these curves, but retaining also the p-adic congruence conditions from the first step. One is then forced to consider singular $\mathbb{F}_p$-points as well. This refinement of Heath-Brown's determinant method is accomplished in [30], leading to proofs of new cases of the dimension growth conjecture.

Recently, Salberger [28] has developed a new version of the p-adic determinant method, where one uses congruence conditions for (almost) all primes p simultaneously. The output is an auxiliary form whose degree is considerably smaller than that given by Theorem 3.1,

$$k \ll_{n,d,\varepsilon} B^{\frac{n-1}{(n-2)d^{1/(n-2)}}+\varepsilon},$$

but with the serious drawback that there is no smaller upper bound for the degrees of its irreducible factors. However, through an intricate procedure, Salberger is able to interpolate between this result and the one obtained by the original argument, to the effect that every point to be counted belongs either to one of at most k hypersurfaces of bounded degree, or to one of $O(B^{(n-1)d^{-1/(n-2)}+\varepsilon})$ subvarieties of codimension two.

3.4 The basic idea

In all versions of the determinant method, the aim is to construct auxiliary polynomials that vanish at the integral points one wishes to count. In general, given a collection of points $\mathbf{a}_1, \dots, \mathbf{a}_s \in \mathbb{C}^n$, one can consider the interpolation problem of finding a polynomial of degree at most δ that vanishes at $\mathbf{a}_1, \dots, \mathbf{a}_s$. This corresponds to solving a system of equations

$$\sum_{|\alpha| \le \delta} c_\alpha \mathbf{a}_j^\alpha = 0, \quad j = 1, \dots, s, \tag{28}$$

non-trivially in indeterminates c_α, $|\alpha| \le \delta$. Here we use multi-index notation $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, and $|\alpha| = \alpha_1 + \ldots + \alpha_n$ for $\alpha \in \mathbb{Z}^n_{\ge 0}$. Assuming that the system (28) is quadratic, such a non-trivial solution exists if

$$\Delta := \det \left(\mathbf{a}_j^\alpha \right)_{\substack{j=1,\dots,s \\ |\alpha| \le \delta}} = 0.$$

For integral points $\mathbf{a}_1, \dots, \mathbf{a}_s \in \mathbb{Z}^n$, this holds as soon as $|\Delta| < 1$. As for an ordinary Vandermonde determinant, one can make Δ small by choosing the points $\mathbf{a}_i$ close to each other (in the Euclidean sense). Alternatively, for any prime p, Δ will vanish as soon as $|\Delta| \cdot \|\Delta\|_p < 1$, which we may try to achieve by choosing the points close to each other in the p-adic sense.

In our situation, it is of course essential that the auxiliary polynomial does not vanish entirely on the variety under consideration. This may be achieved by restricting the set of monomials $\mathbf{x}^\alpha$ occuring in (28) (see Paper III, §3, where this is elaborated using monomial orderings.) The following example illustrates the basic arguments used to estimate such a monomial determinant, in the real setting.

Example 3.1. Let $(u_1, v_1, w_1), \dots, (u_s, v_s, w_s)$ be points in $[-B, B]^3 \cap \mathbb{Z}^3$ satisfying $f(u_i, v_i, w_i) = 0$ for some polynomial f. For simplicity, let us assume that $(u_1, v_1, w_1) = (0, 0, 0)$. Given a set $\mathscr{M} = (m_1, \dots, m_s)$ of monomials in (x, y, z) of degree $\le \delta$, define the determinant

$$\Delta_0 = \begin{vmatrix} m_1(u_1, v_1, w_1) & \cdots & m_1(u_s, v_s, w_s) \\ \vdots & \ddots & \vdots \\ m_s(u_1, v_1, w_1) & \cdots & m_s(u_s, v_s, w_s) \end{vmatrix}.$$

It is convenient to rescale the problem. The points

$$(x_i, y_i, z_i) = \left(\frac{1}{B} u_i, \frac{1}{B} v_i, \frac{1}{B} w_i \right) \in [-1, 1]^3 \cap \mathbb{Q}^3$$

satisfy $f_B(x_i, y_i, z_i) = 0$, where $f_B(x, y, z) = f(Bx, By, Bz)$. Suppose now that (x_i, y_i, z_i) all lie within a cube $\mathbf{K} \subset [-1, 1]^3$ of sidelength ρ. Suppose furthermore that the subset of the hypersurface $f_B = 0$ bounded by $\mathbf{K}$ can be parameterized as $z = \phi(x, y)$, where ϕ has continuous partial derivatives of any order. Now we have

$$\Delta_0 = B^{\sum_i \deg(m_i)}\Delta,$$

where

$$\Delta = \begin{vmatrix} m_1(x_1, y_1, z_1) & \cdots & m_1(x_s, y_s, z_s) \\ \vdots & \ddots & \vdots \\ m_s(x_1, y_1, z_1) & \cdots & m_s(x_s, y_s, z_s) \end{vmatrix}.$$

Define functions $\psi_i(x, y) = m_i(x, y, \phi(x, y))$ and consider the power series expansion around $(0, 0, 0)$

$$\psi_i(x, y) = P_{i,\nu}(x, y) + O(\rho^{\nu+1}),$$

where $P_{i,\nu}$ is a polynomial of total degree ν, say

$$P_{i,\nu}(x, y) = \sum_{\substack{\alpha \in \mathbb{Z}^2 \\ \alpha_1 + \alpha_2 \le \nu}} c_{i,\alpha} x^{\alpha_1} y^{\alpha_2},$$

and ν is chosen so that $P_{i,\nu}$ has at least s terms (including terms with vanishing coefficient). We may then write

$$\Delta = \Delta' + \mathscr{R},$$

with $\mathscr{R}$ of negligible size and $\Delta' = \det P$, where

$$P = \begin{pmatrix} P_{1,\nu}(x_1, y_1) & \cdots & P_{1,\nu}(x_s, y_s) \\ \vdots & \ddots & \vdots \\ P_{s,\nu}(x_1, y_1) & \cdots & P_{s,\nu}(x_s, y_s) \end{pmatrix}.$$

A basis for the row space of P is furnished by the vectors

$$\mathbf{v}_\alpha = (x_1^{\alpha_1} y_1^{\alpha_2} \ \cdots \ x_s^{\alpha_1} y_s^{\alpha_2}),$$

where $\alpha_1 + \alpha_2 \le \nu$. Since, for each k, the subspace generated by $\{\mathbf{v}_\alpha; \alpha_1 + \alpha_2 = k\}$ has dimension at most $k + 1$, the matrix P is clearly row equivalent to a matrix where the first row has entries of size $O(1)$, the next two rows have entries of size $O(\rho)$, the next three rows have entries of size $O(\rho^2)$, and so on. This yields the estimate

$$\Delta \ll \rho^{1\cdot 2 + 2\cdot 3 + \cdots + \nu(\nu+1)} = \rho^{\nu^3/3 + O(\nu^2)}. \tag{29}$$

(The implied constants, of course, depend upon the size of the partial derivatives of the function ϕ.) It is now a matter of choosing the parameters ρ, δ and ν optimally, in terms of B and the degree of f, to get $|\Delta_0| < 1$.

3.5 The real determinant method for higher-dimensional varieties (Paper III)

In the third paper of this thesis, the real determinant method is developed in higher dimensions. We give a new proof of a result (Paper III, Thm. 1.2) that is essentially Theorem 3.2 above. In particular, we recover Theorem 14. It might seem, at a first glance, that we have achieved a generalization in allowing non-rational coefficients for the defining polynomials, but as Heath-Brown notes [16, Cor. 1] it is easy to find auxiliary hypersurfaces for varieties not defined over $\mathbb{Q}$.

The main obstacle in generalizing the procedure of Bombieri and Pila to higher dimensions has to do with local parameterization. In Example 3.1 above, we considered a patch of our variety parameterized by a smooth function. In other words, to carry out our estimate we had to assume that we were in a situation where the Implicit Function Theorem could be invoked. In particular, singular points have to be handled separately by other means. Furthermore, the implied constants in our bounds depended on the sizes of the partial derivatives of the implicit function. It is thus necessary to control these derivatives to get a bound on the determinant that holds uniformly in all patches. In [4], this is done through a rather elaborate iterative procedure, in which patches where the derivatives oscillate are excised and reparameterized.

(In the p-adic setting, there is also a version of the Implicit Function Theorem [5, Lemma 6], allowing for parameterization of the points in a congruence class $S(X, B, \xi)$ appertaining to a non-singular point $\xi \in X_p(\mathbb{F}_p)$, by p-adic power series.)

In Paper III, we employ a powerful result due to Gromov [11] to tackle the parameterization problem. Let $V \subset \mathbb{A}^n_{\mathbb{R}}$ be an algebraic variety of dimension $m < n$ and degree d, and let $Y = V \cap [-1,1]^n$. Then Yomdin-Gromov's algebraic lemma (Lemma 4.1 in Paper III) states that for each $r \in \mathbb{Z}_+$, Y can be parameterized by $O_{n,r,d}(1)$ functions $[-1,1]^m \to [-1,1]^n$, all of whose partial derivatives of order up to r are continuous and bounded in absolute value by 1. This lemma is an example of the theory of C^k-reparameterization of semi-algebraic sets, first introduced by Yomdin to study topological entropy (see [38] or [39] for an account of this field of research). More generally still, a statement of the same nature can be proven to hold for so called definable sets in o-minimal structures. This is proven in [27], where it is used to prove a theorem on the paucity of rational points of such sets.

From Theorem 1.2 in Paper III it is not difficult to derive an affine version, containing the estimate (27) as a special case.

Theorem 3.3 (Paper III, Thm. 1.1). *Let $X \subset \mathbb{A}^n_{\mathbb{R}}$ be an irreducible closed subvariety of dimension m and degree d, and let $I \subset \mathbb{R}[x_1, \dots, x_n]$ be the ideal of X. Then, for any $\varepsilon > 0$, there exists a polynomial $g \in \mathbb{Z}[x_1, \dots, x_n] \setminus I$ of degree*

$$k \ll_{n,d,\varepsilon} B^{md^{-1/m}+\varepsilon},$$

all of whose irreducible factors have degree $O_{n,d,\varepsilon}(1)$, such that $g(\mathbf{x}) = 0$ for each $\mathbf{x} \in X(\mathbb{Z}, B)$.

3.6 An approximative determinant method. Sums and differences of k-th powers (Paper IV)

The fourth paper in this thesis (see also §1.5) deals with counting the number of representations of a positive integer N by a diagonal form, that is, integral solutions to the equation

$$a_1 x_1^k + a_2 x_2^k + a_3 x_3^k + a_4 x_4^k = N. \tag{30}$$

In general, let $F(x_1, x_2, x_3, x_4)$ be a non-singular homogeneous polynomial of degree k. We want to count integral solutions to the equation

$$F(x_1, x_2, x_3, x_4) = N \tag{31}$$

with $|x_i| \leq B$. As a first approach, we may apply Theorem 3.3 to the three-dimensional affine hypersurface defined by (31), to obtain a collection of $O_{k,\varepsilon}(B^{3/k^{1/3}+\varepsilon})$ auxiliary hypersurfaces containing all points we want to count.

Suppose, however, that the positive integer N is considerably smaller than B^k. Then a primitive integer quadruple (x_1, x_2, x_3, x_4) satisfying (31) corresponds to a point in $\mathbb{P}^3(\mathbb{Q})$ lying, in a certain sense, *near* the projective surface defined by

$$F(x_1, x_2, x_3, x_4) = 0. \tag{32}$$

Seeing as Theorem 3.1 would yield a collection of $O_{k,\varepsilon}(B^{3/\sqrt{k}})$ auxiliary forms for rational points of height at most B *on* the surface (32), one could hope to improve the exponent $3/k^{1/3}$ by incorporating this additional information into the determinant method.

Such an approximative version of the determinant method was recently developed by Heath-Brown [17] for studying the corresponding problem in three variables, and that work provides the main ideas for our approach in Paper IV. We prove that every solution to (31) (or indeed, to the corresponding *inequality*) satisfies one of

$$O_{F,N,\varepsilon}(B^{16/(3\sqrt{3k})+\varepsilon})$$

auxiliary homogeneous equations (Paper IV, Prop. 3.1). Thus we successfully interpolate between the exponents $3/k^{1/3}$ and $3/\sqrt{k}$ discussed above.

In the case of a diagonal form

$$F(x_1, x_2, x_3, x_4) = a_1 x_1^k + a_2 x_2^k + a_3 x_3^k + a_4 x_4^k,$$

we proceed by applying the results from [28] described above to each affine surface

$$F(x_1, x_2, x_3, x_4) - N = A_i(x_1, x_2, x_3, x_4) = 0$$

obtained by the above procedure. Here A_i denotes an auxiliary form. The final ingredient in our estimate for the number of representations is a lower bound for the degrees of curves on Fermat hypersurfaces, due to Salberger [28].

References

[1] V. V. Batyrev and Yu. I. Manin. Sur le nombre des points rationnels de hauteur borné des variétés algébriques. *Math. Ann.*, 286(1-3):27–43, 1990.

[2] Victor V. Batyrev and Yuri Tschinkel. Rational points on some Fano cubic bundles. *C. R. Acad. Sci. Paris Sér. I Math.*, 323(1):41–46, 1996.

[3] B. J. Birch. Forms in many variables. *Proc. Roy. Soc. Ser. A*, 265:245–263, 1961/1962.

[4] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.

[5] Niklas Broberg. A note on a paper by R. Heath-Brown: "The density of rational points on curves and surfaces" [Ann. of Math. (2) **155** (2002), no. 2, 553–595; mr1906595]. *J. Reine Angew. Math.*, 571:159–178, 2004.

[6] T. D. Browning and D. R. Heath-Brown. Rational points on quartic hypersurfaces. *J. Reine Angew. Math.*, 629:37–88, 2009.

[7] T. D. Browning, D. R. Heath-Brown, and P. Salberger. Counting rational points on algebraic varieties. *Duke Math. J.*, 132(3):545–578, 2006.

[8] Timothy D. Browning. *Quantitative arithmetic of projective varieties.* Progress in Mathematics 277. Basel: Birkhäuser. xi, 160 p., 2009.

[9] Pierre Deligne. La conjecture de Weil. I. *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.

[10] S. W. Graham and G. Kolesnik. *van der Corput's method of exponential sums*, volume 126 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1991.

[11] M. Gromov. Entropy, homology and semialgebraic geometry. *Astérisque*, (145-146):5, 225–240, 1987. Séminaire Bourbaki, Vol. 1985/86.

[12] Robin Hartshorne. *Ample subvarieties of algebraic varieties*. Notes written in collaboration with C. Musili. Lecture Notes in Mathematics, Vol. 156. Springer-Verlag, Berlin, 1970.

[13] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977.

[14] D. R. Heath-Brown. Hybrid bounds for Dirichlet L-functions. *Invent. Math.*, 47(2):149–170, 1978.

[15] D. R. Heath-Brown. The density of rational points on nonsingular hypersurfaces. *Proc. Indian Acad. Sci. Math. Sci.*, 104(1):13–29, 1994.

[16] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. of Math. (2)*, 155(2):553–595, 2002.

[17] D. R. Heath-Brown. Sums and differences of three kth powers. *J. Number Theory*, 129(6):1579–1594, 2009.

[18] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[19] C. Hooley. On the representations of a number as the sum of four cubes. I. *Proc. London Math. Soc. (3)*, 36(1):117–140, 1978.

[20] C. Hooley. On the number of points on a complete intersection over a finite field. *J. Number Theory*, 38(3):338–358, 1991.

[21] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[22] Nicholas M. Katz. Estimates for "singular" exponential sums. *Internat. Math. Res. Notices*, (16):875–899, 1999.

[23] Wenzhi Luo. Rational points on complete intersections over $\mathbf{F}_p$. *Internat. Math. Res. Notices*, (16):901–907, 1999.

[24] Kurt Mahler. Note on hypothesis *K* of Hardy and Littlewood. *J. Lond. Math. Soc.*, 11:136–138, 1936.

[25] Emmanuel Peyre. Points de hauteur bornée et géométrie des variétés (d'après Y. Manin et al.). *Astérisque*, (282):Exp. No. 891, ix, 323–344, 2002. Séminaire Bourbaki, Vol. 2000/2001.

[26] J. Pila. Density of integral and rational points on varieties. *Astérisque*, (228):4, 183–187, 1995. Columbia University Number Theory Seminar (New York, 1992).

[27] J. Pila and A. J. Wilkie. The rational points of a definable set. *Duke Math. J.*, 133(3):591–616, 2006.

[28] Per Salberger. Counting rational points on projective varieties. Preprint, 2009.

[29] Per Salberger. Integral points on hypersurfaces of degree at least three. unpublished.

[30] Per Salberger. On the density of rational and integral points on algebraic varieties. *J. Reine Angew. Math.*, 606:123–147, 2007.

[31] Stephen Hoel Schanuel. Heights in number fields. *Bull. Soc. Math. France*, 107(4):433–449, 1979.

[32] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, 1994.

[33] J. G. van der Corput. Zahlentheoretische Abschätzungen. *Math. Ann.*, 84:53–79, 1921.

[34] J. G. van der Corput. Verschärfung der Abschätzung beim Teilerproblem. *Math. Ann.*, 87:39–65, 1922.

[35] H. Weyl. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Ann.*, 77:313–352, 1916.

[36] Joel M. Wisdom. *On the representation of numbers as sums of powers*. PhD thesis, University of Michigan, 1998.

[37] Joel M. Wisdom. On the representations of a number as the sum of four fifth powers. *J. London Math. Soc. (2)*, 60(2):399–419, 1999.

[38] Y. Yomdin. Analytic reparametrization of semi-algebraic sets. *J. Complexity*, 24(1):54–76, 2008.

[39] Yosef Yomdin and Georges Comte. *Tame geometry with application in smooth analysis*, volume 1834 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2004.

Corrections to the papers

The versions of Paper I and Paper II included in this thesis differ from the published versions on the following points.

Paper I

In Lemma 2.9, we have added the hypothesis $q \nmid (d_i - 1)$ for $i = 1, \ldots, r$. We have also removed an erroneous, but superfluous, assertion made in the proof of (i).

Paper II

1. In Lemma 4.1, the notation for the "differenced" weight functions used was not consistent with the definition in Notation 4.2. Thus, we have changed this notation slightly throughout Lemma 4.1 and its proof.

2. In Lemma 5.1, we have added the hypothesis that the coefficients of f be coprime, which is of course no restriction in the application of the result.