The Determinant Method and Applications



Thomas Reuss
St Anne's College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy
Michaelmas Term 2015

Acknowledgements

I would like to thank my supervisor Roger Heath-Brown who introduced me to my research and guided me through this project. I thank him for the invaluable help and many insightful discussions during the last three and a half years.

I very much thank my parents for always having supported and believed in me.

Very special thanks goes to my friend Suhail who has shared and supported my path during the last eight years.

I thank Ian very much for all his support and valuable advice.

I am also very grateful to St. Anne's College and the St. Anne's College mathematics tutors for funding and supporting me during this project.

Special thanks goes to Hilary Priestley who has continuously inspired, guided and supported me since the start of my undergraduate degree almost 8 years ago.

I wish to thank Petra Aehle for introducing me to the beautiful world of mathematics. Without her, this thesis would never have existed.

Finally, I would like to thank Clara, Yvonne and aunt Debbie for their support during the last few years!

Thomas Reuss, Oxford, January 2015.

Abstract

The thesis is structured into 5 chapters as follows:

Chapter 1 is an introduction to the tools and methods we use most frequently.

Chapter 2 Pairs of k-free Numbers, consecutive square-full Numbers.

In this chapter, we refine the approximate determinant method by Heath-Brown. We present applications to asymptotic formulas for consecutive k-free integers, and more generally for k-free integers represented by r-tuples of linear forms. We also show how the method can be used to derive an upper bound for the number of consecutive square-full integers. Finally, we apply the method to make a statement about the size of the fundamental solution of Pell equations.

Chapter 3 Power-Free Values of Polynomials.

A conjecture by Erdős states that for any irreducible polynomial f of degree $d \geq 3$ with no fixed $(d-1)$-th power prime divisor, there are infinitely many primes p such that $f(p)$ is $(d-1)$-free. We prove this conjecture and derive the corresponding asymptotic formulas.

Chapter 4 Integer Points on Bilinear and Trilinear Equations. In the fourth chapter, we derive upper bounds for the number of integer solutions on bilinear or trilinear forms.

Chapter 5 In the fifth chapter, we present a method to count the monomials that occur in the projective determinant method when the method is applied to cubic varieties.

Contents

1 Introduction **1**

1.1 Counting Solutions to Diophantine Equations 2

1.1.1 Examples 3

1.1.2 A simple heuristic argument 5

1.1.3 Known Results and the Dimension Growth Conjecture 6

1.2 The Determinant Method 8

1.2.1 The Basic Ideas 8

1.2.2 The Real Determinant Method 10

1.2.3 The Projective Determinant Method 11

1.2.4 The Approximate Determinant Method 13

1.3 Results about Lattices 15

2 Pairs of k-free Numbers, consecutive square-full Numbers **17**

2.1 Introduction 17

2.2 The Proof of Theorem 5 23

2.2.1 Determinant Method 25

2.2.2 Counting Solutions 30

2.2.3 Completion of the proof of Theorem 5 34

2.3 The Proof of Theorem 6 36

2.3.1 Preliminaries 36

2.3.2 The proof of Theorem 6 for $k \geq 3$ 38
2.3.3 Counting Points on Lines, Finishing the proof for $k = 2$ 40
2.3.4 The trivial error term for Theorem 6 47
2.3.5 A connection between $S_2(x)$ and the Riemann ζ-function . . . 48
2.3.6 Theorem 6 and the Riemann ζ-function 49
2.4 The Proof of Theorem 7 51
2.5 The Proof of Theorem 8 56
2.6 The Proof of Theorem 9 and Corollary 10 60

3 Power-Free Values of Polynomials 63
3.1 Introduction 63
3.2 Preliminaries 66
3.3 Analysis in $\mathbb{Q}(\theta)$ 71
3.4 Applying the Approximate Determinant Method 76
3.5 Counting Points inside a box 82
3.6 Finishing the Proof 88

4 Integer Points on Bilinear and Trilinear Equations 90
4.1 Introduction 90
4.2 Bilinear Forms 91
4.3 Trilinear Forms 95

5 Counting Monomials for Cubic Varieties 112
5.1 Introduction 112
5.2 Linear Changes 114
5.3 Notation 116
5.4 Eliminating zero Columns 117
5.5 Calculating $\nu_p(\Delta)$ 120

Bibliography **127**

Chapter 1

Introduction

In this thesis, we are interested in the determinant method and we present various applications of it. The determinant method is a tool to count integer solutions of Diophantine equations. The study of such equations is one of the oldest branches in number theory and mathematics. We give a brief survey of Diophantine equations in section 1.1, highlighting some interesting examples and motivations.

The principal tool in the proofs of most of our papers is the determinant method. Section 1.2 describes the basic ideas and different versions of our methods.

We make frequent use of lattices when working with the determinant method. Section 1.3 outlines the basic results about lattices needed in this thesis.

1.1 Counting Solutions to Diophantine Equations

The key objects of our interest in this thesis are *Diophantine* equations. A Diophantine equation is of the form

$$F(x_1, \ldots, x_n) = 0, \tag{1.1}$$

where F is a polynomial with integer coefficients, and one is interested in studying the points $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ that satisfy (1.1). Such problems are often very intriguing, difficult and have been studied by mathematicians for a very long time. Indeed, the term *Diophantine equation* refers to the mathematician Diophantus of Alexandria who studied the equations sometime around AD 200-300. One can ask whether a Diophantine equation has any (non-trivial) solution at all. The most famous example in this case is perhaps the equation related to *Fermat's Last Theorem*:

$$x^n + y^n = z^n,$$

where $n \geq 3$ is a fixed integer. It was first conjectured by Fermat in 1637 that there are no integer solutions (x, y, z) to this equation with $xyz \neq 0$ and only in 1995 Andrew Wiles published the first complete proof of Fermat's claim. One can also ask for an algorithm that finds one or all the points on a Diophantine equation in a finite number of steps. Unfortunately, such an algorithm cannot exist for a general Diophantine equation, and it is therefore often interesting to look at Diophantine equations in a third way: When we cannot prove that there are no or finitely many solutions, it is interesting to estimate the number of solutions, for example, inside large boxes. This is where the determinant method shines, and where our main interest lies.

The equation (1.1) defines a hypersurface in $\mathbb{A}^n$. If F is a homogeneous polynomial then it defines a projective hypersurface in $\mathbb{P}^{n-1}$ and projective points on this hyper-

surface correspond to non-zero solutions of (1.1). As we described above, we want to count points $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ with $|x_i| \leq B_i$, say that satisfy (1.1). This means that we count solutions inside certain boxes and hope to get an upper bound on the number of solutions in terms of the numbers B_i or the properties of F. More specifically, we wish to bound the quantity

$$N(F, \mathbf{B}) = \#\left\{(x_1, \ldots, x_n) \in \mathbb{Z}^n : F(x_1, \ldots, x_n) = 0, |x_i| \leq B_i\right\}.$$

If F is homogeneous then we consider $(x_1, \ldots, x_n)$ as a projective point, and thus in this case it makes sense to only count points when $\gcd(x_1, \ldots, x_n) = 1$. We will use the same notation for $N(F, \mathbf{B})$, whether or not F is homogeneous. When all the B_i are equal to B, say then we write $N(F, B)$ instead of $N(F, \mathbf{B})$. Note that we write $f \ll g$ or $f = O(g)$ to say that there is a positive constant C such that $|f| \leq Cg$. We use this notation for functions f and g, where $g > 0$. It will be clear from the context over which values the inequality holds. If the constant C depends on parameters, we denote these parameters by subscripts. Furthermore, we write $f \asymp g$ to say that there are two positive constants C_1 and C_2 such that $C_1|g| \leq |f| \leq C_2|g|$. We also use the notation $E \sim C$ to say that $C \leq |E| < 2C$.

1.1.1 Examples

We consider some interesting examples:

1. In *Waring's Problem* (see for example Davenport [9]), one asks for the least integer s such that any sufficiently large integer N can be written as a sum of s k-th powers. This question leads to the equation

$$x_1^k + \ldots + x_s^k = N.$$

If we study the related Diophantine equation

$$x_1^k + \ldots + x_s^k = x_{s+1}^k + \ldots + x_{2s}^k,$$

subject to $|x_i| \leq B$ and if we can show that the number of solutions to this equation is $O(B^{2s-k+\epsilon})$ for any $\epsilon > 0$ then one can derive an asymptotic formula for the number of representations, provided s is large enough.

2. In this thesis, we will examine various problems about power-free values. These problems lead then to related Diophantine equations. For example, we expect - taken aside obvious exceptions - that for any irreducible polynomial f, there are infinitely many integers n such that $f(n)$ is k-free. This problem then leads to the study of the Diophantine equation

$$f(n) = a^k b$$

inside a certain box. Similarly, if one wants to show that there are infinitely many consecutive k-free integers, one obtains the two Diophantine equations $n = a^k b$ and $n = c^k d$ inside certain boxes. By eliminating n, this leads to the study of the equation

$$a^k b - c^k d = 1.$$

3. In the special case of *Manin's conjecture* for non-singular cubic projective surfaces, one considers the case when $F(x_1, x_2, x_3, x_4)$ is a non-singular cubic form with integer coefficients. If there is at least one non-zero integer point on the variety defined by F and if the surface defined by $F = 0$ contains no $\mathbb{Q}$-lines, then Manin's conjecture predicts that

$$N(F, B) \sim cB(\log B)^{r-1},$$

for some suitable constant c, and where r is the rank of the Picard group of the surface $F = 0$. This conjecture is too hard for current methods, even the weaker result that there are only $O(B^{1+\epsilon})$ non-trivial solutions seems out of reach.

1.1.2 A simple heuristic argument

Let $F(x_1, \ldots, x_n)$ be a polynomial of degree $d \leq n$. Note that if $|x_i| \leq B$ for all i then $F(\mathbf{x}) \ll B^d$. Thus, one might argue that the probability that $F(\mathbf{x})$ vanishes for a randomly chosen $\mathbf{x}$ is B^{-d}. There are B^n choices for $\mathbf{x}$. Thus, one might heuristically guess that

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

In a classical result, Birch [2] has used the circle method to prove this heuristic claim for non-singular homogeneous polynomials F of degree d with n variables, provided $n > (d-1)2^d$ and assuming that the equation $F(\mathbf{x}) = 0$ has a non-zero solution in $\mathbb{R}$ and each $\mathbb{Q}_p$. Considering Birch's results, it is particularly interesting to obtain estimates for $N(F, B)$ when the number of variables is relatively small compared to d. This is indeed the case when the determinant method may provide good or optimal results. The heuristic argument can fail, as the example

$$x_1^3 + x_2^3 = x_3^3 + x_4^3$$

shows. Here, we get $\gg B^2$ solutions of the form (a, b, a, b) and thus, we cannot have $N(f, B) \ll B^{n-d} = B$. However, the points (a, b, a, b) lie on a line and it is then a natural questions to bound the number of points not lying on a line contained in the surface. We follow a similar strategy in chapter 2 to refine our bound for consecutive square-free integers.

1.1.3 Known Results and the Dimension Growth Conjecture

This section will only provide a very brief survey. As a starting point, the interested reader should consult Heath-Brown [19] for further details. Let F be an irreducible form of degree d in $n \geq 2$ variables. The trivial bound for $N(F, B)$ is

$$N(F, B) \ll B^{n-1}$$

There are many improvements on this trivial bound. Historically, the first improvement is due to Cohen who showed that

$$N(F, B) \ll_{\epsilon, F} B^{n-3/2+\epsilon}.$$

His argument can be found in the appendix of Heath-Brown [20]. An important general improvement of the trivial bound is due to Pila [36]. He shows that

$$N(F, B) \ll_{\epsilon} B^{n-2+1/d+\epsilon}.$$

Pila uses an inductive argument based on a paper by Bombieri and Pila [3]. We can see that their bound is essentially optimal in the case $n = 2$. As an example, consider the curve given by $y = x^d$. This curve has $\gg B^{1/d}$ integer solutions of the form (a, a^d) with $|a| \leq B$. The key ingredient of their proof is the determinant method. In the case of quadratic forms, one can do better. One can show that

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

This removes the $1/d$ in Pila's exponent and Heath-Brown has conjectured that this might be possible for forms of general degree d. Heath-Brown's conjecture asks whether $N(F, B) \ll_{\epsilon} B^{n-2+\epsilon}$ for irreducible forms F. The conjecture has now been

proven when the absolute constant is allowed to depend on F. In the case when the constant has to be independent of F, the conjecture has been proven in most cases. The remaining case is when F is a certain singular cubic hypersurface. Exponential sums, the circle method and determinant method have been used.

1.2 The Determinant Method

The Determinant Method is a tool for counting solutions of Diophantine equations. It seems most powerful when the number of variables is small. In this section, we will describe the first version of the determinant method developed by Bombieri and Pila [3] and will then show how the method was further refined by Heath-Brown [18]. The determinant method is more efficient in counting rational points on algebraic varieties with smaller dimension. For example, the method is essentially optimal if we use it to count points on plane curves but the results that one obtains with the determinant method in problems with higher dimension usually get weaker as the dimension increases.

In the following section we will outline the original Bombieri-Pila method which is essentially affine in nature, and we will then sketch in the section thereafter how Heath-Brown simplified and developed some aspects of their method so that it works efficiently in projective problems as well.

1.2.1 The Basic Ideas

In all forms of the determinant method, the idea is to construct auxiliary polynomials that vanish at the solutions of the equation $F = 0$ that one wants to count. Consider a list of points $\mathbf{x}^{(1)}, \dots, \mathbf{x}^{(N)} \in \mathbb{Z}^n$, say. Let $\mathcal{M}$ be a set of monomials in the unknowns $x_1, \dots, x_n$, and let $M = |\mathcal{M}|$. If we want to construct a polynomial with monomials from $\mathcal{M}$ such that the constructed polynomial vanishes at these N points, then this leads to the equation system

$$\sum_{m \in \mathcal{M}} c_m m(\mathbf{x}^{(i)}) = 0, \qquad (i = 1, \dots, N). \tag{1.2}$$

Here, $m(\mathbf{x}^{(i)})$ is the monomial m evaluated at the point $\mathbf{x}^{(i)}$. The equation system can be rewritten as a matrix-vector multiplication. Let

$$\mathcal{C} = [m(\mathbf{x}^{(i)})]_{i \leq N,\ m \in \mathcal{M}}$$

be the $N \times M$ matrix which has the monomials evaluated at the points $\mathbf{x}^{(i)}$ as its entries. Let $\mathbf{c} = (c_m)_{m \in \mathcal{M}}$ be the $M \times 1$ coefficient vector. Then, the system (1.2) has a solution $\mathbf{c}$ if and only if the system $\mathcal{C}.\mathbf{c} = \mathbf{0}$ has a solution $\mathbf{c}$. Of course, we are only interested in a non-trivial vector $\mathbf{c} \neq 0$. Such a non-zero solution exists if and only if the rank of $\mathcal{C}$ is less than M. Let Δ be the determinant of the first $M \times M$ submatrix of $\mathcal{C}$. It is then an elementary result in Linear Algebra that a non-zero solution $\mathbf{c}$ of the system (1.2) exists if and only if $\Delta = 0$. Thus, the problem of constructing an auxiliary equation has been reduced to showing that a certain determinant with entries of the form $m(\mathbf{x}^{(i)})$ vanishes. Since the matrix $\mathcal{C}$ is an integer matrix, it suffices to show that $|\Delta| < 1$ to guarantee that $\Delta = 0$. Like for ordinary Vandermonde determinants, if we chose the points $\mathbf{x}^{(i)}$ close to each other in the Euclidean sense then Δ will become small. This is the basic idea in the Bombieri-Pila determinant method, where points are grouped together based on their real distances. A second idea is to consider the p-adic norm of Δ for a suitably large prime $p \asymp P$. If we can show that $p^\nu \mid \Delta$ and that $\Delta \ll B_\Delta$, say and if we can chose $P \gg B_\Delta^{1/\nu}$ with a suitable absolute constant, then $\Delta = 0$. The idea of the projective determinant method is due to Heath-Brown [18]. His method can be seen as a generalization and - in many cases - a simplification of the Bombieri-Pila method. It should be noted what the challenges are when one tries to apply the determinant method. A challenge one encounters when choosing the monomial set $\mathcal{M}$ is to ensure that the auxiliary equation is not just a multiple of the original equation F. It is not always clear what the optimal choice of monomials might be. A further challenge is to calculate $\|\Delta\|_p$

in the p-adic case or to bound $|\Delta|$ in the real case. One wants to use the equation $F = 0$ to eliminate one of the variables from $\mathcal{C}$. This then results in a matrix where each entry is a polynomial or even a power series. It can then be difficult to see what $\|\Delta\|_p$ is because the cancellation in the determinant can be challenging to exploit. In chapter 5, we present an example on how to apply the p-adic determinant method to cubic varieties. We avoid the question on how to chose monomials, by slightly adapting Heath-Brown's arguments, and we calculate the optimal value ν such that $p^\nu \mid \Delta$.

1.2.2 The Real Determinant Method

In [3], Bombieri and Pila consider the quantity

$$N(F, B) = \#\left\{(x, y) \in \mathbb{Z}^2 : F(x, y) = 0, |x| \leq B, |y| \leq B\right\},$$

where $F(x, y) \in \mathbb{R}[x, y]$ is an irreducible polynomial of degree $d \geq 2$. Bombieri and Pila showed with this method that

$$N(F, B) \ll_{d,\epsilon} B^{1/d+\epsilon} \tag{1.3}$$

for any $\epsilon > 0$. This is essentially the optimal bound as the example $F(x, y) = x^d - y$ shows. In this example we have $\gg B^{1/d}$ solutions of the form (a, a^d). We point out that the ϵ in the error exponent of 1.3 has been removed in the projective setting. It has also been removed in the affine case when F defines a cubic curve in Weierstrass form. A remarkable feature in the estimate (1.3) is that the implicit constant depends only on ϵ and d. It is independent of the coefficients of F, which in applications is often most useful. In the work in this thesis, we are most interested in hypersurfaces given by a polynomial F but it should be noted that the Bombieri-Pila method also works for general irreducible algebraic curves $C \subset \mathbb{A}^2$, even analytic curves. The

general idea of the Bombieri-Pila method is to start with the curve $F(x, y) = 0$ and then to construct $O_{d,\epsilon}(B^{1/d+\epsilon})$ algebraic auxiliary curves $\{F_k\}_{k\in K}$, say. The degrees of these auxiliary curves are bounded in terms of d only. These auxiliary curves have the feature that for all (x, y) counted by $N(F, B)$, we have $F_k(x, y) = 0$ for some $k \in K$. One can then use Bézout's theorem to show that each of the $O_{d,\epsilon}(B^{1/d+\epsilon})$ auxiliary curves has at most $O_d(1)$ intersections with the curve defined by $F(x, y) = 0$. This then yields the estimate (1.3). Pila uses this result for an inductive argument to prove the estimate mentioned in section 1.1.3.

1.2.3 The Projective Determinant Method

In his work, Heath-Brown considers equations of the form $F(x_1, \ldots, x_n) = 0$ where $F \in \mathbb{Z}[x_1, \ldots, x_n]$ is an absolutely irreducible polynomial of degree $d \geq 2$. The first theorem that we will illustrate is concerned with the case when F is homogeneous and thus when it defines a hypersurface in $\mathbb{P}^{n-1}$. We are interested in the quantity

$$N(F, B) = \#\{\mathbf{x} \in \mathbb{Z}^n : F(\mathbf{x}) = 0, \mathrm{hcf}(\mathbf{x}) = 1, \max_{1\leq i\leq n} |x_i| \leq B\},$$

where $B \geq 2$. We have the following central theorem due to Heath-Brown:

Theorem 1. *Let $\epsilon > 0$. Then there exist*

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

nonzero auxiliary forms $F_1(\mathbf{x}), \ldots, F_k(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ coprime to $F(\mathbf{x})$ and an integer $D = D(n, d, \epsilon)$ such that the degree of each F_i is at most D and every point $\mathbf{x}$ counted by $N(F, B)$ is a zero of some F_i.

In his paper, Heath-Brown also deduced a similar result for the affine situation. This extension of Theorem 1 does deal with general boxes $|x_i| \leq B_i$. We will state

this theorem here for comparison:

Theorem 2. *Let $F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be an absolutely irreducible polynomial of degree $d \geq 2$ and let $\epsilon > 0, B_1, \dots, B_n \geq 2$ be given. Define*

$$T = \max \left\{ \prod B_i^{e_i} \right\},$$

where the maximum is taken over all integer tuples $(e_1, \dots, e_n)$ for which the corresponding monomial $\mathbf{x}^{\mathbf{e}}$ appears in F with nonzero coefficient.
Then we can find $D = D(n, d, \epsilon)$ and

$$k \ll_{n,d,\epsilon} T^{\epsilon} \exp \left\{ (n-1) \left(\frac{\prod_i \log B_i}{\log T} \right)^{1/(n-1)} \right\} (\log \|F\|)^{2n-3}$$

auxiliary polynomials $F_1(\mathbf{x}), \dots, F_k(\mathbf{x}) \in \mathbb{Z}[x_1, \dots, x_n]$, coprime to $F(\mathbf{x})$ and with degrees at most D, such that every point $\mathbf{x}$ counted by $N(F; \mathbf{B})$ is a zero of some $F_j(\mathbf{x})$.

The proofs of Theorems 1 and 2, are based on the same key ideas. Let F be as described in Theorem 1. One then considers the equation $F(x_1, \dots, x_n) = 0$ modulo large enough primes p. One then considers the sets

$$S(F, B, p, \mathbf{t}) = \{\mathbf{x} \in \mathbb{Z}^n : |x_i| \leq B, \mathbf{x} \equiv \rho \mathbf{t} \pmod{p} \text{ for some } \rho \in \mathbb{Z}\},$$

where $\mathbf{t}$ goes through a set of projective representatives of the non-singular points for the curve $F = 0$ over $\mathbb{F}_p$. Every such $\mathbf{t}$ will then lift to an auxiliary equation $F(\mathbf{x}; \mathbf{t})$, say, which then vanishes at every point of $S(F, B, p, \mathbf{t})$.

In the Bombieri-Pila method, points are grouped together based on their Euclidean distance, and each auxiliary equation comes from a certain chunk of the curve. In the Heath-Brown method, points are separated depending on their p-adic residue classes. Thus, the Bombieri-Pila method is often refereed to as the real determinant method,

while Heath-Brown's method is called p-adic determinant method.

It is important to note that the dependence on the coefficients of F in theorems 1 and 2 may be eliminated by an argument similar to the one in [18, Theorem 4]. By using Bézout's Theorem and Theorem 2, the Bombieri-Pila bound for curves can be recovered by the Heath-Brown methods.

Various generalizations of the results discussed in this section have been developed. See for example Broberg [5], Salberger [39] or Ellenberg and Venkatesh [12]. Broberg generalized Theorem 1 to irreducible algebraic varieties $X \subseteq \mathbb{P}^n$ of arbitrary dimension m. Broberg's results hold over a general number field K. Salberger developed a variant of the p-adic determinant method that allows to consider congruence conditions for most primes p simultaneously. Ellenberg and Venkatesh managed to introduce a dependence of $\|F\|$ into the bound in Theorem 1 such that larger coefficients mean a smaller number k of auxiliary forms. It should also be noted that the ϵ in Theorem 1 has now been removed in some cases. In the projective setting, Walsh [46] has removed the ϵ. In particular, he showed that if F defines an irreducible curve in $\mathbb{P}^n$ then

$$N(F, B) \ll_d N^{2/d},$$

where Heath-Brown's work would have given an upper bound $O_\epsilon(N^{2/d+\epsilon})$. Mendes Da Costa [8] has shown that the if F defines an elliptic curve over $\mathbb{Z}$ in Weierstrass form then the Bombieri-Pila estimate which gives a bound $O(B^{1/3+\epsilon})$ can be improved to $O(B^{1/3-\delta})$ for some δ independent of F. Both Walsh and Mendes Da Costa use the work by Ellenberg and Venkatesh in [12] to obtain their results.

1.2.4 The Approximate Determinant Method

In chapter 2 and 3, we use the approximate determinant method. We briefly explain the principal motivation of the method. In chapter 2, we want to find an upper bound

to the number of solutions to the equation $a^2b - c^2d = 1$. This equation defines a three-fold, and we wish to reduce the dimension of the problem, since the determinant method performs more effectively on problems with smaller dimension. We note that $t = s^2 + O(\mathcal{E})$, where $t = b/d$ and $s = a/b$ and $\mathcal{E} = 1/(b^2d)$ is considered small. With this idea, we can convert our problem from one where we count integer points on a three-fold to one where we count rational points close to a curve. The determinant method seems to do rather well in the latter. Thus, in the approximate determinant method we work with an approximate equation $F(x_1, \ldots, x_n) \ll \mathcal{E}$, where $\mathcal{E}$ should be small. Here, one has to apply the real determinant method. The ideas are as described in the previous section, only that this time, the approximate equation has to be used to eliminate one of the variables from the matrix. The ideas of the approximate determinant method were first introduced by Heath-Brown in [21] and [22].

1.3 Results about Lattices

In our work (most notable in chapter 4), we will frequently use the following fact about lattices:

Lemma 3. *Let $\Lambda \subseteq \mathbb{Q}^n$ be a lattice of dimension m. Then Λ has a basis $\mathbf{b}^{(1)}, \dots, \mathbf{b}^{(m)}$ such that for every $\mathbf{x} = \sum_i \lambda_i \mathbf{b}^{(i)} \in \Lambda$, we have that*

$$\lambda_i \ll \frac{|\mathbf{x}|}{|\mathbf{b}^{(i)}|}.$$

Furthermore,

$$\det(\Lambda) \asymp \prod |\mathbf{b}^{(i)}|.$$

We note that by a lattice $\Lambda \subseteq \mathbb{Q}^n$ we mean a discrete additive subgroup of $\mathbb{Q}^n$. In particular, this implies that Λ is a finitely generated $\mathbb{Z}$-module. Thus, we may write $\Lambda = L\mathbb{Z}^m$, where L is a $m \times m$ matrix with coefficients in $\mathbb{Q}$. Let $M = \lambda I_m$ be a λ multiple of the $m \times m$ identity matrix such that ML is an integer matrix and $M\Lambda$ an integer lattice. Davenport's argument in [10, Lemma 5] now gives that $M\Lambda$ has a basis $\mathbf{g}^{(1)}, \dots, \mathbf{g}^{(m)}$ such that if we write $\mathbf{x} = \sum_i \lambda_i \mathbf{g}^{(i)} \in M\Lambda$ then

$$\lambda_i \ll \frac{|\mathbf{x}|}{|\mathbf{g}^{(i)}|}.$$

Furthermore,

$$\det(M\Lambda) \asymp \prod |\mathbf{g}^{(i)}|.$$

Note that $\det(M\Lambda) = \lambda^m \det(\Lambda)$ and $|M\mathbf{w}| = |\lambda||\mathbf{w}|$ for any vector $\mathbf{w} \in \mathbb{R}^m$. Thus, if we set $\mathbf{b}^{(i)} = M^{-1}\mathbf{g}^{(i)}$ for $i = 1, \dots, m$ then $\mathbf{b}^{(1)}, \dots, \mathbf{b}^{(m)}$ is a basis of Λ with the properties as stated in the Lemma.

We use this lemma to estimate the number of primitive points in $\Lambda \cap R$, where Λ is a lattice and R a region. Let us consider an example, on how one can apply this

lemma in the simple case when $\Lambda \subseteq \mathbb{Z}^2$ and R is the sphere $\{\mathbf{x} \in \mathbb{R}^2 : |x_i| \leq B\}$ (see Heath-Brown [18]). It is clear that the number of $\mathbf{x} \in \Lambda \cap R$ is given by the number of possible coefficient vectors (λ_1, λ_2). If $\lambda_1 = 0$ then $\lambda_2 = \pm 1$, since $\mathbf{x}$ is primitive. Thus, the cases $\lambda_1 = 0$ and similarly $\lambda_2 = 0$ contribute $O(1)$ solutions. By the lemma, there are

$$\ll \frac{|\mathbf{x}|}{|\mathbf{b}^{(1)}|} \cdot \frac{|\mathbf{x}|}{|\mathbf{b}^{(2)}|} \ll \frac{B^2}{\det(\Lambda)}$$

possibilities for (λ_1, λ_2) such that $\lambda_1 \lambda_2 \neq 0$. Thus, the number of points in $\Lambda \cap R$ is $\ll B^2 \det(\Lambda)^{-1} + 1$. In the case when $n = 2$, we will encounter the case when the region R is an ellipse. In this, case the following adapted Lemma due to Heath-Brown [26, Lemma 2] will be employed:

Lemma 4. *Let $\Lambda \subseteq \mathbb{R}^2$ be a lattice of determinant $\det(\Lambda)$. Let $E \subseteq \mathbb{R}^2$ be an ellipse, centered at the origin, together with its interior, and let $A(E)$ be the area of E. Then there is a positive number $\alpha = \alpha(\Lambda, E)$ and a basis $\mathbf{b}_1$, $\mathbf{b}_2$ of Λ such that $\lambda_1 \mathbf{b}_1 + \lambda_2 \mathbf{b}_2 \in E$ implies $|\lambda_1| \leq \alpha$ and $|\lambda_2| \leq A(E)/(\alpha \det(\Lambda))$. Furthermore, the number of primitive lattice points in Λ contained in E is at most*

$$4\left(\frac{A(E)}{\det(\Lambda)} + 1\right).$$

Chapter 2

Pairs of k-free Numbers, consecutive square-full Numbers

2.1 Introduction

Notation

We write $x \sim X$ to say that $X < x < 2X$ and we write $x \asymp X$ to say that there exist positive constants A, B, independent of X, such that $AX \leq |x| \leq BX$.

The Main Theorem

In this paper, we will present a generalization of the approximate determinant method developed by Heath-Brown in [22]. More precisely, we will prove the following theorem:

Theorem 5. *Let $D, E, x > 1$ and $\epsilon > 0$. Let k, l, h be integers such that $1 \leq l < k$ and $h \neq 0$. Suppose $\mathcal{N}(x; D, E)$ is the number of elements in the set*

$$\{(d, e, u, v) \in \mathbb{N}^4 : d \sim D, e \sim E, u \sim U, v \sim V, e^k v^l - d^k u^l = h\},$$

where

$$U = \frac{x^{1/l}}{D^{k/l}}, \quad \textit{and} \quad V = \frac{x^{1/l}}{E^{k/l}}.$$

Let $M > 1$ be defined by

$$\log(M) = \frac{9}{8}\frac{\log(DE)\log(UV)}{\log x},$$

and suppose that the following conditions are satisfied:

1. $\log(DE) \asymp \log(UV) \asymp \log(x)$.

2. $l \geq 2$, *or* $DE \gg_{k,l,h} x^{1/k}$.

Then, if x is large enough in terms of ϵ,

$$\mathcal{N}(x; D, E) \ll_{\epsilon,k,l,h} x^{\epsilon} \min\{(DEM)^{1/2} + D + E, (UVM)^{1/2} + U + V\}.$$

Theorem 5 gives an upper bound for the number of integer points on the algebraic variety defined by

$$e^k v^l - d^k u^l = h, \tag{2.1}$$

where each of the variables d, e, u, v are restricted to certain sizes D, E, U, V. The main strategy of the proof of Theorem 5 will be to reduce the problem of counting integer points on the algebraic variety $e^k v^l - d^k u^l = h$ to counting rational points "close" to the curve $t = s^{k/l}$ where $t = v/u$ and $s = d/e$. The fundamental tool we use to tackle this counting problem will be the approximate determinant method for which the interested reader should consult Heath-Brown [22], where he derives an asymptotic formula for square-free values of the form $n^2 + 1$ up to x, say. Indeed, our proof of Theorem 5 is in many stages a refinement of Heath-Brown's work. In the following paragraphs, we will illustrate our applications of Theorem 5.

Pairs of k-free integers

Let $k \geq 2$ be an integer. We say that $n \in \mathbb{Z}$ is k-free if there is no prime p such that $p^k \mid n$. By convention, a 2-free integer is called square-free. It is an elementary fact that

$$S_k(x) := \#\{n \leq x : n \text{ is } k\text{-free}\} = \frac{x}{\zeta(k)} + O(x^{1/k}). \tag{2.2}$$

We shall now consider the more intricate problem of deriving an asymptotic formula for pairs of k-free integers up to x, say. More precisely, for integers $k \geq 2$ and $h \neq 0$, let $N_{k,h}(x)$ be the number of integers $n \leq x$ such that both n and $n+h$ are k-free. Then, we have the following theorem:

Theorem 6. *For all $\epsilon > 0$ and all sufficiently large x, we have that*

$$N_{k,h}(x) = c_{k,h}x + O_{\epsilon,k,h}(x^{\omega(k)+\epsilon}),$$

where

$$c_{k,h} = \prod_p \left(1 - \frac{\rho_{k,h}(p)}{p^k}\right),$$

with

$$\rho_{k,h}(p) = \begin{cases} 2 & \text{if } p^k \nmid h \\ 1 & \text{if } p^k \mid h \end{cases},$$

and

$$\omega(k) = \begin{cases} \frac{26+\sqrt{433}}{81} \approx 0.578 & \text{if } k = 2 \\ \frac{169}{144k} & \text{for } k \geq 3. \end{cases}$$

The problem of estimating $N_{k,h}(x)$ as in Theorem 6 is most interesting when k is fairly small because $S_k(x)/x \to 1$ as $k \to \infty$. The trivial error term for Theorem 6 is $\omega(k) = 2/(k+1)$ which can be obtained with elementary arguments (see for example Carlitz [7]). We will briefly sketch how one can obtain the trivial bound at the end

of the chapter in section 2.3.4

By considering the Dirichlet series $\zeta(s)/\zeta(ks)$, it is plausible to suspect that the error term of $S_k(x)$ in (2.2) cannot be improved by a proper power of x below $O(x^{1/k})$ without assuming some quasi-Riemann-Hypothesis. By assuming uniformity in the error term of Theorem 6 with respect to $h \ll x$, one can show that an error term $O(x^\theta)$ in Theorem 6 implies an error term $O(x^\theta)$ in the formula for $S_k(x)$ and it is thus reasonable to assume that the error term of Theorem 6 cannot be improved below $O(x^{1/k})$ by a power of x without radically new ideas. We will illustrate this further at the end of the chapter in sections 2.3.5 and 2.3.6

Heath-Brown [24] considered the problem of Theorem 6 in the case $k = 2$ and $h = 1$. He obtained $\omega(2) = 7/11 \approx 0.636$ improving the trivial value $\omega(2) = 2/3$. Heath-Brown's approach uses exponential sums and the Square Sieve. It should be noted that Heath-Brown's method is actually uniform in $h \ll x$. Brandes [4] has generalized Heath-Brown's method for general k. Her argument yields the value $\omega(k) = 14/(7k+8)$. Our error exponent $\omega(k)$ stated in Theorem 6 is such that $\omega(k) \leq 14/(7k+8)$ for all values of k. Dietmann and Marmon [11] have worked independently on improving the exponent $\omega(k)$ at the same time this paper was produced. Their method is similar to ours and they obtain the exponent $\omega(k) = 14/(9k)$, which improves upon Brandes' bound for $k \geq 5$. Our error exponent is currently the smallest available exponent in the literature for all $k \geq 2$. The proof of Theorem 6 will be an application of Theorem 5 with $l = 1$.

An asymptotic formula for r-tuples of k-free integers

The second application of Theorem 5 that we will present is the following:

Theorem 7. *Let $k \geq 2$, $r \geq 2$ and $l_i(x) = a_i x + b_i \in \mathbb{Z}[x]$ for $i = 1, \ldots, r$ such that*

$a_i b_j - a_j b_i \neq 0$ and $a_i \neq 0$ for all i, j with $1 \leq i, j \leq r$ and $i \neq j$. Then define

$$\rho(p) = \#\{n \pmod{p^k} : p^k \mid l_i(n) \text{ for some } i\},$$

and let

$$c = \prod_p \left(1 - \frac{\rho(p)}{p^k}\right).$$

If $N(x)$ is the number of integers $n \leq x$ such that $l_1(n), \ldots, l_r(n)$ are all k-free. Then for any $\epsilon > 0$ and any sufficiently large x we have that

$$N(x) = cx + O_\epsilon(x^{3/(2k+1)+\epsilon}).$$

It should be noted that the implied constant in Theorem 7 depends on the choice of the l_i and that the best error term in the sense of Theorem 7 available in the literature for $k = 2$ was $O(x^{7/11+\epsilon})$ (See Tsang [44]). Tsang's proof uses a form of the Rosser-Iwaniec sieve and the version of Theorem 6 due to Heath-Brown. It should be noted that even though Tsang's error term is weaker than ours, his implied constants are uniform in r and $\max_i ||l_i||$.

Consecutive square-full numbers

We will prove the following theorem about consecutive square-full numbers. Recall that an integer n is called square-full if, for all primes $p \mid n$, we have $p^2 \mid n$.

Theorem 8. *Let $N(x)$ be the number of integers $n \leq x$ such that both n and $n + 1$ are square-full. Then we have for all $\epsilon > 0$ and sufficiently large x that*

$$N(x) \ll_\epsilon x^{29/100+\epsilon}.$$

It can be shown that there are indeed infinitely many consecutive square-full

numbers, for if n and $n+1$ are square-full then so are $4n(n+1)$ and $4n(n+1)+1$. However, it follows from a simple application of the abc-conjecture that there are at most finitely many n such that $n, n+1$ and $n+2$ are all square-full. And Indeed, Erdös conjectured in 1975 that there are no such triples. The proof of Theorem 8 will be an application of Theorem 5 with the variety given by $e^3v^2 - d^3u^2 = 1$.

Size of the fundamental solution of Pell Equations

Let $D > 0$ be an integer which is not a square. Consider the Pell equation

$$T^2 - DU^2 = 1 \tag{2.3}$$

as an equation in (T, U). Write a solution of this equation as $\eta_D = T + U\sqrt{D}$. For each fixed D, the Pell equation (2.3) has a unique solution called the fundamental solution ϵ_D which satisfies $\epsilon_D > 1$ and

$$\{\eta_D : \eta_D \text{ is a solution of } (2.3)\} = \{\pm\epsilon_D^n : n \in \mathbb{Z}\}.$$

It is strongly believed that ϵ_D is almost always much larger than D. In particular, one may study the quantity

$$\mathcal{S}(X, \alpha) = \#\{(D, \eta_D) : D \sim X, D \text{ is not a square}, 1 < \eta_D \leq D^{1/2+\alpha}\}$$

for $\alpha > 1/2$. One can show that

$$\mathcal{S}(X, \alpha) \ll X^{\min(\alpha+\epsilon, 1)}. \tag{2.4}$$

This estimate is illustrated by Fouvry and Jouve in [15] and uses in particular a theorem due to Hooley. In [15], Fouvry and Jouve have shown that this estimate can

be improved to

$$\mathcal{S}(X,\alpha) \ll_\epsilon X^{\frac{\alpha}{3}+\frac{7}{12}+\epsilon}.$$

Their bound improves (2.4) in the range $7/8 < \alpha < 5/4$. We will improve their result further. More precisely, we will prove the following result:

Theorem 9.

$$\mathcal{S}(X,\alpha) \ll_\epsilon X^{\max\left(\frac{9}{16}\frac{\alpha}{\alpha+1/2}+\frac{1}{2}\min(1,\alpha),\frac{1}{2}+\frac{\alpha}{5}\right)}.$$

Our result is stronger than (2.4) in the range $5/8 < \alpha < 5/2$. We obtain the following corollary:

Corollary 10. *For all $0 \leq \theta < 3$, we have*

$$\#\{D : 1 < D \leq X, D \text{ is not a square}, \epsilon_D \leq D^\theta\} = o_\theta(X).$$

This improves upon the result by Fouvry and Jouve [15]. They have shown that one can take $\theta < 7/4$ in Corollary 10. Furthermore, Fouvry and Jove have proved a slightly weaker version of Corollary 10 in [16]. They showed that for all $\theta < 3$, there is a positive proportion of fundamental discriminants D such that $\epsilon_D > D^\theta$. For a more thorough discussion of the history and motivation behind Theorem 9 and Corollary 10, the interested reader should consult their papers [15] and [16].

2.2 The Proof of Theorem 5

We will now start to prove Theorem 5. From now on all implied constants may depend on k, l and h. We may assume without loss of generality that $(ev, du) = 1$, because if $p \mid (ev, du)$ then $p \mid h$. As a first step, we will set $t = v/u$ and $s = d/e$ so

that the equation (2.1) becomes

$$t^l = s^k + O\left(\frac{1}{E^k U^l}\right).$$

Note that

$$t^l - s^k = (t - s^{k/l}) \sum_{a+b=l-1} t^a (s^{k/l})^b.$$

Using that $s \asymp D/E$ and $t \asymp V/U = (D/E)^{k/l}$, we may deduce that

$$\sum_{a+b=l-1} t^a (s^{k/l})^b \asymp \left(\frac{V}{U}\right)^{l-1}.$$

Note that $E^k = x/V^l$ and hence

$$t = s^{k/l} + O\left(\frac{1}{x}\frac{V}{U}\right). \tag{2.5}$$

Thus, we have transformed our problem of counting integer points on a three-fold into a problem where we count rational points close to the curve $t = s^{k/l}$, where the sizes of the numerators and denominators of s and t are determined by D and E. The determinant method seems to be stronger in counting-problems involving varieties of lower dimension so that dealing with a curve rather than a three-fold will provide the key saving in our proof. In section 2.2.1 we will show how the determinant method allows us to subdivide the range of s into intervals I of equal length so that our problem transforms into counting rational points close to the curve $t = s^{k/l}$ where s belongs to some particular interval I. In section 2.2.2, we will then calculate the contribution of one such interval I to $\mathcal{N}(x; D, E)$ and in section 2.2.3 we will then add up all the contributions to finish the proof of the estimate in Theorem 5.

2.2.1 Determinant Method

Note that s is of exact order D/E. Our plan is to pick an integer M such that $\log x \ll \log M \leq \log x$ and split the range of s into $O(M)$ intervals $I = (s_0, s_0(1 + M^{-1})]$. For the rest of this section we will fix one such interval I and consider solutions (s, t) of (2.5) with $s \in I$. We label these solutions as $(s_1, t_1), \ldots, (s_J, t_J)$, say. Consider one such (s_j, t_j). We can write $s_j = s_0(1 + \alpha_j)$ where $0 < \alpha_j \leq 1/M$: Note that $s_0^{k/l} \asymp V/U$ and hence

$$t_j = s_j^{k/l} + O\left(\frac{1}{x}\frac{V}{U}\right) = s_0^{k/l}\left((1+\alpha_j)^{k/l} + O\left(\frac{1}{x}\right)\right).$$

Hence, after applying Taylor's Theorem with a suitable degree in α_j to $(1 + \alpha_j)^{k/l}$, we can write

$$\begin{aligned} s_j &= s_0(1+\alpha_j) && \text{with } 0 < \alpha_j \leq \frac{1}{M}, \\ t_j &= s_0^{k/l}(1 + p(\alpha_j) + \beta_j) && \text{with } \beta_j \ll \frac{1}{x}, \end{aligned}$$

where $p(\alpha_j)$ is a polynomial in α_j with no constant coefficient and with coefficients of size $O(1)$. The next step is to choose positive integers A and B and to label the monomials $s^a t^b$ with $a \leq A$ and $b \leq B$ as $m_1(s, t), \ldots, m_H(s, t)$, where $H = (A + 1)(B+1)$. Then one considers the $J \times H$ matrix $\mathcal{M}$ whose (j, h)-th entry is $m_h(s_j, t_j)$. We will show that the rank of $\mathcal{M}$ is strictly less than H provided we choose A, B and M appropriately. This will enable us to deduce that there is a non-zero vector $\mathbf{c}$ such that $\mathcal{M}\mathbf{c} = 0$. If we now consider the polynomial $C_I(s, t) = C(s, t) = \sum_{h=1}^{H} c_h m_h(s, t)$ then we can see that $C(s_j, t_j) = 0$ for all our solutions with $s_j \in I$. The vector $\mathbf{c}$ can be constructed from minors of $\mathcal{M}$ which shows that $\mathbf{c} \in \mathbb{Q}^H$ has rational entries. Note that the values s_j and t_j have numerators and denominators of size $\ll$ some power of x. By clearing out the common denominator of the coefficients of C we may

therefore assume that C has integer coefficients of size $\ll x^{\kappa(A,B)}$, say.

To show that $\mathcal{M}$ has rank strictly less than H we can assume that $H \leq J$ since otherwise this gets trivial. Thus, it suffices to show that every $H \times H$ minor of $\mathcal{M}$ vanishes. Without loss of generality it suffices to show that the determinant Δ coming from the first H rows and columns of $\mathcal{M}$ vanishes. The j-th row of $\mathcal{M}$ has entries with common denominator $e_j^A u_j^B$ which implies that

$$\left(\prod_{j\leq H} e_j^A u_j^B\right)\Delta \in \mathbb{Z}. \tag{2.6}$$

Observe that $\prod_{j\leq H} e_j^A u_j^B \ll E^{AH}U^{BH}$ and hence if we can show

$$|\Delta| \ll_{A,B} E^{-AH}U^{-BH},$$

with a suitable implied constant, then the integer in (2.6) has to be an integer strictly less than 1 which implies $\Delta = 0$. We substitute $s_j = s_0(1+\alpha_j)$ and $t_j = s_0^{k/l}(1 + p(\alpha_j) + \beta_j)$ so that $\mathcal{M}$ has entries

$$s_0^{a+bk/l}(1+\alpha_j)^a(1+p(\alpha_j)+\beta_j)^b.$$

Hence

$$\Delta = \left(\prod_{a=0}^{A}\prod_{b=0}^{B} s_0^{a+bk/l}\right)\Delta_1 = s_0^{\frac{1}{2}H(A+Bk/l)}\Delta_1,$$

where Δ_1 is the determinant of the generalized Vandermonde matrix with its entries being polynomials in α_j and β_j and coefficients of size $O_{A,B}(1)$. Note that we have

$$|\alpha_j| \leq X_1^{-1} \text{ and } |\beta_j| \leq X_2^{-1},$$

where X_1 is of exact order M and X_2 is of exact order x. In particular, note that $\log X_1$ and $\log X_2$ are both of exact order $\log x$. We now order the monomials $X_1^{-a}X_2^{-b}$ decreasing in size, $1 = M_0, M_1, \ldots, M_H, \ldots$ say. Then by Lemma 3 in Heath-Brown [21], we may bound Δ_1 and hence Δ as follows:

$$\Delta = s_0^{\frac{1}{2}H(A+Bk/l)}\Delta_1 \ll_{A,B} (D/E)^{\frac{1}{2}H(A+Bk/l)} \prod_{h=1}^{H} M_h.$$

Let $M_H = W^{-1}$. Then $X_1^{-a}X_2^{-b} \geq M_H$ if and only if

$$a \log X_1 + b \log X_2 \leq \log W. \tag{2.7}$$

The number of pairs (a, b) which satisfy this inequality is

$$\frac{1}{2}\frac{(\log W)^2}{(\log X_1)(\log X_2)} + O\left(\frac{\log W}{\log x}\right) + O(1).$$

This number must be equal to H which gives

$$|2H(\log X_2)(\log X_1) - (\log W)^2| \ll (\log W)(\log x) + (\log x)^2,$$

and hence

$$|\sqrt{2H(\log X_2)(\log X_1)} - \log W| \ll (\log x)\frac{(\log W) + (\log x)}{\sqrt{2H(\log X_2)(\log X_1)} + \log W} \ll \log x,$$

since $(\log X_2)(\log X_1) \asymp (\log x)^2$. Therefore

$$\log W = \sqrt{2H(\log X_2)(\log X_1)} + O(\log x). \tag{2.8}$$

Next, observe that

$$\begin{aligned}\log \prod_{h=1}^{H} M_h &= -\sum_{a,b}(a \log X_1 + b \log X_2) \\ &= -\frac{1}{3}\frac{(\log W)^3}{(\log X_1)(\log X_2)} + O\left(\frac{(\log W)^2}{\log x}\right) + O(\log x),\end{aligned}$$

where the summation is subject to the inequality (2.7). Using the value for $\log W$ in (2.8), we get

$$\log \prod_{h=1}^{H} M_h = -\frac{2\sqrt{2}}{3} H^{\frac{3}{2}} \sqrt{(\log X_1)(\log X_2)} + O(H \log x).$$

This shows that

$$\log |\Delta| \leq O_{A,B}(1) + \frac{1}{2}H(A + B\frac{k}{l}) \log \frac{D}{E} - \frac{2\sqrt{2}}{3} H^{\frac{3}{2}} \sqrt{(\log X_1)(\log X_2)} + O(H \log x).$$

Thus, to get our required bound on $\log |\Delta|$ it suffices to show that

$$\begin{aligned}A \log E + B \log U + \frac{1}{2}(A + B\frac{k}{l}) \log \frac{D}{E} + C_1(A, B) + C_2 \log x \\ \leq \frac{2\sqrt{2}}{3} H^{\frac{1}{2}} \sqrt{(\log X_1)(\log X_2)},\end{aligned}$$

where $C_1(A, B)$ is some constant depending on A and B and C_2 is an absolute constant. Note that $AB \leq H$ and

$$A \log E + B \log U + \frac{1}{2}(A + B\frac{k}{l}) \log \frac{D}{E} = \frac{A}{2} \log(DE) + \frac{B}{2} \log(UV).$$

Hence, it suffices to show

$$\frac{1}{2}A \log(DE) + \frac{1}{2}B \log(UV) + C_1(A, B) + C_2 \log x \leq \frac{2\sqrt{2}}{3}(AB)^{\frac{1}{2}} \sqrt{(\log X_1)(\log X_2)}.$$

We will optimize the error by choosing $A = \left\lfloor \frac{B\log(UV)}{\log(DE)} \right\rfloor$. The first assumption of Theorem 5 implies that $\nu := \frac{\log(UV)}{\log(DE)} \asymp 1$. In particular, if $B \geq 2/\nu$ then we may apply the inequalities $\frac{1}{2}B\nu \leq \lfloor B\nu \rfloor \leq B\nu$ for $B \geq 2/\nu$ to get that $A \asymp B$. Analyzing Lemma 3 of Heath-Brown [21] which produces our constant $C_1(A, B)$, we can see that $C_1(A, B)$ can be replaced by some $C_3(B)$, say. Now observe that $\frac{1}{2}A\log(DE) + \frac{1}{2}B\log(UV) \leq B\log(UV)$ and that

$$\begin{aligned}\frac{2\sqrt{2}}{3}(AB)^{\frac{1}{2}}\sqrt{(\log X_1)(\log X_2)} \geq& \frac{2\sqrt{2}}{3}B\nu^{\frac{1}{2}}\left(1-\frac{1}{B\nu}\right)^{\frac{1}{2}}\sqrt{(\log X_1)(\log X_2)}\\ \geq& \frac{2\sqrt{2}}{3}B\nu^{\frac{1}{2}}\left(1-\frac{1}{B\nu}\right)\sqrt{(\log X_1)(\log X_2)}\\ =& \frac{2\sqrt{2}}{3}B\sqrt{\frac{\log(UV)}{\log(DE)}}\sqrt{(\log X_1)(\log X_2)} + O(\log x)\end{aligned}$$

since $(\log X_1)(\log X_2) \asymp (\log x)^2$. It therefore suffices if we have

$$B\log(UV) + C_3(B) + C_2\log x \leq \frac{2\sqrt{2}}{3}B\sqrt{\frac{\log(UV)}{\log(DE)}}\sqrt{(\log X_1)(\log X_2)}.$$

Let $\delta > 0$ be arbitrary and pick X_1 such that

$$\frac{2\sqrt{2}}{3}\sqrt{\frac{\log(UV)}{\log(DE)}}\sqrt{(\log X_1)(\log X_2)} \geq (1+\delta)\log(UV),$$

whence it suffices if we have $B\log(UV) + C_3(B) + C_2\log x \leq B(1+\delta)\log(UV)$ which holds if and only if $B\delta\log(UV) \geq C_3(B) + C_2\log x$. Pick

$$B = B(\delta) \geq \frac{2C_2\log x}{\delta\log(UV)}$$

so that $C_2\log x \leq \frac{1}{2}\delta B\log(UV)$ and pick x large enough in terms of δ so that $C_3(B) \leq \frac{1}{2}\delta B\log(UV)$. Thus, we have shown that if we pick B (and hence A) and x large enough in terms of δ and if we can pick a suitable X_1 as above then $\Delta = 0$. Observing

that $X_1 \gg M$ and $X_2 \gg x$, we may rewrite the condition with a redefined δ as

$$\log M \geq \frac{9}{8}(1+\delta)\frac{\log(UV)\log(DE)}{\log x}.$$

In summary, we get the following lemma:

Lemma 11. *Let $\delta > 0$, and assume that an integer M satisfies $\log x \ll \log M \leq \log x$ and*

$$\log M \geq \frac{9}{8}(1+\delta)\frac{\log(DE)\log(UV)}{\log x}.$$

Then for any interval $I = (s_0, s_0(1+M^{-1})]$, there exists a non-zero integer polynomial $C_I(s,t)$ of total degree $O_\delta(1)$ and coefficients of size $O(x^\kappa)$ where $\kappa = \kappa(\delta)$ and such that $C_I(s,t) = 0$ for all solutions of (2.5) with $s \in I$.

2.2.2 Counting Solutions

Next, we want to estimate how much a fixed interval I contributes to $\mathcal{N}(x; D, E)$. As in [22], we may assume that C_I is absolutely irreducible. By clearing the denominators of $C_I(s,t) = 0$, we may rewrite the equation in the form

$$F(d, e; v, u) = 0. \tag{2.9}$$

In summary, we have created an auxiliary polynomial F which is bi-homogeneous of degree (a, b), say, has a total degree of size $O_\delta(1)$ and coefficients of size $O(x^{\kappa(\delta)})$ and it vanishes at the solutions (s,t) of (2.5) with $s \in I$. The condition $s \in I$ gives $|d - es_0| \ll D/M$. We also have $|e| \ll E$. It is convinient to define the linear map $T : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$T(x_1, x_2) = \left(\frac{M}{D}(x_1 - x_2 s_0), \frac{1}{E}x_2\right).$$

This linear map defines a lattice

$$\Lambda = \{T(x_1, x_2) : (x_1, x_2) \in \mathbb{Z}^2\}$$

of determinant $\det(\Lambda) = M/(ED)$. Consider the rectangle

$$R = \{(\alpha_1, \alpha_2) : |\alpha_1| \ll 1, |\alpha_2| \ll 1\},$$

with suitable implied constants so that $s = d/e \in I$, implies $T(d, e) \in \Lambda \cap R$. Thus, we will now count points falling into $\Lambda \cap R$.

Let $\mathbf{g}^{(1)}$ be the shortest non-zero vector in Λ and let $\mathbf{g}^{(2)}$ be the shortest vector in Λ not parallel to $\mathbf{g}^{(1)}$. Then $\mathbf{g}^{(1)}, \mathbf{g}^{(2)}$ will be a basis for Λ. Moreover, $\lambda_1\mathbf{g}^{(1)} + \lambda_2\mathbf{g}^{(2)} \in R$ implies $|\lambda_1\mathbf{g}^{(1)}| \ll 1$ and $|\lambda_2\mathbf{g}^{(2)}| \ll 1$. By defining L_i to be a suitable constant times $|\mathbf{g}^{(i)}|^{-1}$ for $i = 1, 2$, we may write $|\lambda_i| \leq L_i$. Note that $|\mathbf{g}^{(1)}| \leq |\mathbf{g}^{(2)}|$ and $|\mathbf{g}^{(1)}||\mathbf{g}^{(2)}| \ll \det(\Lambda) = M/(DE)$ from which we may conclude $L_2 \ll L_1$ and $L_1L_2 \gg \frac{DE}{M}$. Next set

$$\mathbf{h}^{(i)} = (\frac{D}{M}\mathbf{g}_1^{(i)} + s_0 E\mathbf{g}_2^{(i)}, E\mathbf{g}_2^{(i)}).$$

Then $\mathbf{h}^{(1)}$ and $\mathbf{h}^{(2)}$ will form a basis for $\mathbb{Z}^2$ and if $\mathbf{x} = \lambda_1\mathbf{h}^{(1)} + \lambda_2\mathbf{h}^{(2)}$ is in the region given by $|x_1 - x_2 s_0| \ll D/M$ and $|x_2| \ll E$ then $\lambda_1\mathbf{g}^{(1)} + \lambda_2\mathbf{g}^{(2)} \in R$. Thus, after a change of basis we may replace (d, e) by (λ_1, λ_2) with $|\lambda_i| \leq L_i$ where $L_2 \ll L_1$ and $L_1L_2 \gg (DE)/M$.

Our value s_0 is of the form $s_0 = \frac{x_3}{M}\frac{D}{E}$ where x_3 is an integer of exact order M. Define $x_4 := \lfloor x_3^{k/l} M^{1-k/l} \rfloor$ and $t_0 := \frac{x_4}{M}\frac{V}{U}$ so that $s_0^{k/l} = t_0 + O\left(\frac{1}{M}\frac{V}{U}\right)$. Observe that

$$t = s_0^{k/l} + s_0^{k/l} p(\alpha) + s_0^{k/l}\beta = s_0^{k/l} + O\left(\frac{1}{M}\frac{V}{U}\right) + O\left(\frac{1}{x}\frac{V}{U}\right) = t_0 + O\left(\frac{1}{M}\frac{V}{U}\right),$$

since $M \leq x$. This leads to the conditions $|v - ut_0| \ll \frac{V}{M}$ and $|u| \ll U$ and hence we can analogously to the above argument replace (v, u) by (τ_1, τ_2) say where $|\tau_i| \leq T_i$ with $T_2 \ll T_1$ and $T_1 T_2 \gg \frac{UV}{M}$. These substitutions convert equation (2.1) into an equation

$$G_0(\lambda_1, \lambda_2; \tau_1, \tau_2) = h, \tag{2.10}$$

say where G_0 is bi-homogeneous of degree (k, l). Similarly, equation (2.9) will turn into an equation of the form

$$G_1(\lambda_1, \lambda_2; \tau_1, \tau_2) = 0, \tag{2.11}$$

where G_1 is bi-homogeneous of degree (a, b) and satisfies the same conditions as F. Also, from the above argument it is clear that the vectors (λ_1, λ_2) and (τ_1, τ_2) are primitive. For example, if $p \mid (\lambda_1, \lambda_2)$ then $p \mid (d_1, e_1) = 1$.

If $a = 0$ then (2.11) determines $O_\delta(1)$ pairs (τ_1, τ_2) each of which gives a pair (u, v). The number of pairs (d, e) corresponding to such a (u, v) is

$$\#\{(d, e) : d \asymp D, e \asymp E, e^k v^l - d^k u^l = h\} \ll x^\epsilon. \tag{2.12}$$

For $k = 2$, the estimate (2.12) follows from Estermann [14]. For $k \geq 3$, we note that $e^k v^l - d^k u^l = h$ is a Thue-Mahler equation [43]. By a result of Lewis and Mahler, this equation has only $O_{k,l,h}(1)$ solutions (see [33]). (More precisely, the number of solutions does not exceed $c^{\omega(h)}$, where $\omega(h)$ is the number of prime divisors of h and c is a power of k, independent of the coefficients u, v of the equation). Thus, the case $a = 0$ contributes $O_\delta(x^\delta)$ to $\mathcal{N}(x; D, E)$.

If $b = 0$ then (2.11) determines $O_\delta(1)$ pairs (λ_1, λ_2) each of which gives a pair (d, e).

The number of pairs (u, v) corresponding to such a pair (d, e) is

$$\#\{(u,v) : u \asymp U, v \asymp V, e^k v^l - d^k u^l = h\} \ll x^\epsilon.$$

If $l = 2$ then this follows again by Estermann's result and if $l \geq 3$ the estimate follows from the above result about Thue equations. If $l = 1$ then the equation $e^k v - d^k u = h$ is a linear Diophantine equation in (u, v) and thus, for each pair (d, e), the number of solutions (u, v) to (2.1) is

$$\ll \frac{V}{D^k} + 1 = \frac{x}{(DE)^k} + 1 \ll 1,$$

where the last estimate follows from the assumption $DE \gg x^{1/k}$ of the theorem. Hence, the case $b = 0$ contributes $O_\delta(1)$ to $\mathcal{N}(x; D, E)$.

If $a \geq 2$ then Lemma 2 of Heath-Brown [22] gives us that (2.11) has $O_{\epsilon,\delta}(T_1^{1+\epsilon} x^{\kappa\epsilon})$ solutions. (recall that the coefficients of G_1 are of order x^κ). Picking ϵ small enough in terms of δ, we may assume that this is $O_\delta(T_1^{1+\delta} x^\delta)$. Each solution of (2.11) produces at most one solution of (2.1). So in the case $a \geq 2$ the contribution of I to $\mathcal{N}(x; D, E)$ is $O_\delta(T_1^{1+\delta} x^\delta)$. Similarly, if $b \geq 2$ then the contribution of I to $\mathcal{N}(x; D, E)$ is $O_\delta(L_1^{1+\delta} x^\delta)$.

If $a = 1$ then (2.11) can be written as

$$\lambda_1 G_{11}(\tau_1, \tau_2) + \lambda_2 G_{12}(\tau_1, \tau_2) = 0,$$

and hence $q\lambda_1 = G_{12}(\tau_1, \tau_2)$ and $q\lambda_2 = -G_{11}(\tau_1, \tau_2)$ for some integer q. We define two polynomials $g_1, g_2 \in \mathbb{Z}[x]$ by $G_{1i}(\tau_1, \tau_2) = \tau_1^b g_i(\tau_2/\tau_1)$ for $i = 1, 2$. Observe that g_1 and g_2 must be coprime since G_1 is absolutely irreducible. Hence, by Euclid's Algorithm there exist polynomials $h_1, h_2 \in \mathbb{Z}[x]$ and an integer H such that

$$g_1 h_1 + g_2 h_2 = H$$

where $H = O(x^\kappa)$. Evaluating this equation at τ_2/τ_1 we may deduce that $q \mid H\tau_1^K$ where K is some integer. and similarly we may conclude that $q \mid \tilde{H}\tau_2^K$ where $\tilde{H} = O(x^\kappa)$. But τ_1 and τ_2 are coprime. Thus, we may deduce that we have $O_\delta(x^\delta)$ choices for q. Each value of q gives us a value of λ_1 and λ_2 in terms of τ_1 and τ_2 which we may substitute into (2.10) to get a Thue equation of the form $G_3(\tau_1, \tau_2) = hq^k$, say. This equation gives $O(T_1)$ possible pairs τ_1, τ_2 which shows that the case $a = 1$ contributes at most $O_\delta(x^\delta T_1)$ to $\mathcal{N}(x; D, E)$. Similarly, we may deduce that the case $b = 1$ contributes at most $O_\delta(x^\delta L_1)$ to $\mathcal{N}(x; D, E)$. In summary, we obtain the following:

Lemma 12. *For any $\delta > 0$, the contribution of the solutions (s, t) with $s \in I$ to $\mathcal{N}(x; D, E)$ is $O_\delta(x^\delta \min(L_1^{1+\delta}, T_1^{1+\delta}))$.*

2.2.3 Completion of the proof of Theorem 5

In the previous section, we calculated the contribution of each interval I to $\mathcal{N}(x; D, E)$. It remains to sum up the contribution of the various intervals. To proceed, we write $\mathbf{g}^{(1)}$ from the previous section as

$$\mathbf{g}^{(1)} = ((M/D)(x_1 - x_2 s_0), (1/E)x_2)\,.$$

Recall that L_1 was defined to be a suitable multiple of $|\mathbf{g}^{(1)}|^{-1}$. This gives

$$L_1(x_1 - x_2 s_0) \ll D/M, \quad \text{and} \quad L_1 x_2 \ll E.$$

Recall that we produce the intervals $I = (s_0, s_0 + \frac{1}{M}\frac{D}{E}]$ by taking $s_0 = x_3 \frac{1}{M}\frac{D}{E}$ for integers $x_3 \asymp M$. Hence, the number of intervals I for which $L < L_1 \le 2L$ is at most the number of triples $(x_1, x_2, x_3) \in \mathbb{Z}^3$ for which $\gcd(x_1, x_2) = 1$ and

$$x_2 x_3 = \frac{ME}{D} x_1 + O\left(\frac{E}{L}\right), \quad x_2 \ll \frac{E}{L}, \quad x_3 \asymp M.$$

Recalling that $L_1 \gg L_2$ and $L_1 L_2 \gg (DE)/M$, we can deduce that $L \gg (DE/M)^{1/2}$.

Assume that $L_1 \ll 1$ for a suitably small implied constant. Then $|\lambda_1| \leq L_1$ and $|\lambda_2| \leq L_2 \ll L_1$ imply that $(\lambda_1, \lambda_2) = (0, 0)$ and hence, after reversing the linear change of variables, the corresponding point (d, e) would be $(0, 0)$ which is impossible since d and e are coprime. Thus, we may assume that $L \gg 1$.

If $x_2 = 0$ then $x_1 = \pm 1$ since $(x_1, x_2) = 1$. Hence, $L \asymp |\mathbf{g}^{(1)}|^{-1} = D/M$. Note that $x_3 \neq 0$. Thus, there are $O(M)$ choices for x_3. Hence, the number of intervals I for which $x_2 = 0$ and $L < L_1 \leq 2L$ is $O(M)$. By Lemma 12, each such interval contributes at most $O(x^\delta L^{1+\delta})$ to $\mathcal{N}(x; D, E)$ which gives a total contribution of $O(x^\delta D)$ corresponding to these intervals.

Next consider the cases when $x_1 = 0$. In this case $x_2 = \pm 1$ because $(x_1, x_2) = 1$, and hence $L \asymp E/M$. And thus, a similar argument as above shows that the intervals I for which $x_1 = 0$ and $L < L_1 \leq 2L$ contribute a total of $O(x^\delta E)$ to $\mathcal{N}(x; D, E)$.

We are therefore left with the case when x_1 and x_2 are both non-zero. We can now see that $|\mathbf{g}^{(1)}| \gg E^{-1}$ which implies that $L \ll E$. The above conditions on (x_1, x_2, x_3) imply that $x_1 \ll D/L$. Thus, there are $O(D/L)$ choices for x_1 and each x_1 produces $O(E/L)$ choices for the product $x_2 x_3$. And since $x_2 x_3 \neq 0$, a divisor function estimate shows that each value of $x_2 x_3$ arises from at most $O_\delta(x^\delta)$ pairs (x_2, x_3). Thus, there are $O_\delta(x^\delta DE/L^2)$ intervals I so that L_1 is of exact order L. Each interval contributes $O_\delta(x^\delta L^{1+\delta})$ by Lemma 12. Note that $L^\delta \ll E^\delta \ll x^\delta$ and hence we get a total contribution of $O_\delta(x^\delta DE/L)$ corresponding to the intervals with $x_1 x_2 \neq 0$. By dyadic subdivision of the range of $L \gg (DE/M)^{1/2}$ we can conclude that

$$\mathcal{N}(x; D, E) \ll_\delta x^\delta((DEM)^{1/2} + D + E).$$

Similarly, we may consider the (x_1, x_2) lattice from the previous section corresponding to (v, u) to get $T_1(x_1 - x_2 t_0) \ll V/M$ and $T_1 x_2 \ll U$. Recall that $t_0 = x_4 \frac{1}{M}\frac{V}{U}$ where $x_4 = \left\lfloor \frac{x_3^k}{M^{k-1}} \right\rfloor$. We can see that $x_3 \asymp M$ implies $x_4 \asymp M$ for large enough x. Hence by a completely analogous argument to the above we can deduce that

$$\mathcal{N}(x; D, E) \ll_\delta x^\delta((UVM)^{1/2} + U + V).$$

Thus, we have established the bound for $\mathcal{N}(x; D, E)$ as stated in Theorem 5. Now write $DE = x^\psi$ where $\psi > 0$. Then $UV = x^{2/l - k\psi/l}$. We pick the integer M such that

$$\frac{\log M}{\log x} = \frac{9}{8}(1+\delta)\psi(2/l - k\psi/l).$$

Note that

$$\frac{9}{8}\psi(2/l - k\psi/l) \leq \frac{9}{8kl} < 1.$$

So, indeed with our choice of M we have that $\log M \leq \log x$. This finishes the proof of Theorem 5.

2.3 The Proof of Theorem 6

2.3.1 Preliminaries

First, we illustrate on how finding an asymptotic formula for $N_{k,h}(x)$ can be reduced to counting points on the algebraic variety $e^k v - d^k u = h$ inside a certain bounded box. In what follows all implied constants may depend on h and k. First observe that by dyadic subdivision it is enough to show that

$$N_{k,h}(2x) - N_{k,h}(x) = c_{k,h} x + O_\epsilon(x^{\omega(k)+\epsilon}).$$

Let

$$\xi(n) = \left(\prod_{p^k|n} p\right)\left(\prod_{p^k|n+h} p\right).$$

Then $\xi(n) = 1$ if and only if n and $n+h$ are k-free. Thus, we may deduce that

$$\begin{aligned} N_{k,h}(2x) - N_{k,h}(x) &= \sum_{x<n\leq 2x} \sum_{m|\xi(n)} \mu(m) \\ &= \sum_{m=1}^{\infty} \mu(m) N(x;m), \end{aligned}$$

where

$$N(x;m) = \#\left\{x < n \leq 2x : \xi(n) \equiv 0 \pmod{m}\right\}.$$

Observe that the congruence $\xi(n) \equiv 0 \pmod{p}$ has exactly $\rho_{k,h}(p)$ solutions modulo p^k. Thus, by an argument similar to the proof of the Chinese remainder theorem, the congruence $\xi(n) \equiv 0 \pmod{m}$ has exactly

$$\rho_{k,h}(m) = \prod_{p|m} \rho_{k,h}(p)$$

solutions modulo m^k. Hence

$$N(x;m) = \rho_{k,h}(m)\left(\frac{x}{m^k} + O(1)\right).$$

Note that for square-free m, we have that

$$\rho_{k,h}(m) \leq 2^{\omega(m)} \ll m^{\epsilon}.$$

Next, we introduce a parameter y with $x^{1/k} \leq y \leq x^{2/(k+1)}$ which we shall pick in a moment. Now, we look at the small terms in the above sum corresponding to the

values of m with $m \leq y$. These terms contribute

$$\begin{aligned}
&\sum_{m\leq y} \mu(m)\rho_{k,h}(m)\left(\frac{x}{m^k}+O(1)\right)\\
=&x\sum_{m\leq y}\frac{\mu(m)\rho_{k,h}(m)}{m^k}+O\left(\sum_{m\leq y}\rho_{k,h}(m)\right)\\
=&x\sum_{m=1}^{\infty}\frac{\mu(m)\rho_{k,h}(m)}{m^k}+O\left(x\sum_{m>y}\frac{\rho_{k,h}(m)}{m^k}+\sum_{m\leq y}\rho_{k,h}(m)\right)\\
=&c_{k,h}x+O(x^{1+\epsilon}y^{1-k})+O(x^{\epsilon}y)\\
=&c_{k,h}x+O(x^{\epsilon}y),
\end{aligned}$$

where the last equality follows from $x^{1/k} \leq y$. To minimize the remaining error term, we pick $y = x^{1/k}$. Thus, we can see that the values of m with $m \leq x^{1/k}$ contribute our main term. Hence, we are left to consider the values of m with $m > x^{1/k}$. For each such m we write $m = de$ where $d^k \mid n$ and $e^k \mid n + h$. By dyadic subdivision, these values d, e lie in $O((\log x)^2)$ boxes $D/2 < d \leq D$, $E/2 < e \leq E$ where $D, E \ll x^{1/k}$ and $DE \gg x^{1/k}$. Hence, for one such pair D, E we must have

$$N_{k,h}(2x) - N_{k,h}(x) = c_{k,h}x + O(x^{1/k+\epsilon}) + O(x^{\epsilon}\mathcal{N}(x; D, E)),$$

where $\mathcal{N}(x; D, E)$ is the number of elements in the set

$$\{(d, e, u, v) \in \mathbb{N}^4 : D/2 < d \leq D, E/2 < e \leq E, x < d^k u + h = e^k v \leq 2x\}.$$

2.3.2 The proof of Theorem 6 for $k \geq 3$

We apply Theorem 5 with $l = 1$, $U = x/D^k$ and $V = x/E^k$ to deduce that

$$\mathcal{N}(x; D, E) \ll_{\epsilon} x^{\epsilon} \min\{(DEM)^{1/2} + D + E, (UVM)^{1/2} + U + V\}. \tag{2.13}$$

We assume without loss of generality that $D \le E$ and hence $V \le U$. Note that $U/V \ge E/D \ge 1$. First we consider the case $M \ge U/V$. In this case, the estimate (2.13) becomes

$$\mathcal{N}(x; D, E) \ll_\epsilon x^\epsilon M^{1/2} \min(DE, UV)^{1/2}. \tag{2.14}$$

We now set $DE = x^\psi$ so that $UV = x^{2-k\psi}$. Then

$$\frac{\log \mathcal{N}(x; D, E)}{\log x} - \epsilon \le \frac{1}{2}\min(\psi, 2 - k\psi) + \frac{9}{16}\psi(2 - k\psi) =: f_k(\psi),$$

say. The function $f(\psi)$ takes its maximal value at $\psi = 2/3$ if $k = 2$ and at $\psi = 13/(9k)$ if $k \ge 3$. Note that $f_2(2/3) = 7/12$ and $f_k(13/(9k)) = 169/(144k)$ for $k \ge 3$. Note that

$$(DEM)^{1/2} + D + E \ll x^{\frac{169}{144k}} + x^{1/k} \ll x^{\frac{169}{144k}},$$

no matter if $M \ge U/V$ does or does not hold. This completes the proof of Theorem 6 for $k \ge 3$. However, for $k = 2$, we have $169/(144k) \ge 7/12$ and a better argument is required. Thus, we shall employ the following trivial estimate, where we first sum over the pairs e, u as follows:

$$\begin{aligned}
\mathcal{N}(x; D, E) &\ll \sum_{\substack{E \ll e \ll E \\ U \ll u \ll U}} \#\{d : d \asymp D, e^2 v - d^2 u = h\} \\
&\ll \sum_{\substack{E \ll e \ll E \\ U \ll u \ll U}} \#\{d : d \asymp D, d^2 \equiv -hu^{-1} \pmod{e^2}\} \\
&\ll \sum_{\substack{E \ll e \ll E \\ U \ll u \ll U}} \left(\frac{D}{e^2} + 1\right) \#\{d \mod e^2, d^2 \equiv -hu^{-1} \pmod{e^2}\} \\
&\ll EU\left(\frac{D}{E^2} + 1\right) x^\epsilon.
\end{aligned} \tag{2.15}$$

Note that

$$EU\frac{D}{E^2} = \frac{x}{DE} \ll x^{1/2},$$

Thus we may assume that $EU \geq x^{1/2}$ and, hence:

$$\frac{D^3}{E^3} = \frac{x^2}{(EU)^2 ED} \ll \frac{x^2}{(x^{1/2})^3} = x^{1/2}.$$

Thus, $\frac{D}{E} \ll x^{1/6}$ and $\frac{V}{U} \ll x^{1/3}$. By interchanging E and D and doing the same argument, we may deduce that all of the quotients $\frac{D}{E}$, $\frac{E}{D}$, $\frac{V}{U}$, $\frac{U}{V}$ are $\ll x^{1/3}$. We may impose the condition $M \geq x^{1/3} \geq U/V$, so that the bound (2.14) does indeed hold. This shows that we can take the value $\omega(2) = 7/12$ in Theorem 6. But we can do better than this by considering points on lines contained in the three-fold $e^2 v - d^2 u = h$. The following section will illustrate this idea.

2.3.3 Counting Points on Lines, Finishing the proof for $k = 2$

In this section, we will conclude the proof of Theorem 6 by considering points on lines contained in the three-fold (2.1). For convenience, we will illustrate the proof when $h = 1$ but with minor changes, the proof can be adapted to general h. We begin by a similar procedure as in the proof of Theorem 5. We will pick $M \in [x^{1/2}, x]$ and $A = B = 1$ as in section 2.2.1. Note that this will produce a 4×4 matrix $\mathcal{M}$ where the j-th row is

$$\begin{pmatrix} 1 & s_0(1+\alpha_j) & s_0^2(1+2\alpha_j+\beta_j) & s_0^3(1+\alpha_j)(1+2\alpha_j+\beta_j) \end{pmatrix},$$

with $\alpha_j \ll M^{-1}$ and $\beta_j \ll x^{-1}$. (Note that $\alpha_j^2 \ll M^{-2} \leq x^{-1}$). Performing column operations, we get a matrix with j-th row

$$s_0^6 \cdot \begin{pmatrix} 1 & \alpha_j & \beta_j & \alpha_j(2\alpha_j+\beta_j) \end{pmatrix}.$$

Recalling that $s_0 \asymp D/E$, we may deduce that $\Delta \ll \frac{1}{M^3 x} \frac{D^6}{E^6}$. As before, we require $|\Delta| \ll E^{-4} U^{-4}$ in order to deduce that $\Delta = 0$. This is satisfied if $M > (xUV)^{1/3+\delta}$

where $\delta > 0$ is arbitrarily small and x is large enough in terms of δ. Setting as before $DE = x^{\psi}$ and $UV = x^{2-2\psi}$ we can see that $x^{1/2} \leq (xUV)^{1/3+\delta} \leq x$. This enables us to pick $M = (xUV)^{1/3+\delta}$ provided δ is small enough and x is large enough in terms of δ.

Hence, as before, the determinant method will produce an irreducible auxiliary polynomial $F(d, e; u, v)$. This polynomial will be bilinear since we picked the monomials in $\mathcal{M}$ accordingly. That is, in section 2.2.2 the case that will occur is $a = b = 1$. Hence, (2.11) can be written as

$$dL_1(u, v) + eL_2(u, v) = 0,$$

where $L_1(u, v) = c_1u + c_2v$ and $L_2(u, v) = c_3u + c_4v$ are linear forms with integral coefficients. As in section 2.2.2, we get $O(x^{\delta})$ choices for an integer q such that

$$eq = -L_1(u, v), \qquad dq = L_2(u, v). \tag{2.16}$$

Plugging this into the equation $e^2v - d^2u = 1$ gives us a Thue equation

$$G_3(u, v) = (L_1(u, v))^2v - (L_2(u, v))^2u = q^2,$$

say. When G_3 is irreducible then this equation will only have a finite number of solutions (see Thue [43]). Thus, the equation will produce $O(x^{\delta})$ solutions (u, v) for each q except if G_3 is splitting into three equal linear factors,

$$G_3(u, v) = \alpha(\alpha_1v - \alpha_2u)^3,$$

say where $\alpha, \alpha_1, \alpha_2 \in \mathbb{Z}$. Our aim is to show that the points under consideration corresponding to this case actually lie on a line contained in the three-fold defined by

(2.1). Comparing coefficients we get the equations

$$\alpha\alpha_2^3 = c_3^2$$
$$\alpha\alpha_1^3 = c_2^2$$
$$3\alpha\alpha_1^2\alpha_2 = c_4^2 - 2c_1c_2$$
$$3\alpha\alpha_1\alpha_2^2 = c_1^2 - 2c_3c_4.$$

The first two equations give $\alpha_1 = (c_2^2/\alpha)^{1/3}$ and $\alpha_2 = (c_3^2/\alpha)^{1/3}$ which turns the third and fourth equation into

$$3c_2^{4/3}c_3^{2/3} = c_4^2 - 2c_1c_2, \qquad \text{and} \tag{2.17}$$
$$3c_2^{2/3}c_3^{4/3} = c_1^2 - 2c_3c_4 \tag{2.18}$$

respectively. If $c_2 = 0$ then we may deduce from these equations that $c_4 = 0$ and hence $c_1 = 0$. Hence $L_1 = 0$ which gives a contradiction since $qe \neq 0$. Thus, $c_2 \neq 0$ and similarly $c_3 \neq 0$. Using (2.17) and (2.18) we may deduce that $c_3^{2/3}(c_4^2 - 2c_1c_2) = c_2^{2/3}(c_1^2 - 2c_3c_4)$ which may be written as

$$(c_3^{1/3}c_4 + c_3^{2/3}c_2^{2/3})^2 = (c_2^{1/3}c_1 + c_2^{2/3}c_3^{2/3})^2.$$

After taking the square-root, this either lets us deduce directly that $c_4^3c_3 = c_1^3c_2$ or that

$$c_3^{1/3}c_4 + c_2^{1/3}c_1 + 2c_2^{2/3}c_3^{2/3} = 0.$$

Multiply this equation by $c_3^{2/3}$ and plug in the expression for c_3c_4 given by (2.18) to get $(c_1 + c_2^{1/3}c_3^{2/3})^2 = 0$. Similarly, we may deduce from (2.17) that $(c_4 + c_3^{1/3}c_2^{2/3})^2 = 0$. This implies that in either case we have $c_4^3c_3 = c_1^3c_2$. Plugging this value of c_3 into

(2.17) we get that

$$c_1 = \frac{1}{\kappa}\frac{c_4^2}{c_2}, \quad c_3 = \frac{1}{\kappa^3}\frac{c_4^3}{c_2^2},$$

where $\kappa \in \{-1, 3\}$. Consider the equation $c_4^3 c_3 = c_1^3 c_2$. We set $c_1 = h\alpha$ and $c_4 = h\beta$ where $h = (c_1, c_4)$. From this, we can deduce that $c_2 = k\beta^3$ and $c_3 = k\alpha^3$ for some integer k. Observe that $(h, k) = 1$ since $(c_1, c_2, c_3, c_4) = 1$ as F is irreducible. Considering the equation $c_4^2 = \kappa c_1 c_2$ we see that $h = \kappa k \alpha\beta$ which implies $k = 1$ and

$$c_1 = \kappa\alpha^2\beta,\ c_2 = \beta^3,\ c_3 = \alpha^3,\ c_4 = \kappa\alpha\beta^2.$$

Our original Thue equation has now turned into

$$v = \frac{\alpha^2}{\beta^2}u + \frac{Q^2}{\beta^2},$$

where $q = Q^3$ for $Q \in \mathbb{Z}$ with $Q > 0$. Substituting this expression for v into (2.16), we obtain that (d, e, u, v) must lie on the line

$$\ell : (d, e, u, v) = \left(\frac{\kappa\alpha}{Q}, -\frac{\beta}{Q}, 0, \frac{Q^2}{\beta^2}\right) + u\left((1+\kappa)\frac{\alpha^3}{Q^3}, -(\kappa+1)\frac{\alpha^2\beta}{Q^3}, 1, \frac{\alpha^2}{\beta^2}\right).$$

Assume that the line does indeed have an integral point counted by $\mathcal{N}(x; D, E)$. Pick u_1 to be the smallest integer such that (d_1, e_1, u_1, v_1) is on ℓ and counted by $\mathcal{N}(x; D, E)$. This gives us the equations

$$Q^2 = v_1\beta^2 - u_1\alpha^2 \tag{2.19}$$

$$\alpha\kappa Q^2 + u_1(1+\kappa)\alpha^3 = d_1 Q^3 \tag{2.20}$$

$$-\beta Q^2 - u_1(1+\kappa)\alpha^2\beta = e_1 Q^3. \tag{2.21}$$

We now consider the lines with $\kappa = -1$. In this case, we may deduce from (2.20) and (2.21) that $Q = 1$, $d_1 = -\alpha$ and $e_1 = -\beta$. Thus our points under consideration must

lie on the line

$$(d, e, u, v) = (d_1, e_1, u_1, v_1) + \lambda(0, 0, \beta^2, \alpha^2),$$

where $\lambda \in \mathbb{Z}$. Note that there are no parallel lines with $\kappa = -1$ having the same α and β since (2.19) determines the pair (u_1, v_1) modulo (β^2, α^2). The number of distinct lines with $\kappa = -1$ is therefore determined by the number of choices for the direction vectors, that is, by the number of choices for α and β. We must have $\alpha\beta \ll (UV)^{1/2} \ll x^{1/2}$ which shows that the number of distinct lines with $\kappa = -1$ is $O(x^{1/2+\delta})$. The number of points on each line is $\ll 1 + U/\beta^2 \ll 1$ since $E \asymp e_1 = -\beta$. Thus, the total number of points counted by $\mathcal{N}(x; D, E)$ lying on lines with $\kappa = -1$ is $O(x^{1/2+\delta})$.

Next, we consider the lines with $\kappa = 3$. From (2.20) and (2.21) we may deduce that $(\beta d_1 + \alpha e_1)Q = 2\alpha\beta$. Let $a = (Q, \alpha)$ and $b = (Q, \beta)$ so that $\alpha = aA, \beta = bB$ and $Q = abQ_1$ and $(Q_1, AB) = 1$ say. After canceling ab from the last equation, we may deduce that $A \mid d_1$ and $B \mid e_1$. Set $d_1 = AD_1$ and $e_1 = BE_1$. Finally, (2.19) implies that $a^2 \mid v_1$ and $b^2 \mid u_1$. Let $v_1 = a^2V_1$ and $u_1 = b^2U_1$. Furthermore, we can deduce from (2.19) that $(U_1, Q_1) = 1$ and hence (2.21) shows that $Q_1^2 \mid 4U_1A^2$ and therefore $Q_1^2 \mid 4$. The direction vector of the line ℓ is now

$$\left(\frac{A^3}{b^3}C, -\frac{A^2B}{ab^2}C, 1, \frac{a^2A^2}{b^2B^2}\right),$$

where $C = 4/Q_1^3 \in \{4, 1/2\}$. Note that a, A, b, B are pairwise coprime since $d_1^2u_1$ and $e_1^2v_1$ as well as α and β are coprime. Thus, all lines lying on the surface (2.1) can be written as

$$(AD_1, BE_1, b^2U_1, a^2V_1) + \lambda(aA^3B^2C, -bA^2B^3C, ab^3B^2, a^3bA^2),$$

where λ goes through $\mathbb{Z}$, $\mathbb{Z}/2$ or $2\mathbb{Z}$ and subject to the conditions

$$Q_1^2 = V_1 B^2 - U_1 A^2 \tag{2.22}$$

$$bD_1 + aE_1 = 2Q_1^{-1} \tag{2.23}$$

$$U_1 A^2 Q_1 C - D_1 b Q_1 = -3. \tag{2.24}$$

Fix Q_1. Given a line ℓ, the direction vector and hence A, B, a, b are uniquely determined up to sign. Thus we also fix A and B and consider the number of points on lines with our fixed values of Q_1, A and B.

If D_1', E_1', U_1', V_1' is one solution of (2.22), (2.23), (2.24) then the other solutions D_1, E_1, U_1, V_1 are given by

$$D_1 = D_1' + \mu a A^2 B^2$$

$$E_1 = E_1' - \mu b A^2 B^2$$

$$U_1 = U_1' + \mu a b B^2 / C$$

$$V_1 = V_1' + \mu a b A^2 / C.$$

Thus, the number of distinct lines with $\kappa = 3$ and given A, B is

$$\ll \#\left\{(a,b) : a \ll D, b \ll E, ab^3 \ll U, a^3 b \ll V\right\}$$
$$\ll \#\left\{(a,b) : ab \ll (UV)^{1/4}\right\} \ll (UV)^{1/4+\delta}.$$

The number of points on each line is

$$\ll \min\left\{\frac{D}{aA^3B^2}, \frac{E}{bA^2B^3}\right\} \ll \frac{\min(D,E)}{A^2B^2}.$$

Thus, the total number of points on lines with $\kappa = 3$ counted by $\mathcal{N}(x; D, E)$ is

$$\sum_{A,B}(UV)^{1/4+\delta}\frac{\min(D,E)}{A^2B^2} \ll \min(D,E)(UV)^{1/4+\delta} \ll x^{1/2+\delta}.$$

Let $\mathcal{N}_0(x; D, E)$ denote the number of elements in the set

$$\{(d,e,u,v) \in \mathcal{N}(D,E) : (d,e,u,v) \text{ is not on a line contained in (2.1)}\}.$$

We have just shown that

$$\mathcal{N}_0(x; D, E) \ll_\delta x^\delta M \ll_\delta x^{2\delta+1-2\psi/3}.$$

In section 2.3.2, we have deduced the bound (2.14). Hence,

$$\mathcal{N}_0(x; D, E) \leq \mathcal{N}(x; D, E) \ll_\delta x^{\delta+\min(\psi,2-2\psi)/2+\max(1/6,9\psi(1-\psi)/8)},$$

where essentially $1/2 \leq \psi \leq 1$. One can check that the worst value for the exponent occurs if $\psi \leq 2/3$ and then that the worst value for ψ must satisfy

$$1 - \frac{2}{3}\psi = \frac{9}{8}\psi(1-\psi) + \frac{\psi}{2}.$$

Hence the critical value for ψ is $(55 - \sqrt{433})/54 = 0.6331\ldots$ and we may deduce that $\mathcal{N}_0(x; D, E) \ll_\delta x^{3\delta+\omega}$ where $\omega = (26 + \sqrt{433})/81 \leq 0.5779 \leq 7/12 = 0.5833\ldots$. By the above argument, the points counted by $\mathcal{N}(x; D, E)$ but not being elements of $\mathcal{N}_0(x; D, E)$ contribute $O(x^{1/2+\delta})$. This finishes the proof of Theorem 6.

2.3.4 The trivial error term for Theorem 6

The trivial error term for Theorem 6 is $\omega(k) = 2/(k+1)$ which can be obtained by the use of elementary arguments (see for example Carlitz [7]). We briefly sketch how one can obtain such a trivial error term in the case $h = 1$. Let $x \geq 1$ and $x^{1/k} \leq y \leq x^{2/k}$. We proceed as in section 2.3.1 (but without specifying y) to show that for some real numbers D, E with $D, E \ll x^{1/k}$ and $DE \gg y$:

$$N_{k,1}(2x) - N_{k,1}(x) = c_{k,1}x + O(yx^{\epsilon}) + O(x^{\epsilon}\mathcal{N}(x; D, E)),$$

where $\mathcal{N}(x; D, E)$ is as before. That is, we have reduced the problem into one where we have to estimate the number of integer solutions to the equation $e^k v - d^k u = 1$, where each of the points (d, e, u, v) lies inside a certain box. If we pick y small then $\mathcal{N}(x; D, E)$ will count more points (because of the condition $DE \gg y$), and if we pick y large then the error term $O(yx^{\epsilon})$ will be large. Thus, we have to find an upper bound for $\mathcal{N}(x; D, E)$ and then pick y optimally. As in (2.15), we get the trivial estimate

$$\mathcal{N}(x; D, E) \ll x^{\epsilon}\left(\frac{x}{(DE)^{k-1}} + EU\right) \ll \max\{x^{1/k}, EU\}.$$

By interchanging the roles of d and e and the roles of u and v in this argument, we get a similar bound in terms of D and V. Observe that

$$\min(EU, DV) \leq \sqrt{DEUV} = x(DE)^{(1-k)/2}.$$

This then yields the bound

$$\mathcal{N}(x; D, E) \ll \max\{x^{1/k}, \min(EU, DV)\} \ll xy^{(1-k)/2},$$

since $DE \gg y$ and $y \leq x^{2/k}$. We then want to equate the error terms $O(x^{1+\epsilon}y^{(1-k)/2})$ and $O(yx^{\epsilon})$ to find that the choice $y = x^{2/(k+1)}$ is optimal and yields the overall error term $\omega(k) = 2/(k+1)$, as anticipated.

2.3.5 A connection between $S_2(x)$ and the Riemann ζ-function

It is an interesting question to ask how small we can $\omega(k)$ expect to be. To understand this further, we reconsider the asymptotic formula (2.2). We will informally examine a connection between Theorem 6 and the Riemann ζ-function in the case when $k = 2$. We start with the Dirichlet series having the indicator function of square-free numbers as coefficients:

$$D(s) = \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}$$

The right-hand side can be extended to a meromorphic function on $\mathbb{C}$ with the only poles being at $s = 1$ and $s = \rho/2$ for all ρ with $\zeta(\rho) = 0$. Furthermore, $D(s)$ converges absolutely for $\sigma > 1$. Thus, Perron's formula then lets us deduce that for $x \geq 1, x \notin \mathbb{Z}$ and $c > 1$:

$$S_2(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\zeta(s)}{\zeta(2s)} \frac{x^s}{s}\, ds,$$

where the integral converges in the Cauchy principal value sense. The residue of $D(s)$ at $s = 1$ will contribute the main term $x/\zeta(2)$ whereas the residue of $D(s)$ at a value $s = \rho/2$ is $c_\rho x^{\rho/2}$ where c_ρ can be expressed in terms of the residue of $1/\zeta(s)$ at $s = \rho$. Such an argument suggests that

$$S_2(x) = \frac{x}{\zeta(2)} + O\left(\left|\sum_{\rho} c_\rho x^{\rho/2}\right|\right).$$

If we assume the Riemann Hypothesis and write $\rho = 1/2 + i\gamma$ then

$$S_2(x) = \frac{x}{\zeta(2)} + O\left(x^{1/4}\left|\sum_{\rho} c_\rho x^{i\gamma/2}\right|\right).$$

Thus, it is plausible to conjecture that

$$S_2(x) = \frac{x}{\zeta(2)} + O(x^{\frac{1}{4}+\epsilon})$$

and that an error term $O(x^{\frac{\alpha}{2}})$ corresponds to a zero-free region $1/2 \leq \alpha < \sigma \leq 1$ of $\zeta(s)$. It is worth noting that the strongest error term that can currently be derived assuming the Riemann Hypothesis is $O(x^{17/54+\epsilon})$ (Jia [31]), whereas a standard contour integration argument with the line of integration at $\sigma = 1/4 + \epsilon$ yields an error term $O(x^{2/5+\epsilon})$ (Axer [1]). Given the above considerations it is perhaps not surprising that the best unconditional results available use zero-free regions and require at least an argument similar to the prime number theorem. Such error terms essentially look like $O(x^{1/2}\exp(-c\sqrt{\log x}))$ (Landau [32]) where with the strongest results on zero-free regions one can improve the term $\sqrt{\log x}$ to $(\log x)^{3/5}(\log\log x)^{-1/5}$ (Walfisz [45]). Finally, we want to note that using oscillation theorems one can show that

$$S_2(x) = \frac{x}{\zeta(2)} + \Omega_{\pm}(x^{1/4}).$$

Thus, we expect the error term of $S_2(x)$ to be essentially $O(x^{1/4})$ but establishing any error exponent better than $O(x^{1/2})$ by a power of x seems to require radically new ideas.

2.3.6 Theorem 6 and the Riemann ζ-function

We are now going to establish a connection between the error term of Theorem 6 and the error term of $S_2(x)$. Let $c_{2,h}$ be defined as in Theorem 6 and note that $c_{2,0} = 1/\zeta(2)$. To illustrate our argument we assume that it would be possible to establish an asymptotic formula of the form

$$N_{2,h}(x) = c_{2,h}x + O(x^{\theta}), \qquad \theta > 0$$

where the implied constant is independent of h. We start from observing that

$$\begin{aligned} S_2(x)^2 &= S_2(x) + 2\sum_{h<x} N_{2,h}(x-h) \\ &= 2\sum_{h<x} c_{2,h}(x-h) + O(x^{1+\theta}). \end{aligned}$$

By partial summation we have

$$2\sum_{h<x} c_{2,h}(x-h) = 2\int_1^x \sum_{h\le t} c_{2,h}\, dt.$$

Define $\chi_h(b)$ to be 1 if $b^2 \mid h$ and 0 otherwise. Then note that for square-free e, we have

$$\rho_h(e) = \sum_{ab=e} d(a)\mu(b)\chi_h(b).$$

Hence the constants $c_{2,h}$ may be written as

$$c_{2,h} = \sum_{n=1}^{\infty}\sum_{ab=n} \frac{\mu(ab)d(a)\mu(b)\chi_h(b)}{(ab)^2}.$$

Furthermore, it is clear that

$$\sum_{h\le t} \chi_h(b) = \#\left\{h \le t : b^2 \mid h\right\} = \frac{t}{b^2} + O(1),$$

whence

$$2\sum_{h<x} c_{2,h}(x-h) = x^2 \sum_{n=1}^{\infty} \frac{\mu(n)\sum_{ab=n} d(a)a^2\mu(b)}{n^4} + O(x) = x^2 c_{2,0}^2 + O(x),$$

where the last equation follows by considering the appropriate Euler product. Thus, we can conclude that our assumptions lead to

$$S_2(x)^2 = c_{2,0}^2 x^2 + O(x^{1+\theta}),$$

which then implies

$$S_2(x) = c_{2,0}x + O(x^{\theta}).$$

Thus, our considerations above make it plausible that, provided we assume uniformity in the error term with respect to h, the error exponent of Theorem 6 should be expected to be not smaller than $O(x^{1/2})$ without some striking new ideas. In general, by considering the Dirichlet series of $\zeta(s)/\zeta(ks)$, it is plausible to suspect that the error term of $S_k(x)$ cannot be improved by a proper power of x below $O(x^{1/k})$ without assuming some quasi-Riemann-Hypothesis.

2.4 The Proof of Theorem 7

We now turn to the proof of Theorem 7. We define

$$\xi(n) = \prod_{i=1}^{r} \prod_{p^k | l_i(n)} p,$$

and for $w > 1$ let

$$\mathcal{P}(w) = \prod_{p<w} p$$

be the product of primes $p < w$. Furthermore, for $z > 1$ define

$$\mathcal{S}(z) = \sum_{\substack{x<n\leq 2x \\ (\xi(n),\mathcal{P}(z))=1}} 1.$$

That is, $\mathcal{S}(z)$ is the number of integers n in the interval $(n, 2n]$ so that $l_1(n), \ldots, l_r(n)$ all do not have any k-th power prime divisor p^k with $p < z$. In particular, $N(2x) -$

$N(x) = \mathcal{S}(O(x^{1/k}))$. We also define

$$\mathcal{S}_d(w) = \sum_{\substack{x<n\leq 2x \\ \xi(n)\equiv 0 \pmod{d} \\ (\xi(n),\mathcal{P}(w))=1}} 1.$$

Next, we will employ the following identity which is essentially Buchstab's identity. That is, for $1 < w < z$ observe that

$$\mathcal{S}(z) = \mathcal{S}(w) - \sum_{w\leq p<z} \mathcal{S}_p(p).$$

Applying the identity twice, we obtain for $w > 1$:

$$N(2x) - N(x) = \mathcal{S}(O(x^{1/k})) = \mathcal{S}(w) - \sum_{w\leq p\ll x^{1/k}} \mathcal{S}_p(w) + \sum_{w\leq q<p\ll x^{1/k}} \mathcal{S}_{pq}(q).$$

First, we will estimate the sum $\sum_p \mathcal{S}_p(w)$. We split the sum over p in two parts, the first range will be $w \leq p < y$ and for the second range $y \leq p \ll x^{1/k}$ a trivial estimate will suffice. It will turn out that the optimal choice for y is $y = (x/w)^{1/k}$. Similarly to section 2.3.1 we can deduce that:

$$N(x;d) = \#\left\{x < n \leq 2x : \xi(n) \equiv 0 \pmod{d}\right\} = \rho(d)\left(\frac{x}{d^k} + O(1)\right). \tag{2.25}$$

Thus,

$$\begin{aligned}\sum_{y\leq p\ll x^{1/k}} \mathcal{S}_p(w) &\ll \sum_{y\leq p\ll x^{1/k}} N(x;p) \ll x^{\epsilon} \sum_{y\leq p\ll x^{1/k}} \left(\frac{x}{p^k} + 1\right) \\ &\ll x^{\epsilon}(xy^{1-k} + x^{1/k}) \ll x^{1+\epsilon}y^{1-k},\end{aligned}$$

since $y \ll x^{1/k}$. To estimate the the sum over the remaining range $w \leq p < y$ we will apply the following Fundamental Sieve Lemma due to Heath-Brown [25] which

adapted to our purpose states as follows:

Lemma 13. *For $z > 1$ and $w > 1$ we have that*

$$\sum_{d|(\xi(n),\mathcal{P}(w))} \mu(d) = \sum_{\substack{d|(\xi(n),\mathcal{P}(w)) \\ d<z}} \mu(d) + O\left(\sum_{\substack{d|(\xi(n),\mathcal{P}(w)) \\ z\le d<zw}} 1 \right).$$

Observe that a prime $p > w > 1$ and some $d \mid \mathcal{P}(w)$ both divide $\xi(n)$ if and only if pd divides $\xi(n)$. Thus, we pick some parameter $z_p > 1$ which we will determine later and we split $\mathcal{S}_p(w)$ using the Lemma as follows:

$$\begin{aligned}
\mathcal{S}_p(w) &= \sum_{\substack{x<n\le 2x \\ \xi(n)\equiv 0 \pmod p}} \sum_{d|(\xi(n),P(w))} \mu(d) \\
&= \sum_{\substack{x<n\le 2x \\ \xi(n)\equiv 0 \pmod p}} \sum_{\substack{d|(\xi(n),\mathcal{P}(w)) \\ d<z_p}} \mu(d) + O\left(\sum_{\substack{x<n\le 2x \\ \xi(n)\equiv 0 \pmod p}} \sum_{\substack{d|(\xi(n),\mathcal{P}(w)) \\ z_p\le d<z_p w}} 1 \right) \\
&= \sum_{\substack{d|\mathcal{P}(w) \\ d<z_p}} \mu(d) N(x;pd) + O\left(\sum_{\substack{d|\mathcal{P}(w) \\ z_p\le d<z_p w}} N(x;pd) \right) \\
&= S_1(p) + O(S_2(p)),
\end{aligned}$$

say. For $S_2(p)$ we obtain

$$S_2(p) \ll x^{\epsilon} \sum_{z_p\le d<z_p w} \left(\frac{x}{d^k p^k} + 1 \right) \ll x^{\epsilon} \left(\frac{x}{p^k z_p^{k-1}} + z_p w \right).$$

We will pick $z_p = p^{-1}(x/w)^{1/k}$ to minimize this error term. Here we set $y = (x/w)^{1/k}$ to ensure that $z_p > 1$. Note that $y = pz_p$. Using the fact that $\sum_{p\le x} p^{-1} \ll x^{\epsilon}$ we can deduce that

$$\sum_{w\le p<y} S_2(p) \ll x^{1/k+\epsilon} w^{1-1/k}.$$

Next, we use the trivial estimate (2.25) again to conclude that

$$-\sum_{w\le p<y} S_1(p) = x\sum_{w\le p<y}\sum_{\substack{d\mid\mathcal{P}(w)\\ pd<y}}\frac{\mu(pd)\rho(pd)}{(pd)^k} + O(yx^{\epsilon}).$$

The double sum equals

$$x\sum_{d<y}{}'\frac{\mu(d)\rho(d)}{d^k} = x\sum_{d=1}^{\infty}{}'\frac{\mu(d)\rho(d)}{d^k} + O(x^{1+\epsilon}y^{1-k}), \tag{2.26}$$

where the $\sum'$ restricts the sum to those $d \mid \mathcal{P}(x^{1/k})$ with exactly one exceptional prime divisor $p \mid d$ such that $p > w$. Thus, we have shown that

$$-\sum_{w\le p\ll x^{1/k}} \mathcal{S}_p(w) = c^{(1)}x + O(x^{1/k+\epsilon}w^{1-1/k}),$$

where $c^{(1)}$ is the constant from (2.26), the sum over those d having exactly one large prime divisor $p > w$. Next, we consider the sum $\mathcal{S}(w)$. Similarly to the above argument, we may apply Lemma 13 for some $z > 1$ to obtain

$$\mathcal{S}(w) = \sum_{\substack{d\mid\mathcal{P}(w)\\ d<z}}\mu(d)N(x;d) + O\left(\sum_{\substack{d\mid P(w)\\ z\le d<zw}} N(x;d)\right). \tag{2.27}$$

Again, we use a trivial estimate for the second sum which yields an error term $O(x^{1/k+\epsilon}w^{1-1/k})$ provided we chose $z = (x/w)^{1/k}$ optimally. The first sum in (2.27) is

$$x\sum_{\substack{d\mid\mathcal{P}(w)\\ d<z}}\frac{\mu(d)\rho(d)}{d^k} + O(z).$$

Thus, we have shown that

$$\mathcal{S}(w) = c^{(0)}x + O(x^{1/k+\epsilon}w^{1-1/k}),$$

where

$$c^{(0)} = \sum_{d|\mathcal{P}(w)} \frac{\mu(d)\rho(d)}{d^k}$$

is the sum over those d having no large prime divisors $p > w$. Recall that the overall main term is $cx = x\sum_{d=1}^{\infty} \mu(d)\rho(d)d^{-k}$. The sum $c - c^{(0)} - c^{(1)}$ is the sum over those d having at least 2 distinct prime divisors $> w$ and thus we have

$$c^{(0)} + c^{(1)} = c + O\left(x^{\epsilon} \sum_{d>w^2} \frac{1}{d^k}\right) = c + O(x^{\epsilon} w^{2-2k}).$$

We minimize the error terms by choosing $w = x^{1/(2k+1)}$ so that both our error terms $O(x^{1+\epsilon}w^{2-2k})$ and $O(x^{1/k+\epsilon}w^{1-1/k})$ become $O(x^{3/(2k+1)+\epsilon})$. Thus, we have shown

$$\mathcal{S}(w) - \sum_{w\leq p\ll x^{1/k}} \mathcal{S}_p(w) = cx + O(x^{3/(2k+1)+\epsilon}),$$

and it remains to find a bound for the sum $\sum_{w\leq q<p\ll x^{1/k}} \mathcal{S}_{pq}(q)$. First we consider the terms corresponding to those prime pairs $q < p$ with $pq \ll x^{1/k}$. A trivial estimate suffices to yield the bound

$$\sum_{\substack{w\leq q<p\ll x^{1/k}\\ pq\ll x^{1/k}}} \mathcal{S}_{pq}(q) \ll \sum_{\substack{w\leq q<p\ll x^{1/k}\\ pq\ll x^{1/k}}} N(x;pq) \ll x^{\epsilon} \sum_{\substack{w\leq q<p\ll x^{1/k}\\ pq\ll x^{1/k}}} \left(\frac{x}{p^k q^k} + 1\right) \ll x^{3/(2k+1)+\epsilon}.$$

For the values with $pq \gg x^{1/k}$ observe that

$$\mathcal{S}_{pq}(q) \ll N(x;pq) = \#\{x < n \leq 2x : p^k \mid l_i(n), q^k \mid l_j(n) \text{ for some } i \neq j\}.$$

(The case $i = j$ cannot occur since $pq \gg x^{1/k}$ for any suitable implied constant).

Thus, we can fix a particular i and j and conclude that

$$\sum_{\substack{w\le q<p\ll x^{1/k}\\ pq\gg x^{1/k}}} \mathcal{S}_{pq}(q) \ll_r \#\mathcal{K},$$

where

$$\mathcal{K} = \{(p,q,u,v) : w \le q < p \ll x^{1/k}, pq \gg x^{1/k}, p^k u = l_i(n), q^k v = l_j(n)\}.$$

Without loss of generality we may write $l_i(n) = a_1 n + b_1$ and $l_j(n) = a_2 n + b_2$ so that we are left with the Diophantine equation $a_1 q^k v - a_2 p^k u = a_1 b_2 - a_2 b_1 = h \neq 0$ say. Note that $(a_1 q^k v, a_2 p^k u) = (a_1 v, a_2 u)$ since neither p nor q divide h since h is $O(1)$ and p and q are $\gg x^{1/(2k+1)}$. Each common divisor of $a_1 v$ and $a_2 u$ is a divisor of h and thus is $O(1)$. Since also a_1 and a_2 are $O(1)$ we can reduce our problem to $d(h) = O(1)$ equations of the form (2.1) with the additional constraint that $(du, ev) = 1$ and $de \gg x^{1/k}$. Thus, we have reduced the problem to the case we dealt with in Theorem 6. Thus, this gives an error term $O(x^{\max\{\omega(k),3/(2k+1)\}+\epsilon})$ for the asymptotic formula in Theorem 7. Note that $\omega(k) \le 3/(2k+1)$ for all $k \ge 2$ which concludes the proof.

2.5 The Proof of Theorem 8

We now turn to the problem of consecutive square-full integers. Recall that here, $N(x)$ is the number of integers $n \le x$ such that both n and $n+1$ are square-full. Observe that every square-full integer n can uniquely be written as $n = a^2 b^3$ with $\mu^2(b) = 1$. Thus, we have

$$N(2x) - N(x) \ll \#\left\{(d,e,u,v) \in \mathbb{N}^4 : x < d^3u^2 = e^3v^2 - 1 \le 2x\right\}.$$

As in the proof of Theorem 6 we can now split the ranges of d and e into $O(x^\epsilon)$ boxes with $D/2 < d < D$ and $E/2 < e \leq E$ where $D, E \ll x^{1/3}$. For one such box we then get

$$N(2x) - N(x) \ll x^\epsilon \mathcal{N}(x; D, E),$$

where

$$\mathcal{N}(x; D, E) = \#\left\{(d, e, u, v) \in \mathbb{N}^4 : x < d^3u^2 = e^3v^2 - 1 \leq 2x, d \asymp D, e \asymp E\right\}.$$

Thus, in order to prove Theorem 8, it remains to show that

$$\mathcal{N}(x; D, E) \ll_\epsilon x^{29/100+\epsilon}.$$

For convenience, we will set $y = x^{29/100}$. We may now apply Theorem 5 with $k = 3, l = 2$ and $U := x^{1/2}D^{-3/2}$, $V := x^{1/2}E^{-3/2}$ so that $v \asymp V$ and $u \asymp U$. We get the bound

$$\mathcal{N}(x; D, E) \ll_\epsilon x^\epsilon \min\{(DEM)^{1/2} + D + E, (UVM)^{1/2} + U + V\}, \tag{2.28}$$

where the value of M is as stated in Theorem 5. We will further impose the condition $M \geq x^{9/50}$. We will see below that this will not make our bound worse. The situation we are now in is different compared to the situation in section 2.3.2, where we used the estimate $D + E \ll x^{1/k}$. In our situation here this would produce an estimate $\mathcal{N}(x; D, E) \ll_\epsilon x^{1/3+\epsilon}$ which is worse than our anticipated bound. And without further restricting the ranges of D and E, it will not be possible to improve this bound. The results by Estermann and Thue allow us to assume further that $\min(DE, UV) \geq y$. This is however still not enough to improve upon the estimate $\mathcal{N}(x; D, E) \ll_\epsilon$

$x^{1/3+\epsilon}$. Thus, we shall employ an estimate similar to (2.15), namely:

$$\mathcal{N}(x; D, E) \ll_\epsilon EU \left(\frac{D}{E^3} + 1\right) x^\epsilon. \tag{2.29}$$

We will now distinguish two cases depending on whether $DE^{-3} \ll 1$ does or does not hold. If $DE^{-3} \ll 1$ for some suitable constant, then we may assume $EU \geq y$ by the above estimate. Note that by definition of U,

$$y^5 \leq (DE)(EU)^4 = \left(\frac{E}{D}\right)^5 x^2,$$

so that

$$\frac{V}{U} = \left(\frac{D}{E}\right)^{3/2} \leq \frac{x^{3/5}}{y^{3/2}} = x^{33/200} < x^{9/50} \leq M.$$

Next, we consider the case $DE^{-3} \gg 1$. Here, the estimate (2.29) is too weak for our purposes and we need a stronger approach. The idea is to fix a pair (e, u) and estimate the number of solutions (d, e, u, v) counted by $\mathcal{N}(x; D, E)$. Let $d_1, \ldots, d_\mu$ be the solutions to the congruence $d^3 \equiv -u^{-2} \pmod{e^3}$. In particular, $\mu \ll e^\epsilon \ll x^\epsilon$ and we get the estimate

$$\mathcal{N}(x; D, E) \ll \sum_{e \sim E} \sum_{u \sim U} \sum_{i=1}^{\mu} \#\{(a, v) : v \sim V, a \ll D/E^3, e^3v^2 - (d_i + ae^3)^3u^2 = 1\}.$$

Thus, it suffices to estimate the number of points (a, v) that satisfy

$$p(v) - q(a) - 1 = 0, \tag{2.30}$$

where p is a polynomial of degree 2 and q is a polynomial of degree 3. The left-hand side of (2.30) is absolutely irreducible (see for example Schmidt [41, Theorem III.1B]). Next, we will proceed to apply Theorem 15 of Heath-Brown [19] to get an upper bound for the number of pairs (v, a) satisfying (2.30). Using the notation of Heath-Brown's

theorem we will set $n := 2$, $B_1 = V$ and $B_2 = DE^{-3} + 1$ so that indeed $v \leq B_1$ and $a \leq B_2$ with $B_1, B_2 \geq 1$. Note that $T = \max(B_1^2, B_2^3) \geq B_1^2$ so that the points (v, a) satisfying (2.30) lie on at most $k \ll_\epsilon x^\epsilon B_2^{1/2}$ auxiliary curves. Thus, using Bézout's Theorem, we may deduce that the number of points (v, a) under consideration is $\ll_\epsilon x^\epsilon B_2^{1/2}$. Thus, we get the estimate

$$\mathcal{N}(D, E) \ll_\epsilon x^\epsilon EU \left(\frac{D}{E^3} + 1\right)^{1/2} \ll \frac{x^{1/2+\epsilon}}{DE^{1/2}},$$

where the last estimate is because $1 \ll D/E^3$. Hence, we may assume that

$$x^{1/2} D^{-1} E^{-1/2} \geq y.$$

Thus,

$$y^7 \leq \left(\frac{x^{1/2}}{DE^{1/2}}\right)^4 (DE)^3 = x^2 \frac{E}{D},$$

so that

$$\frac{D}{E} \leq \frac{x^2}{y^7} \leq 1.$$

Thus, we have shown that in all cases, $V/U \leq M$. By interchanging the roles of D and E, we may similarly prove that $U/V \leq M$ and hence we conclude that

$$\max(D/E, E/D, U/V, V/U) \leq M.$$

By considering (2.28) again, we may now deduce that

$$\mathcal{N}(x; D, E) \ll_\epsilon x^\epsilon M^{1/2} \min\{DE, UV\}^{1/2}.$$

We will set $DE = x^\psi$ so that $UV = x^{1-3\psi/2}$. Observe that

$$\frac{\log \mathcal{N}(x; D, E)}{\log x} \leq \delta + \frac{1}{2}\min(\psi, 1 - 3\psi/2) + \frac{1}{2}\max\left\{\frac{9}{8}\psi(1 - 3\psi/2), \frac{9}{50}\right\} := f(\psi),$$

say. The function $f(\psi)$ takes its maximum at $\psi = 2/5$ and $f(2/5) = 29/100$. This completes the proof of Theorem 8.

2.6 The Proof of Theorem 9 and Corollary 10

In this proof, all implied constants may depend on α. Our initial argument is the same as in [15]. We want to find $r = r(\alpha)$ as small as possible so that the estimate $S(X, \alpha) \ll_\epsilon X^{r+\epsilon}$ holds. As illustrated in [15], we may assume that $\alpha \geq 1/2$. The estimate (2.4) allows us to assume that $r \geq 1/2$. As in [15], we obtain the estimate $S(X, \alpha) \ll \mathcal{N}(X; D, E)$, where $\mathcal{N}(X; D, E)$ is the number of elements in the set

$$\#\{(d, e, u, v) : d \sim D, e \sim E, u \sim U, v \sim V, e^2 v - d^2 u = h\},$$

where $h \in \{\pm 1, \pm 2\}$ and D, E, U, V, X are positive real numbers such that $E^2 V \asymp D^2 U$, $UV \asymp X$ and $DE \ll X^\alpha$. In particular,

$$V \asymp X^{1/2} D/E \quad \text{and} \quad U \asymp X^{1/2} E/D. \tag{2.31}$$

We want to apply Theorem 5 with $x = E^2 V$, $k = 2$ and $l = 1$. Note the trivial estimate

$$\mathcal{N}(X; D, E) \ll DE \left(\frac{V}{D^2} + 1 \right) \ll X^{1/2} + DE.$$

Hence, if $DE \ll X^r$ then this estimate suffices. Thus, we may assume that $DE \geq X^r$. In particular, this shows that $DE \geq X^{1/2}$ and from $x^2 \asymp (DE)^2 X$ we can then conclude that $DE \gg x^{1/2}$. So, Theorem 5 does indeed apply. We get the estimate

$$\mathcal{N}(X; D, E) \ll_\epsilon X^\epsilon \min\{(XM)^{1/2} + U + V, (DEM)^{1/2} + D + E\},$$

where D, E, U and V are as in (2.31) and

$$\log M = \frac{9}{8}\frac{\log(DE)\log X}{\log(DEX^{1/2})},$$

since $x = E^2V \asymp DEX^{1/2}$ and $UV \asymp X$. As in the proof of Theorem 14, we get the estimate

$$\mathcal{N}(X; D, E) \ll_\epsilon X^\epsilon EU\left(\frac{D}{E^2} + 1\right) = X^\epsilon(X^{1/2} + EU).$$

Note that $EU = X^{1/2}E^2/D$. Hence we may assume that $E^2/D \geq X^{r-1/2}$ and similarly we assume that $D^2/E \geq X^{r-1/2}$. Without loss of generality, let $D \leq E$ so that $V \leq U$. First, we consider the case when $M < U/V = (E/D)^2$. In this case,

$$(XM)^{1/2} + U + V < X^{1/2}E/D + U + V \ll U.$$

From $DE \ll X^\alpha$ and $D^2/E \geq X^{r-1/2}$, it follows that $(E/D)^{3/2} \ll X^{(\alpha+1)/2-r}$, and hence

$$\mathcal{N}(X; D, E) \ll_\epsilon X^\epsilon U = X^{1/2+\epsilon}\frac{E}{D} \ll X^{\frac{1}{3}\alpha+\frac{5}{6}-\frac{2}{3}r+\epsilon} \ll X^{r+\epsilon},$$

provided $r > 1/2 + \alpha/5$. This concludes the case $M < U/V$. So, we may now consider the case $M \geq U/V$. Note that $M \geq U/V = (E/D)^2 \geq E/D$ which yields the estimate

$$\mathcal{N}(X; D, E) \ll_\epsilon X^\epsilon M^{1/2}\min\{X, DE\}^{1/2}.$$

We will set $DE = X^\psi$ so that essentially $\psi \leq \alpha$. Then

$$\frac{\log M}{\log X} = \frac{9}{8}\frac{\psi}{\psi + 1/2} =: f(\psi),$$

say. The function $f(\psi)$ is increasing for $\psi > 0$ and hence $f(\psi) \leq f(\alpha)$. This shows that

$$\frac{\log \mathcal{N}(X; D, E)}{\log X} \leq O_\epsilon(1) + \frac{1}{2}f(\alpha) + \frac{1}{2}\min(1, \alpha).$$

This concludes the case $M \geq U/V$. We have therefore proved Theorem 9. Corollary 10 is an easy consequence of Theorem 9.

Chapter 3

Power-Free Values of Polynomials

3.1 Introduction

Let k and n be integers such that $k \geq 2$. Then n is said to be k-free if there is no prime p such that $p^k \mid n$. For an irreducible polynomial $f(x) \in \mathbb{Z}[x]$ of degree d, one expects in general that the set $f(\mathbb{Z}) = \{f(n), n \in \mathbb{Z}\}$ contains infinitely many k-free values. This is clearly not true if f has a fixed k-th power prime divisor, that is, if there exists a prime p such that $p^k \mid f(n)$ for all $n \in \mathbb{Z}$. One can conjecture that this is the only condition under which $f(\mathbb{Z})$ fails to contain infinitely many k-free values. In 1933, Ricci [37] proved this conjecture for $k \geq d$. In fact, he derived an asymptotic formula for the quantity

$$\#\{n \leq X : f(n) \text{ is } k\text{-free}\}. \tag{3.1}$$

Further progress was made by Erdős [13] who proved the conjecture in the case $k = d - 1$ for $d \geq 3$. Later, Hooley [29] derived an asymptotic formula for each such k.

In [13], Erdős proposed the similar question, whether $f(\mathbb{P}) = \{f(p), p \text{ prime}\}$ contains infinitely many $(d-1)$-free values. Hooley [30] proved this conjecture for $d \geq 51$. Nair [34, 35] further refined this result and proved Erdős' conjecture for $d \geq 7$.

Recently, Helfgott [27, 28] has established the conjecture for $d = 3$ and for all quartic polynomials with sufficiently high entropy. Finally, Browning [6] has settled the conjecture for $d \geq 5$. Thus, the conjecture remains open for irreducible quartic polynomials with $Gal(f) = A_4$ or $Gal(f) = S_4$.

In this work, we will settle the conjecture for the remaining cases and establish the following theorem:

Theorem 14. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $d \geq 3$ and assume that f has no fixed $(d-1)$-th power prime divisor. Define*

$$N'_f(X) = \#\{p \leq X : p \text{ prime}, f(p) \text{ is } (d-1)\text{-free}\}.$$

Then, for any $C > 1$, we have

$$N'_f(X) = c'_f \pi(X) + O_{C,f}\left(\frac{X}{(\log X)^C}\right),$$

as $x \to \infty$, where

$$c'_f = \prod_p \left(1 - \frac{\rho'(p^{d-1})}{\phi(p^{d-1})}\right),$$

and

$$\rho'(d) = \#\{n \pmod d : (d, n) = 1, d \mid f(n)\}.$$

It should be noted that our methods are sufficiently robust to save an arbitrary power of $\log X$ in the error term which gives us an improvement over Helfgott's results. Indeed, the worst part of our error term comes from the Siegel-Walfisz Theorem and our methods can save a power of X in the error term for the asymptotic formula for the quantity (3.1) when $k = d - 1$. More precisely, we get the following theorem for a polynomial f as in Theorem 14:

Theorem 15. *Let*

$$N_f(X) = \#\{n \leq X : f(n) \text{ is } (d-1)\text{-free}\}.$$

Then, for some $\delta = \delta(d)$, we have

$$N_f(X) = c_f X + O_f(X^{1-\delta}),$$

as $x \to \infty$, where

$$c_f = \prod_p \left(1 - \frac{\rho(p^{d-1})}{p^{d-1}}\right),$$

and

$$\rho(d) = \#\{n \pmod d : d \mid f(n)\}.$$

It should be noted that our methods break down in the case of $(d-2)$.free values, for example. The work of Browning [6] is in parts a refinement of Heath-Brown [19]. Their proofs use the determinant method and their key idea is to reduce the problem of Theorem 14 to a counting problem where one wants to find an upper bound for the number of points (p, q, h) on the algebraic variety defined by $f(p) = q^{d-1}h$, where p, q and h are restricted to certain sizes. One then uses Theorem 15 of [19] to create a number of auxiliary polynomials $F_i(x, y, z)$ so that for each point (p, q, h) under consideration there exists at least one i such that $F_i(p, q, h) = 0$. One then uses this information to deduce the final bound. Browning's argument then partially relies on work by Salberger [39] about the density of integer points on affine surfaces.

It should be noted that Heath-Brown has applied the approximate determinant method to problems involving power-free values of polynomials previously. In [23], he considered irreducible polynomials of the shape $f(x) = x^d + c$. This problem gets then converted into the approximate Diophantine equation $a^k b = f(n) = n^d + O(1)$.

And points (n, a, b) therefore lie close to the weighted projective curve $X_0^d = X_1 X_2^k$. Thus, the particular shape of f allows Heath-Brown to consider points close to a curve rather than points on a surface. And since the determinant method seems to be more efficient in counting points on varieties with lower dimension, this provides the key saving in his argument. Heath-Brown is able to handle Theorem 14 for $k = d-1$ and $d \geq 3$, provided f has special shape.

Our proofs of Theorem 14 and Theorem 15 will start similarly to the work of Browning and Heath-Brown. We will start with the equation $f(p) = q^{d-1}h$. From there, we will analyze the equation in $\mathbb{Q}(\theta)$, where θ is a root of f. This idea is based on Heath-Brown [22] and we describe the key idea in more detail at the beginning of section 3.3.

3.2 Preliminaries

We will now start the proof of Theorem 14 and Theorem 15. We will use the following terminology in this chapter.

- Pick $\theta \in \mathbb{C}$ such that $f(\theta) = 0$. Then $K = \mathbb{Q}(\theta)$ is a number field and $\mathcal{O}_K$ is the ring of integers of K.
- Let $\mathcal{B} = \{b_0, \ldots, b_{d-1}\}$ be an integral basis of K.
- Let $\mathcal{B}_\theta$ be the $\mathbb{Q}$-basis $\{1, \theta, \ldots, \theta^{d-1}\}$ of K.
- Let $\mathcal{O}_K^\times$ denote the units in $\mathcal{O}_K$.
- Let $\langle \alpha_1, \ldots, \alpha_r \rangle$ denote the ideal of $\mathcal{O}_K$ generated by $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$.
- Let the embeddings of K be $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \ldots, \sigma_{r+2s}$, so that $\sigma_1, \ldots, \sigma_r$ are the real embeddings and $\sigma_{r+1}, \ldots, \sigma_{r+s}$ are each one of the complex conjugate pairs of embeddings. In particular, $r + 2s = [K : \mathbb{Q}] = d$.

- If $\gamma \in K$ then we denote the conjugate of γ under an embedding σ by γ^σ.
- Let Δ_K^2 be the discriminant of K and let let $\Delta^2(\theta)$ be the discriminant associated to $\mathcal{B}_\theta$. In particular, $\Delta^2(\theta) = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 \cdot \Delta_K^2$.
- We write $x \sim X$ to say that $X < x \leq 2X$ and we write $x \asymp X$ to say that there exist positive constants A, B, independent of X, such that $AX \leq |x| \leq BX$.

Our first task is to turn the problem into a problem where we count solutions of a Diophantine equation. More precisely, we shall prove the following lemma:

Lemma 16. *Let X be sufficiently large and let $\delta > 0$ and $\eta > 0$ be arbitrary. Then there exists values A and B with*

$$X^{1-\delta} \ll A, B \ll X^{1+\delta}, \tag{3.2}$$

and δ', depending on δ and d, such that

$$N_f'(2X) - N_f'(X) = c_f'(\pi(2X) - \pi(X)) + O\left(\frac{X}{(\log X)^C}\right) + O(X^\eta \mathcal{N}(X; A, B)), \tag{3.3}$$

and

$$N_f(2X) - N_f(X) = c_f X + O(X^{1-\delta'}) + O(X^\eta \mathcal{N}(X; A, B)), \tag{3.4}$$

where

$$\mathcal{N}(X; A, B) = \#\{(n, a, b) \in \mathbb{N}^3 : n \sim X, a \sim A, b \sim B, \mu^2(a) = 1, a^{d-1}b = f(n)\}.$$

Proof. First, we observe that

$$\sum_{m^{d-1} | f(p)} \mu(m) = \begin{cases} 1 & \text{if } f(p) \text{ is } (d-1)\text{-free,} \\ 0 & \text{otherwise.} \end{cases}$$

Thus,

$$N'_f(2X) - N'_f(X) = \sum_{p\sim X} \sum_{m^{d-1}|f(p)} \mu(m)$$
$$= \sum_m \mu(m) N'_0(X;m), \tag{3.5}$$

where

$$N'_0(X;m) = \#\{X < p \le 2X : f(p) \equiv 0 \pmod{m^{d-1}}\}.$$

Recall that

$$\rho(d) = \#\{n \pmod{d} : d \mid f(n)\}.$$

Hence, ρ is multiplicative and $\rho(p^{d-1}) \ll_f 1$ and thus,

$$\rho'(m^{d-1}) \le \rho(m^{d-1}) \ll_{\epsilon,f} m^{\epsilon}.$$

The terms of the sum in (3.5) corresponding to small $m \le (\log X)^{2C}$ will contribute the main term of the asymptotic formula. Define $\rho_m = \rho(m^{d-1})$ and let $a_1, \ldots, a_{\rho_m}$ be the solutions of $f(a_i) \equiv 0 \pmod{m^{d-1}}$. Then, an application of the Siegel-Walfisz Theorem yields a constant $c > 0$ such that

$$N'_0(X;m) = \sum_{i=1}^{\rho_m} \#\{X < p \le 2X : p \equiv a_i \pmod{m^{d-1}}\}$$
$$= \sum_{\substack{i \le \rho_m \\ (a_i,m)=1}} (\pi(2X; m^{d-1}, a_i) - \pi(X; m^{d-1}, a_i)) + O(\rho(m^{d-1}))$$
$$= (\pi(2X) - \pi(X)) \frac{\rho'(m^{d-1})}{\phi(m^{d-1})} + O\left(\frac{\rho(m^{d-1})X}{\exp(c\sqrt{\log X})}\right).$$

Let $\epsilon > 0$. Because of the estimate $\phi(n) \gg_\epsilon n^{1-\epsilon}$, we can conclude that

$$\sum_{m \leq (\log X)^{2C}} \frac{\mu(m)\rho'(m^{d-1})}{\phi(m^{d-1})} = \sum_{m=1}^{\infty} \frac{\mu(m)\rho'(m^{d-1})}{\phi(m^{d-1})} + O\left(\sum_{m > (\log X)^{2C}} m^{\epsilon-(d-1)} \right)$$
$$= c'_f + O((\log X)^{-C}).$$

Furthermore,

$$\sum_{m \leq (\log X)^{2C}} \rho(m^{d-1}) \ll \sum_{m \leq (\log X)^{2C}} m^{\epsilon} \ll (\log X)^{4C},$$

and hence altogether:

$$\sum_{m \leq (\log X)^{2C}} \mu(m) N'_0(X; m) = c'_f \pi(X) + O\left(\frac{X}{(\log X)^C} \right).$$

Next, let us consider the contribution to (3.5) of the m in the range $(\log X)^{2C} < m \leq X^{1-\delta_1}$, where $\delta_1 > 0$. For these m, we shall employ the trivial estimate

$$N'_0(X; m) \leq \#\{X < n \leq 2X : m^{d-1} \mid f(n)\} = \rho(m^{d-1}) \left(\frac{X}{m^{d-1}} + O(1) \right)$$
$$\ll X m^{\epsilon-d+1} + m^{\epsilon}.$$

Thus,

$$\sum_{(\log X)^{2C} < m \leq X^{1-\delta_1}} \mu(m) N'_0(X; m) \ll X \sum_{m > (\log X)^{2C}} m^{1-d+\epsilon} + \sum_{m \leq X^{1-\delta_1}} m^{\epsilon}$$
$$= O\left(\frac{X}{(\log X)^C} \right).$$

It remains to find an upper bound for the terms in (3.5) corresponding to the large values of $m > X^{1-\delta_1}$. We get

$$\sum_{m > X^{1-\delta_1}} \mu(m) N'_0(X; m) \ll \#\{(n, a, b) : n \sim X, a > X^{1-\delta_1}, \mu^2(a) = 1, a^{d-1} b = f(n)\}.$$

After a dyadic subdivision of the ranges for a and b, we can deduce that for any $\delta_1 > 0$, there exist values $A \gg X^{1-\delta_1}$ and B such that the equation (3.3) holds.

One can similarly establish (3.4). One starts with the expression

$$\sum_m \mu(m) \#\{X < n \leq 2X : m^{d-1} \mid f(n)\}.$$

The terms corresponding to small $m \leq Y$, say contribute $c_f X + O(X^\epsilon(XY^{2-d} + Y))$ and to optimize the error term, we pick $Y = X^{1/(d-1)}$. The terms with m in the range $X^{1/(d-1)} < m \leq X^{1-\delta_1}$ contribute $O(X^{(1-\delta_1)(1+\epsilon)})$, which is $O(X^{1-\delta'})$ for some δ' depending on δ_1. Similarly to the above argument, the terms with $m > X^{1-\delta_1}$ contribute the remaining error term of (3.4).

Our overall goal is therefore to show that $\mathcal{N}(X; A, B) \ll_\epsilon X^{1-\epsilon}$ for some $\epsilon > 0$, which will then prove Theorem 14 and Theorem 15. Next, we aim to further restrict the ranges of a and b. Note that

$$B \ll_f X^d A^{-(d-1)} \ll X^{1+(d-1)\delta_1},$$

since $A \gg X^{1-\delta_1}$. For our next auxiliary bound, we shall consider the estimate

$$\mathcal{N}(X; A, B) \ll \sum_{b \sim B} \#\{(n, a) : n \sim X, a \sim A, \mu^2(a) = 1, f(n) = a^{d-1}b\}.$$

In the following argument, we fix b and let $n_1, \ldots, n_\nu$ be the solutions of $f(n) \equiv 0 \pmod{b}$. In particular, $\nu = \rho(b) \ll X^\epsilon$. Thus, we get the estimate

$$\mathcal{N}(X; A, B) \ll \sum_{b \sim B} \sum_{i=1}^{\nu} \#\{(t, a) : a \sim A, t \ll X/B + 1, \mu^2(a) = 1, f(n_i + tb) = a^{d-1}b\}. \tag{3.6}$$

Thus, we shall now count solutions (t, a) of the equation

$$f(n_i + tb) - a^{d-1}b = 0. \tag{3.7}$$

The equation (3.7) is of the form $p_1(t) - p_2(a) = 0$, where p_1 is a polynomial of degree d and p_2 is a polynomial of degree $d-1$. To get an upper bound on the number of pairs (t, q) that satisfy (3.7), we shall employ Heath-Brown [19, Theorem 15]. It is easy to see that the polynomial $f(x, y) = p_1(x) - p_2(y)$ is absolutely irreducible and with the same notation as in [19], we may apply the Theorem with $n = 2$, $B_1 \asymp X/B + 1$ and $B_2 \asymp A$, so that $T = \max\{B_1^d, B_2^{d-1}\} \geq B_2^{d-1}$ and hence the points (t, a) satisfying (3.7) lie on at most $k \ll X^{\epsilon} B_1^{\frac{1}{d-1}}$. auxiliary curves. Thus, by Bézout's Theorem and (3.6), we get the estimate

$$\mathcal{N}(X; A, B) \ll X^{\epsilon_1} B (X/B + 1)^{\frac{1}{d-1}}.$$

for any arbitrary $\epsilon_1 > 0$. Let $\delta_2 > 0$. We get a negligible contribution if $B \ll X^{1-\delta_2}$. Hence, we can also assume that for any $\delta_2 > 0$, $B \gg X^{1-\delta_2}$. By using the relation $A^{d-1}B \asymp X^d$, we can furthermore assume, that $A \ll X^{1+\delta_2/(d-1)}$. By picking δ_1 and δ_2 small enough, we can conclude the proof of Lemma 16. □

3.3 Analysis in $\mathbb{Q}(\theta)$

In the previous section, we have shown that the proof of Theorems 14 and 15 can be concluded if we find a suitable upper bound for the number of solutions (n, a, b) of the Diophantine equation $a^{d-1}b = f(n)$. The idea is now to analyze this equation in the field K. This idea is basically from Heath-Brown [22], where he derives an asymptotic formula for the number of $n \leq X$ such that $f(n) = n^2 + 1$ is square-free. Heath-Brown considers the corresponding equation $e^2 f = n^2 + 1$ in the Gaussian integers

$\mathbb{Z}[i]$. Using that $\mathbb{Z}[i]$ has unique factorization, he deduces that there are $\alpha, \beta \in \mathbb{Z}[i]$ such that $n + i = \alpha^2\beta$ with $N(\alpha) = e$ and $N(\beta) = f$. Taking the imaginary part of this equation then gives a bi-homogeneous equation $G(x_0, x_1; y_1, y_2) = 1$ which Heath-Brown then applies the approximate determinant method to.

In our more general setting, there are three issues to tackle. First, in our problem it is not necessarily true that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Secondly, $\mathcal{O}_K$ might not have unique factorization and thirdly, our method will produce an equation system of $d - 1$ bi-homogeneous auxiliary equations. We shall prove the following lemma:

Lemma 17. *Let (n, a, b) be a triple counted by $\mathcal{N}(X; A, B)$. In particular, a is square-free and we can write $a = a_1a_2$ such that $a_1 \mid \Delta^2(\theta)$ and $(a_2, \Delta^2(\theta)) = 1$. Then there exist a triple $(m, m_1, m_2) \in (\mathbb{Z} \setminus \{0\})^3$ such that $m, m_1, m_2 \ll_K 1$ and $\alpha, \beta \in \mathbb{Z}[\theta]$ such that*

$$m(n - \theta) = \alpha^{d-1}\beta, \tag{3.8}$$

with $|N(\alpha)| = m_1a_2$ and $|N(\beta)| = m_2b$. Furthermore, the order of magnitude of the conjugates of α is given by

$$|\alpha^\sigma| \asymp |N(\alpha)|^{1/d}.$$

Proof. In what follows, all ideals will be ideals of $\mathcal{O}_K$. All algebraic integers occuring in the proof can be considered as elements in $\mathcal{O}_K$ unless it is not explicitly stated that they are in fact elements of $\mathbb{Z}[\theta]$.

Step 1: The first step in our proof of Lemma 17 is to consider the ideal $J = \langle n - \theta \rangle$. We observe that $f(n) = N(J)$. In what follows, we want to factorize J. Let q be a prime divisor of a_2 and let P be a prime ideal above q such that $P \mid J$. We will now show that in fact $P^{d-1} \mid J$ and that there is indeed no other prime ideal above q that divides J. Observe that

$$[\mathcal{O}_K : \mathbb{Z}[\theta] + P] \cdot [\mathbb{Z}[\theta] + P : P] = [\mathcal{O}_K : P] = N(P). \tag{3.9}$$

Hence, $[\mathcal{O}_K : \mathbb{Z}[\theta] + P] \mid N(P)$, and thus, $[\mathcal{O}_K : \mathbb{Z}[\theta] + P]$ is a power of q. However, we also have

$$\Delta_K^2 \cdot [\mathcal{O}_K : \mathbb{Z}[\theta] + P]^2 \cdot [\mathbb{Z}[\theta] + P : \mathbb{Z}[\theta]]^2 = \Delta_K^2 \cdot [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 = \Delta^2(\theta).$$

Hence, $[\mathcal{O}_K : \mathbb{Z}[\theta] + P] \mid \Delta^2(\theta)$ and $q \nmid \Delta^2(\theta)$. Thus, $[\mathcal{O}_K : \mathbb{Z}[\theta] + P] = 1$. Hence, by (3.9), $N(P) = [\mathbb{Z}[\theta] + P : P]$. This together with $P \mid \langle n - \theta \rangle$ and $P \mid \langle q \rangle$ gives that a set of representatives for $(\mathbb{Z}[\theta] + P)/P$ is given by $\{0, 1, \ldots, q-1\}$, so that in fact $N(P) = q$. Now assume that there are two prime ideals P_1, P_2 above q, both dividing J. We can factorize $f(x)$ into irreducible factors modulo q:

$$f(x) \equiv \left(\prod_i (x - n_i) \right) \prod_j f_j(x) \pmod{q},$$

where $\prod_i (x - n_i)$ is the product of the linear factors of f. Recall that $q \nmid \Delta^2(\theta)$ and that $N(P_1) = N(P_2) = q$. Hence, we may employ Kummer's Theorem on factorizations of prime ideals (see for example Weiss [47, Theorem 4-9-1, Exercise 4-9-2]). We deduce that without loss of generality, $P_i = \langle q, \theta - n_i \rangle$ for $i = 1, 2$. Since P_1 divides both $\langle \theta - n_1 \rangle$ and $J = \langle \theta - n \rangle$, we must have that $n - n_1 \in P_1$ and hence $q = N(P_1) \mid N(n - n_1)$. Therefore, $n \equiv n_1 \pmod{q}$ and similarly $n \equiv n_2 \pmod{q}$. Thus, $n_1 \equiv n_2 \pmod{q}$ and therefore, $P_1 = P_2$. Thus, the factor P of J occurs with multiplicity $d - 1$. Hence, we get the ideal factorization $J = I_1^{d-1} I_2$, with $N(I_1) = a_2$ and $N(I_2) = a_1^{d-1} b$.

Step 2: The next idea is to multiply the equation $J = I_1^{d-1} I_2$ by a suitable ideal, so that we can transform the ideals I_1 and I_2 into principal ideals. This well then allow us to get an equation about elements of $\mathcal{O}_K$. It is important that we insure that the norm of the ideal we multiply by is bounded in terms of K. By a corollary of Minkowski's Theorem, we may pick $\alpha_1 \in I_1 \setminus \{0\}$ be such that $|N(\alpha_1)| \leq c_K N(I_1)$

and $\beta_1 \in I_2 \setminus \{0\}$ be such that $|N(\beta_1)| \leq c_K N(I_2)$. In particular, there exist non-zero ideals J_1 and J_2 of $\mathcal{O}_K$ such that $\langle \alpha_1 \rangle = I_1 J_1$ and $\langle \beta_1 \rangle = I_2 J_2$, with $N(J_1) \leq c_K$ and $N(J_2) \leq c_K$. Recall that $\langle n - \theta \rangle = I_1^{d-1} I_2$ and hence $\langle n-\theta \rangle J_1^{d-1} J_2 = \langle \alpha_1^{d-1} \beta_1 \rangle$. Thus, the ideal $J_1^{d-1} J_2$ must be principal. We may therefore assume that $J_1^{d-1} J_2 = \langle \mu \rangle$ for some $\mu \in \mathcal{O}_K \setminus \{0\}$ with $|N(\mu)| \leq C_K^d$. Thus, there are only $O_K(1)$ choices for $N(\mu)$, $N(J_1)$ and $N(J_2)$. There are also only $O_K(1)$ choices for a_1. We can conclude from the above that

$$(n - \theta)\mu = \alpha_1^{d-1} \beta_1 \epsilon_1, \tag{3.10}$$

where $\epsilon_1 \in \mathcal{O}_K^\times$.

Step 3: Later in this chapter, we will need that all the conjugates of α are of equal order of magnitude, which is the motivation of the following sub-lemma:

Lemma 18. *Let $\gamma \in K \setminus \{0\}$. Then, there exists an $\epsilon \in \mathcal{O}_K^\times$ such that $|(\epsilon\gamma)^\sigma| \asymp_K |N(\gamma)|^{1/d}$ for all embeddings σ.*

Proof. Recall from the notation section that the real and complex conjugate embeddings of K are $\sigma_1, \ldots, \sigma_r$ and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$, respectively, where $r + 2s = d$. Let $\underline{v}$ be the vector $(1, 1, \ldots, 1) \in \mathbb{Z}^{r+s}$. We now define the maps ψ and ϕ by

$$\begin{aligned} \psi : K^\times &\to \mathbb{R}^{r+s}, \\ \alpha &\mapsto (\log |\alpha^{\sigma_i}|)_{i=1,\ldots,r+s}, \end{aligned}$$

and

$$\begin{aligned} \phi : \mathbb{R}^{r+s} &\to \mathbb{R}^{r+s}, \\ (x_1, \ldots, x_{r+s}) &\mapsto \eta \cdot \underline{v}, \end{aligned}$$

where $\eta = d^{-1}(\sum_{k=1}^{r} x_k + 2\sum_{k=r+1}^{r+s} x_k)$. Note that ψ is a homomorphism and that ϕ

is a $\mathbb{R}$-linear idempotent map. Furthermore, $(d^{-1}\log|N(\gamma)|)\cdot\underline{v}=\phi(\psi(\gamma))$. Thus, it suffices to show that there exists a unit ϵ such that

$$\phi(\psi(\gamma))-\psi(\epsilon\gamma)\ll_K 1. \tag{3.11}$$

We observe that by Dirichlet's Unit Theorem, ψ maps the units onto a lattice Λ of dimension $r+s-1$. Furthermore, $\phi(\psi(\gamma))-\psi(\gamma)\in$ Ker ϕ and for any unit ϵ, $\psi(\epsilon)\in$ Ker ϕ. Thus, Ker ϕ is a $r+s-1$-dimensional vector space containing the lattice Λ. Thus, by considering $\phi(\psi(\gamma))-\psi(\gamma)$ modulo the fundamental domain of Λ, we can indeed pick ϵ such that (3.11) holds and the implied constant in (3.11) depends only on the size of the fundamental domain of Λ which is determined by K. This proves Lemma 18. □

Thus, by multiplying ϵ_1 and α_1 in (3.10) with suitable units, if necessary, we may assume without loss of generality that $|\alpha_1^\sigma|\asymp|N(\alpha_1)|^{1/d}$ for all σ.

Step 4: The final idea of the proof is to adapt the equation (3.10) so that we get α and β as elements of $\mathbb{Z}[\theta]$, as stated in the Lemma. We want to emphasize once more that we can have $\mathbb{Z}[\theta]\neq\mathcal{O}_K$. Recall that $\mathcal{B}=\{b_0,\dots,b_{d-1}\}$ is an integral basis for K and that $\{1,\theta,\dots,\theta^{d-1}\}$ is a $\mathbb{Q}$-basis for K. Thus, there exist $r_{ij}\in\mathbb{Q}$ such that $b_i=\sum_j r_{ij}\theta^j$. Let r be the least common multiple of the denominators of the r_{ij}. Then, r is an integer determined by K and $\mathcal{B}$ such that $rb_i\in\mathbb{Z}[\theta]$ for all i. Multiplying (3.10) by $r^dN(\mu)\mu^{-1}\in\mathcal{O}_K$, we obtain

$$(n-\theta)N(\mu)r^d=(r\alpha_1)^{d-1}(r\beta_1\epsilon_1N(\mu)\mu^{-1}).$$

We shall put $\alpha=r\alpha_1$ and $\beta=r\beta_1\epsilon_1N(\mu)\mu^{-1}$. Note that α_1 and $\beta_1\epsilon_1N(\mu)\mu^{-1}$ are in $\mathcal{O}_K$ and thus, $\alpha,\beta\in\mathbb{Z}[\theta]$. Also, $|\alpha^\sigma|\asymp|N(\alpha)|^{1/d}$. Furthermore, $N(\alpha)=r^dN(J_1)a_2$ and $N(\beta)=r^dN(J_2)N(\mu)^{d-1}a_1^{d-1}b$. Thus, if we set $m=N(\mu)r^d$, $m_1=r^dN(J_1)$

and $m_2 = r^d N(J_2) N(\mu)^{d-1} a_1^{d-1}$, then m, m_1 and m_2 are non-zero rational integers determined by up to $O_{K,\mathcal{B}}(1)$ choices and the proof of Lemma 17 follows. □

3.4 Applying the Approximate Determinant Method

Recall that $\mathcal{B}_\theta = \{1, \theta, \ldots, \theta^{d-1}\}$ is the θ-power basis of K over $\mathbb{Q}$. We shall need the following lemma:

Lemma 19. *There exist constants $c_0, \ldots, c_{d-1} \in K$ only depending on K with the following property: If $\gamma = \sum_{i=0}^{d-1} r_i \theta^i$ with $r_i \in \mathbb{Q}$ is an arbitrary element of K, then $r_i = \mathrm{Tr}(c_i \gamma)$.*

Proof. Note that $c_0, \ldots, c_{d-1} \in K$ is just the complementary basis $\mathcal{B}_\theta$. It is possible to derive explicit formulae for the c_i (See Weiss [47, Prop. 3-7-12], for example) but this does not seem to help to improve our results. We give a quick proof of Lemma 19. We write $\mathbf{v}$ for a vector $(v_i)_{i=0,\ldots,d-1}$, and we also define the trace of a vector to be the coordinate-wise application of the trace, i.e. $\mathrm{Tr}(\mathbf{v}) = (\mathrm{Tr}(v_i))_i$. Furthermore, let $\mathcal{C}$ be the matrix $(\mathrm{Tr}(\theta^{i+j}))_{j,i=0,\ldots,d-1}$. Then $\mathcal{C} \in \mathbb{M}_d(\mathbb{Z})$. Observe that $\mathcal{C}$ has determinant $\det(\mathcal{C}) = \Delta^2(\theta) \neq 0$ and hence is invertible with $\mathcal{C}^{-1} \in \mathbb{M}_d(\mathbb{Q})$. Let $\mathbf{b}_\theta = (1, \theta, \ldots, \theta^{d-1})$. It is clear that $\mathrm{Tr}(\gamma \mathbf{b}_\theta) = \mathcal{C}\mathbf{r}$, and thus

$$\mathbf{r} = \mathcal{C}^{-1} \mathrm{Tr}(\gamma \mathbf{b}_\theta) = \mathrm{Tr}(\mathcal{C}^{-1} \mathbf{b}_\theta \gamma).$$

Hence, if we define $\mathbf{c} = \mathcal{C}^{-1}\mathbf{b}_\theta$, then the claim of the lemma follows. □

We define the map

$$\pi_j(\gamma) = \mathrm{Tr}(c_j \gamma),$$

which thus is the projection of $\gamma \in K$ to its j-th coordinate with respect to the basis

$\mathcal{B}_\theta$.Now let us go back to the equation (3.8). For the remainder of this chapter, we shall write

$$\alpha = \sum_{i=0}^{d-1} x_i \theta^i, \qquad \beta = \sum_{i=0}^{d-1} y_i \theta^i,$$

with $x_i, y_i \in \mathbb{Z}$. By Lemma 19, we have that $y_i = \mathrm{Tr}(c_i\beta) = \sum_\sigma c_i^\sigma \beta^\sigma$. Let

$$y_{i,0} = \sum_\sigma \frac{mnc_i^\sigma}{\alpha^{(d-1)\sigma}}.$$

We use the equation (3.8) to deduce that

$$y_i = y_{i,0} + O_K\left(\max_\sigma |\alpha^{-(d-1)\sigma}|\right). \tag{3.12}$$

By Lemma 17, $|\alpha^\sigma| \asymp |N(\alpha)|^{1/d} \asymp A^{1/d}$ for all σ so that

$$y_i = y_{i,0} + O(A^{-(d-1)/d}).$$

To simplify our notation, we shall now assume that $|x_i| \leq |x_0|$ and $|y_i| \leq |y_0|$ for all i. This assumption will in fact be without loss of generality and x_0 and y_0 could be replaced with any largest x_k and y_l, say. The fact that $N(\alpha) \asymp A$ and $N(\beta) \asymp B$ then implies

$$|x_0| \gg A^{1/d} \text{ and } |y_0| \gg B^{1/d}.$$

Note that from (3.2), we can easily deduce that $X^d \asymp_f A^{d-1}B$, since otherwise $\mathcal{N}(X; A, B) = 0$. Thus, (3.12) implies that $y_i \ll XA^{-(d-1)/d} \ll B^{1/d}$. We also have that $x_i = \mathrm{Tr}(c_i\alpha) \ll A^{1/d}$. Thus, we can deduce the estimates

$$|x_i| \ll A^{1/d}, \text{ and } |y_i| \ll B^{1/d} \text{ for all } i.$$

We also have $|y_{0,0}| \gg B^{1/d}$. Thus, if we set $s_i = x_i/x_0$ and $t_i = y_i/y_0$ for $i = 0, \ldots, d-1$ then

$$t_j = \frac{y_{j,0}}{y_{0,0}} + O\left(\frac{1}{X}\right)$$

for $j = 1, \ldots, d-1$. We write $z_j = N(\alpha^{d-1})y_{j,0}$ for all j. Thus, z_j is a form in $x_0, \ldots, x_{d-1}$ of degree $(d-1)^2$ with coefficients in $\mathbb{C}$. We noted above that $|y_{0,0}| \gg B^{1/d}$ and $N(\alpha) \gg A$. Hence,

$$|z_0 x_0^{-(d-1)^2} n^{-1}| \asymp A^{d-1} B^{1/d} A^{-(d-1)^2/d} X^{-1} = A^{1-1/d} B^{1/d} X^{-1} \asymp 1.$$

Hence, $y_{j,0}/y_{0,0}$ is a rational function in the variables $s_1, \ldots, s_{d-1}$, where the denominator and numerator are both forms of degree $(d-1)^2$. This rational function has coefficients in $\mathbb{C}$ and is independent of n. Thus, we set

$$t_j = F_j(s_1, \ldots, s_{d-1}) + O\left(\frac{1}{X}\right), \tag{3.13}$$

where $F_j = y_{j,0}/y_{0,0}$. We have shown above that the denominator of F_j is $\gg 1$. We now want to find an upper bound on the number of points $(x_0, \ldots, x_{d-1}) \in \mathbb{Z}^d$. We continue by splitting the possible range of the $(d-1)$-tuple $(s_1, \ldots, s_{d-1})$ into $O(M^{d-1})$ boxes of the shape

$$\hat{B} = \{(s_1, \ldots, s_{d-1}) \in \mathbb{Q}^{d-1} : s_i \in (s_{i,0}, s_{i,0} + O(M^{-1})),\ i = 1, \ldots, d-1\}. \tag{3.14}$$

Our goal is to find an upper bound on the number of points $(s_1, \ldots, s_{d-1}) \in \mathbb{Q}^{d-1}$ inside one such box. We impose the conditions

$$X^\eta \ll M^{d-1} \ll \min(A, X)$$

on M. Here, η is a sufficiently small number. Thus, we may now fix all $s_{i,0} \ll 1$ and

one such box $\hat{B}$. Hence, we may assume that

$$s_i = s_{i,0} + \alpha_i, \qquad \alpha_i \ll M^{-1}, \tag{3.15}$$

for $i = 1, \dots, d-1$. Next, consider equation (3.13). Since $M \gg X^{\eta}$, and since F_j has a denominator bounded away from zero, we can assume that F_j has partial derivatives of all orders, and thus, we may apply Taylor's Theorem to deduce that

$$t_j = P_j(\alpha_1, \dots, \alpha_{d-1}) + \beta_j, \qquad \beta_j \ll X^{-1}, \tag{3.16}$$

for $j = 1, \dots, d-1$. Here, P_j is a polynomial in $d-1$ variables of sufficiently large degree (depending on η) with coefficients of size $O(1)$. This is because the coefficients only depend on $s_{1,0}, \dots, s_{d-1,0}$, and $s_{i,0} \ll 1$ for all i, and because the denominator of F_j is $\gg 1$.

We are now ready to apply the approximate determinant method. The idea is to consider the monomials $s_i t_j$, for $(i, j = 0, \dots, d-1)$, where we recall that $s_0 = t_0 = 1$ by definition. We write these monomials as $m_r(\mathbf{s}, \mathbf{t})$, where $r \leq R$, with $R = d^2$. Assume that the solutions of (3.8) with $\mathbf{s} \in \hat{B}$ are $(\mathbf{s}^{(1)}, \mathbf{t}^{(1)}), \dots, (\mathbf{s}^{(J)}, \mathbf{t}^{(J)})$. Then we define the $J \times R$ matrix $\mathcal{M}$ with (j, r)-th entry being $m_r(\mathbf{s}^{(j)}, \mathbf{t}^{(j)})$. Our aim is to show that $\mathcal{M}$ has rank strictly less than R, provided we chose M appropriately. This will then enable us to show that there is a non-zero vector $\mathbf{v}$ such that $\mathcal{M}\mathbf{v} = 0$. Thus, if we define the polynomial $C_{\hat{B}}(\mathbf{s}, \mathbf{t}) = \sum_{r=1}^{R} v_r m_r(\mathbf{s}, \mathbf{t})$, then $C_{\hat{B}}(\mathbf{s}^{(j)}, \mathbf{t}^{(j)}) = 0$ for all our solutions $(\mathbf{s}^{(j)}, \mathbf{t}^{(j)})$ with $\mathbf{s}^{(j)} \in \hat{B}$. Observe that $\mathcal{M}$ is a matrix with rational entries and the vector $\mathbf{v}$ can be constructed from subdeterminants of $\mathcal{M}$. Thus, $\mathbf{v} \in \mathbb{Q}^R$ and by clearing the denominators of the coefficients of $C_{\hat{B}}$, we may assume that $C_{\hat{B}}$ has integer coefficients of size bounded by a power of X. Thus, we shall assume that $\|C_{\hat{B}}\| \ll X^{\kappa}$, say.

We now proceed to show that $\mathcal{M}$ has rank strictly less than R. Without loss of generality $J \geq R$, since otherwise this is trivial. Thus, it suffices to show that every $R \times R$ subdeterminant of $\mathcal{M}$ vanishes. Without loss of generality, let us consider the minor Δ of $\mathcal{M}$ coming from the first R rows and columns. Note that the j-th row of $\mathcal{M}$ has entries with common denominator of size $A^{1/d}B^{1/d}$. Hence, if we can show that $\Delta \ll (AB)^{-\frac{R}{d}}$, then $\Delta = 0$. Substituting (3.15) and (3.16) into our matrix, we obtain a generalized $R \times R$ Vandermonde determinant in α_i and β_j with entries of the shape

$$(s_{i,0} + \alpha_i)^{\epsilon_1}(P_j(\alpha_1, \ldots, \alpha_{d-1}) + \beta_j)^{\epsilon_2},$$

with $i, j \in \{1, \ldots, d-1\}$ and $\epsilon_1, \epsilon_2 \in \{0, 1\}$. Note that we have

$$\alpha_i \ll T_1^{-1}, \qquad \beta_j \ll T_2^{-1},$$

where $T_1 \asymp M$ and $T_2 \asymp X$. We assign to a monomial in $\alpha_1, \ldots, \alpha_{d-1}, \beta_1, \ldots, \beta_{d-1}$ its obvious size of the form $T_1^{-a}T_2^{-b}$. We then order all the possible monomial sizes in decreasing size, $1 = M_0 \geq M_1 \geq \ldots$, say. In this list, we count the sizes with multiplicities. For example, all the monomials α_i will give rise to the same size T_1^{-1} and hence T_1^{-1} occurs $d-1$ times in the list. Lemma 3 of Heath-Brown [21] gives us the following bound on Δ:

$$\Delta \ll_d \prod_{r=1}^{R} M_r.$$

We have that $T_1 \ll T_2^{1/(d-1)}$ and $d \geq 3$. We first consider the case $d \geq 4$ in which the largest monomial sizes are $1 \geq T_1^{-1} \geq T_1^{-2} \geq T_1^{-3}$. The number of monomials of degree D in N variables is

$$n(D, N) = \binom{N + D - 1}{D}.$$

The number of monomials M_h with size T_1^{-m} is $n(m, d-1)$. Observe that

$$\mathcal{S} := \sum_{m=0}^{2} n(m, d-1) = \frac{1}{2} d(d+1) < d^2 = R,$$

and

$$\sum_{m=0}^{3} n(m, d-1) = \frac{1}{6} d(d+1)(d+2) \geq d^2 = R$$

for all $d \geq 3$. Thus, the factors in $\prod_r M_r$ are all of size T_1^{-m}, with $m \in \{0, 1, 2, 3\}$, and we obtain the bound $\Delta \ll T_1^{-\xi} \ll M^{-\xi}$, where

$$\xi = \sum_{m=0}^{2} mn(m, d-1) + 3 \cdot (R - \mathcal{S}) = \frac{1}{2}(d-1)(5d+2).$$

Thus, if $(AB)^d M^{-\xi} \ll 1$ with a suitably small implied constant, then $\Delta = 0$.

We apply a similar argument in the case $d = 3$. We will pick M such that $X^{1/3} \leq M \leq X^{1/2}$. As above, we consider an $R \times R$ matrix with $R = 9$. The largest 9 monomials are $1, \alpha_1, \alpha_2, \alpha_1^2, \alpha_1\alpha_2, \alpha_2^2, \beta_1, \beta_2, \alpha_1^3$. Thus, $\Delta \ll M^{-11} X^{-2}$. Therefore, $M^{11} \gg (AB)^3 X^{-2}$ implies $\Delta = 0$. And indeed, $(AB)^{3/11} X^{-2/11} \gg X^{1/3}$, since $A, B \gg X^{1-\delta}$, if δ is small enough. Thus, we have proved the following lemma:

Lemma 20. *Assume that M is an integer satisfying*

$$(AB)^{\frac{2d}{(5d+2)(d-1)}} \ll M \ll \min(X^{1/(d-1)}, A^{1/(d-1)}),$$

if $d \geq 4$ and

$$(AB)^{3/11} X^{-2/11} \ll M \ll \min(X^{1/2}, A^{1/2})$$

if $d = 3$. Then for any box $\hat{B}$ of shape (3.14)*, there exists a non-zero bilinear integer form $C_{\hat{B}}(\mathbf{x}; \mathbf{y})$, with coefficients of size $\|C_{\hat{B}}\| \ll X^{\kappa}$ such that $C_{\hat{B}}(\mathbf{x}, \mathbf{y}) = 0$ for all solutions of* (3.8) *with $\mathbf{s} \in \hat{B}$.*

3.5 Counting Points inside a box

Observe that by Lemma 17,

$$\sum_{j=0}^{d-1} y_j \pi_i(\alpha^{d-1}\theta^j) = \pi_i(\alpha^{d-1}\beta) = m\pi_i(n+\theta) = \begin{cases} m & \text{if } i = 1 \\ 0 & \text{if } 2 \le i \le d-1 \end{cases}$$

for $1 \le i \le d-1$. We ignore the equation for $i = 0$ because we want the left-hand side of our equations to have size $O_K(1)$. We define $G_{i,j}(\mathbf{x}) = \pi_i(\alpha^{d-1}\theta^j)$ for $1 \le i \le d-1$ and $0 \le j \le d-1$. Then, the $G_{i,j}(\mathbf{x})$ are forms of degree $d-1$ with integer coefficients in the variables $\mathbf{x}$. We shall write the form $C_{\hat{B}}$ from Lemma 20 as $C_{\hat{B}}(\mathbf{x};\mathbf{y}) = \sum_{j=0}^{d-1} y_j G_{d,j}(\mathbf{x})$. Then the forms $G_{d,j}(\mathbf{x})$ are linear with integer coefficients. Let $\mathbf{e} = (m, 0, 0, \ldots, 0) \in \mathbb{Z}^d$ and define the matrix

$$\mathcal{G} = \mathcal{G}(\mathbf{x}) = (G_{i,j}(\mathbf{x}))_{i=1,\ldots,d;\ j=0,\ldots,d-1}.$$

Then $\mathcal{G}$ is a $d \times d$ matrix and we have the equation system

$$\mathcal{G}(\mathbf{x}).\mathbf{y} = \mathbf{e}. \tag{3.17}$$

Our next aim is to apply a change of variables to the vector $\mathbf{x}$ in order to rewrite the condition $\mathbf{s} \in \hat{B}$ more conveniently. We will proceed similarly to Heath-Brown [23]. We recall that for $i = 1, \ldots, d-1$ we have that $s_i = s_{i,0} + O(1/M)$ and that $s_i = x_i/x_0$, where $x_0 \asymp A^{1/d}$. Thus,

$$|x_i - s_{i,0}x_0| \ll A^{1/d}/M.$$

Next, we define the linear operator $T : \mathbb{R}^d \to \mathbb{R}$ by

$$T(x_0, x_1, \ldots, x_{d-1}) = (MA^{-1/d}(x_1 - s_{1,0}x_0), \ldots, MA^{-1/d}(x_{d-1} - s_{d-1,0}x_0), A^{-1/d}x_0).$$

Then

$$\Lambda = \{T(\mathbf{x}) : \mathbf{x} \in \mathbb{Z}^d\}$$

is a lattice of determinant $\det(\Lambda) = M^{d-1}A^{-1}$. If we define the rectangle

$$\mathcal{R} = \{(v_0, \ldots, v_{d-1}) \in \mathbb{R}^d : |v_i| \ll 1 \text{ for } 0 \leq i \leq d-1\},$$

where the implied constants are suitably chosen, then we are interested in counting the points falling into $\Lambda \cap \mathcal{R}$. There exists a basis $\mathbf{g}^{(0)}, \ldots, \mathbf{g}^{(d-1)}$ of vectors in Λ such that if we write $\mathbf{v} \in \Lambda$ as $\mathbf{v} = \sum_i \lambda_i \mathbf{g}^{(i)}$, then

$$\lambda_i \ll |\mathbf{v}|/|\mathbf{g}^{(i)}|$$

for all i. Furthermore,

$$\prod_{i=0}^{d-1} |\mathbf{g}^{(i)}| \asymp \det(\Lambda).$$

It can be deduced from the proof of Davenport [10, Lemma 5] that a basis with such properties exists. Next, we define U_i to be a suitable constant times $|\mathbf{g}^{(i)}|^{-1}$ for $i = 0, \ldots, d-1$, say. Then we can change the basis so that our variables $x_0, \ldots, x_{d-1}$ become $u_0, \ldots, u_{d-1}$, and $|u_i| \leq U_i \leq U_0$ for all i. Furthermore, the U_i satisfy

$$\prod_{i=0}^{d-1} U_i \asymp \det(\Lambda)^{-1} = \frac{A}{M^{d-1}}.$$

Thus, our equation system (3.17) becomes

$$\mathcal{G}(L(\mathbf{u})).\mathbf{y} = \mathbf{e},$$

with $|u_i| \leq U_i \leq U_0$ and $U_0^d \gg A/M^{d-1} \gg 1$, and where L is the invertible linear function such that $L(\mathbf{u}) = \mathbf{x}$.

Our goal is now to count the contribution from each of our boxes $\hat{B}$ using the equation system (3.17). More precisely, we shall prove the following:

Lemma 21. *The number of* $\mathbf{x}$ *with* $\mathbf{s} \in \hat{B}$ *which satisfy the equation* (3.17) *for some* $\mathbf{y}$ *is* $O(U_0^{d-1} X^{\epsilon})$.

Proof. Let $\Delta = \Delta(\mathbf{x})$ be the determinant of $\mathcal{G}(\mathbf{x})$ and for $i = 0, \ldots, d-1$, let $\Delta_i = \Delta_i(\mathbf{x})$ be the determinant of the matrix that we obtain when we replace the $(i+1)$-th column of $\mathcal{G}$ by the vector $\mathbf{e}$. Then, by Cramer's Rule we obtain the equation system

$$\Delta y_i = \Delta_i \qquad (i = 0, \ldots, d-1).$$

We can see that Δ is a form of degree $(d-1)^2 + 1$ in $\mathbf{x}$, and that Δ_i are forms of degree $(d-1)(d-2)+1$ in $\mathbf{x}$.

We proceed to show that Δ does not vanish identically. Consider the $d \times d$ matrix $\mathcal{G}_1 = (\sigma_i(\theta^j))_{i=1,\ldots,d;j=0,\ldots,d-1}$. Then

$$\det(\mathcal{G}_1) = \prod_{1 \leq i < j \leq d} (\sigma_i(\theta) - \sigma_j(\theta)) = \Delta(\theta) \neq 0,$$

and thus, $\mathcal{G}_1$ is invertible and we may define the linear forms $F_1, \ldots, F_d$ by the following vector-matrix multiplication:

$$(F_1, \ldots, F_d) = (G_{d,0}, \ldots, G_{d,d-1}) \mathcal{G}_1^{-1}.$$

For the purposes of showing $\Delta \not\equiv 0$, the F_i may be seen as linear forms in the variables $\mathbf{a} = (\sigma_1(\alpha), \ldots, \sigma_d(\alpha))$ with coefficients in $\bar{\mathbb{Q}}$. Furthermore, let $\mathcal{G}_2$ be the diagonal $d \times d$ matrix with diagonal entries $\sigma_1(\alpha^{d-1}), \ldots, \sigma_d(\alpha^{d-1})$. Then, we may factorize

the matrix $\mathcal{G}$ as follows:

$$\mathcal{G} = \begin{pmatrix} \pi_1(\alpha^{d-1}) & \dots & \pi_1(\alpha^{d-1}\theta^{d-1}) \\ \vdots & & \vdots \\ \pi_{d-1}(\alpha^{d-1}) & \dots & \pi_{d-1}(\alpha^{d-1}\theta^{d-1}) \\ G_{d,0} & \dots & G_{d,d-1} \end{pmatrix} = \begin{pmatrix} \sigma_1(c_1) & \dots & \sigma_d(c_1) \\ \vdots & & \vdots \\ \sigma_1(c_{d-1}) & \dots & \sigma_d(c_{d-1}) \\ \frac{F_1(\mathbf{a})}{\sigma_1(\alpha^{d-1})} & \dots & \frac{F_d(\mathbf{a})}{\sigma_d(\alpha^{d-1})} \end{pmatrix} \mathcal{G}_2\mathcal{G}_1.$$

Thus,

$$\det(\mathcal{G}) = \pm N_{K/\mathbb{Q}}(\alpha^{d-1})\Delta(\theta)\sum_{i=1}^{d} \frac{F_i(\mathbf{a})}{\sigma_i(\alpha^{d-1})}(-1)^{i+1}\det(\mathcal{A}_i), \tag{3.18}$$

where

$$\mathcal{A} = (\sigma_j(c_i))_{i=0,\dots,d-1;j=1,\dots,d}$$

is a $d \times d$ matrix and for $r = 1, \dots, d$, the $(d-1) \times (d-1)$ matrix $\mathcal{A}_r$ is obtained by deleting the first row and the r-th column of $\mathcal{A}$. Recall from Lemma 19 that the vector $\mathbf{c}$ is given by $\mathcal{C}\mathbf{c} = \mathbf{b}_\theta$ and that $\det(\mathcal{C}) = \Delta^2(\theta) \in \mathbb{Q} \setminus \{0\}$. For $i = 1, \dots, d$, let $\mathcal{C}_i$ be the matrix obtained by replacing the i-th column of $\mathcal{C}$ by $\mathbf{b}_\theta$. Then, by Cramer's Rule,

$$\det(\mathcal{C})c_i = \det(\mathcal{C}_{i+1}) \qquad (i = 0, \dots, d-1).$$

Note that $\mathcal{C} = \mathcal{C}_1$ and hence $\mathrm{Tr}(c_0) = 1$. Furthermore, $\mathcal{C}_{i+1}$ has two equal columns for $i \neq 0$ and hence $\mathrm{Tr}(c_i) = 0$ for $1 \leq i \leq d-1$. (The fact that $\mathrm{Tr}(c_i) = \delta_{i=0}$ also follows from the fact that the c_i form a complementary basis to $\mathbf{b}_\theta$). Thus, we can deduce that $\det(\mathcal{A}_i) + \det(\mathcal{A}_{i+1}) = 0$ for all $i = 1, \dots, d-1$. In particular,

$$(-1)^{i+1}\det(\mathcal{A}_i) = \det(\mathcal{A}_1)$$

for all i. The matrix $\mathcal{C}$ has entries in $\mathbb{Z}$ and hence we get $\mathcal{C}\sigma(\mathbf{c}) = \sigma(\mathbf{b}_\theta)$ for any embedding σ. Hence $\mathcal{C}\mathcal{A} = \mathcal{G}_1^T$ and therefore $\det(\mathcal{A}) = (\Delta(\theta))^{-1}$. By expanding

$\det(\mathcal{A})$ along the first row, we get

$$(\Delta(\theta))^{-1} = \sum_{i=1}^{d} \sigma_i(c_0)(-1)^{i+1} \det(\mathcal{A}_i) = \det(\mathcal{A}_1)\,\mathrm{Tr}(c_0) = \det(\mathcal{A}_1).$$

Putting this into (3.18), we obtain that

$$\det(\mathcal{G}) = \pm N_{K/\mathbb{Q}}(\alpha^{d-1}) \sum_{i=1}^{d} \frac{F_i(\mathbf{a})}{\sigma_i(\alpha^{d-1})} = \pm \sum_{i=1}^{d} F_i(\mathbf{a}) \prod_{\substack{j=1 \\ j\neq i}}^{d} a_j^{d-1},$$

where $a_j = \sigma_j(\alpha)$. The auxiliary form $C_{\hat{B}}$ created by Lemma 20 does not vanish identically. Hence, at least one of the forms F_i does not vanish identically. Thus, we may assume that F_r, say is not identically zero. Note that

$$\det(\mathcal{G}) \equiv \pm F_r(\mathbf{a}) \prod_{\substack{j=1 \\ j\neq r}}^{d} a_j^{d-1} \qquad (\mathrm{mod}\ a_r^{d-1}).$$

By considering the right-hand side as a polynomial in a_r, it cannot vanish identically because $F_r(\mathbf{a})$ is a non-zero linear form. Therefore, $\det(\mathcal{G})$ does not vanish identically.

Recall that the total degree of $\Delta = \det(\mathcal{G})$ is $D = (d-1)^2+1$, say. Our next aim is to apply a further linear change of variables, $\mathbf{u} = M\mathbf{v}$, so that v_0^D occurs with non-zero coefficient in Δ. We have shown that Δ does not vanish identically and hence we may use Theorem 1 of Heath-Brown [18] to deduce that there exists a primitive vector $\mathbf{u_0} \in \mathbb{Z}^d$ such that $\Delta(\mathbf{u_0}) \neq 0$ and $|\mathbf{u_0}| \ll_d 1$. Let $\mathbf{u_0}$ be the first column of M. It is then possible to complete M to a $d \times d$ matrix having integer entries and determinant 1. The entries of M are all bounded in size in terms of $\mathbf{u_0}$ so that $\max_{i,j} |M_{i,j}| \ll_d 1$. Furthermore, $\Delta(M.(1,0,\ldots,0)^T) = \Delta(\mathbf{u_0}) \neq 0$. Since M is unimodular, M^{-1} has entries in $\mathbb{Z}$. This ensures indeed that $v_i \in \mathbb{Z}$ with $v_i \ll U_0$ for all i. Thus, the linear change of variables $\mathbf{u} = M\mathbf{v}$ ensures that v_0^D occurs with non-zero coefficient in Δ but it does not make any difference to our argument otherwise. We shall therefore

consider $\Delta' = \Delta(M\mathbf{v})$ and $\Delta'_0 = \Delta_0(M\mathbf{v})$ in the remaining argument.

The number of vectors $\mathbf{v}$ with $\Delta' = 0$ is $O_d(U_0^{d-1})$. This can be established after factorizing Δ' into irreducible factors and by applying [18, Theorem 1] to each factor. Thus, we may now consider the points $\mathbf{v}$ with $\Delta'(\mathbf{v}) \neq 0$.

There are $O(U_0^{d-1})$ choices for the points $(v_1, \ldots, v_{d-1})$. We fix one such point and we will show that there are only $O_\epsilon(X^\epsilon)$ choices for v_0. Consider $\Delta' = \Delta'(v_0)$ and $\Delta'_0 = \Delta'_0(v_0)$ as polynomials in v_0 with integer coefficients. By dividing the polynomial equation $\Delta' y_0 = \Delta'_0$ by a common factor, if necessary, we may assume that $F(v_0)y_0 = F_0(v_0)$, where $F(x)$ and $F_0(x)$ are coprime polynomials in $\mathbb{Z}[x]$. Also note that the degree of F must be at least 1 because the degree of Δ' in v_0 is strictly larger than the degree of Δ'_0 in v_0. By the Euclidean algorithm, there exist polynomials $g_0(x), g(x) \in \mathbb{Z}[x]$ such that

$$g_0(x)F_0(x) + g(x)F(x) = R, \tag{3.19}$$

where R is the resultant of F and F_0 in the variable v_0, depending on $v_1, \ldots, v_{d-1}$. Note that $R \neq 0$ because F and F_0 do not have a common root. The resultant can be defined as the determinant of the Sylvester Matrix of F and F_0 which only depends on the coefficients of F and F_0. Recall that these coefficients only depend on the polynomial f and on the coefficients of the auxiliary equation created by Lemma 20. Thus, R is bounded by a power of X. Substituting $F(v_0)y_0 = F_0(v_0)$ into (3.19), we get that $F(v_0) \mid R$, and hence there are only $O_\epsilon(X^\epsilon)$ choices for v_0. And therefore, if we put all cases together, then there are $O(U_0^{d-1}X^\epsilon)$ choices for $(v_0, \ldots, v_{d-1})$ and each choice of $\mathbf{v}$ gives exactly one choice for $\mathbf{x}$ with $\mathbf{s} \in \hat{B}$. This finishes the proof of Lemma 21. $\square$

3.6 Finishing the Proof

We shall now finish the proof of Theorem 14 and Theorem 15. In the previous section we have shown that the number of $\mathbf{x}$ with $\mathbf{s} \in \hat{B}$ that satisfy (3.17) is $O(U_0^{d-1}X^{\epsilon})$. It thus remains to sum up the contributions from all boxes. We write the vector $\mathbf{g}^{(0)}$ in Λ from the previous section as

$$\mathbf{g}^{(0)} = (MA^{-1/d}(x_1 - s_{1,0}x_0), \dots, MA^{-1/d}(x_{d-1} - s_{d-1,0}x_0), A^{-1/d}x_0).$$

Recall further that U_0 was defined to be a suitable constant times $|\mathbf{g}^{(0)}|^{-1}$. Thus,

$$\begin{aligned} &U_0|x_i - s_{i,0}x_0| \ll A^{1/d}M^{-1} \qquad (i = 1, \dots, d-1), \\ &U_0|x_0| \ll A^{1/d}. \end{aligned}$$

We produce the boxes $\hat{B}$ by taking $s_{i,0} = \frac{z_i}{M}$, where $z_i \ll M$ is an integer. Hence, the number of boxes $\hat{B}$ for which $U_0 \sim U$ is at most the number of $(2d-1)$-tuples $(x_0, \dots, x_{d-1}, z_1, \dots, z_{d-1})$ for which

$$z_i x_0 = Mx_i + O\left(\frac{A^{1/d}}{U}\right), \qquad x_0 \ll \frac{A^{1/d}}{U}, \qquad z_i \ll M,$$

where $i = 1, \dots, d-1$. Recall that by asumption on M, we have that $U^d \gg A/M^{d-1} \gg 1$. Recall that $x_i \leq |x_0|$ for all i and hence, if $x_0 = 0$ then $\mathbf{x} = \mathbf{0}$ which is impossible. So, we may assume that $|x_0| \geq 1$ and therefore $A^{1/d}U^{-1} \gg 1$. We now fix one of the $O(A^{1/d}/U)$ choices for x_0. For $i = 1, \dots, d-1$, there exist integers $r_i \ll A^{1/d}U^{-1}$ such that

$$z_i x_0 = Mx_i + r_i. \tag{3.20}$$

Thus, there are $O\left((A^{1/d}U^{-1})^{d-1}\right)$ choices for $r_1, \ldots, r_{d-1}$, since $A^{1/d}U^{-1} \gg 1$. The congruences

$$Mx_i \equiv -r_i \pmod{x_0}$$

determine $x_1, \ldots, x_{d-1}$ modulo x_0, provided x_0 and M are coprime. Indeed,

$$1 \leq |x_0| \ll \frac{A^{1/d}}{U} \ll M^{1-1/d},$$

and thus $|x_0| < M$ if X and hence M are large enough. Furthermore, we may pick M to be a prime in Lemma 20, which then indeed insures that M and x_0 are coprime. Now, x_i, x_0 and r_i determine z_i by (3.20). Thus, the number of intervals for which $U_0 \sim U$ is $O\left(\frac{A}{U^d}\right)$. By Lemma 21, each of these intervals contributes at most $O(U^{d-1}X^{\epsilon})$ choices for $\mathbf{x}$. Thus, the intervals for which $U_0 \sim U$ contribute

$$X^{\epsilon}\frac{A}{U^d} \cdot U^{d-1} = X^{\epsilon}\frac{A}{U} \ll X^{\epsilon}(AM)^{1-1/d}$$

choices for $\mathbf{x}$. Hence, after a dyadic subdivision for the range of U_0, we may assume that the total number of choices for $\mathbf{x}$ is $X^{\epsilon}(AM)^{1-1/d}$. Each such $\mathbf{x}$ determines α and hence, each $\mathbf{x}$ gives $O(1)$ choices for a_2 by Lemma 17. Note that there are only $O_K(1)$ values for a_1 such that $a_1 \mid \Delta_K^2$. Hence, $\#\{a : (n, a, b) \text{ is counted by } \mathcal{N}(X; A, B)\} \ll X^{\epsilon}(AM)^{1-1/d}$. Thus, by a trivial estimate, we deduce that for each $\epsilon, \epsilon' > 0$,

$$\begin{aligned}\mathcal{N}(X; A, B) &\ll \sum_a \#\{n \sim X : f(n) \equiv 0 \pmod{a^{d-1}}\} \ll \sum_a \rho(a^{d-1})\left(\frac{X}{a^{d-1}} + 1\right) \\ &\ll X^{\epsilon}\sum_a 1 \ll X^{2\epsilon}(AM)^{1-1/d} \ll M^{1-1/d}X^{1-1/d+\epsilon'}.\end{aligned}$$

Thus, it suffices if there exists a $\eta > 0$ such that $M^{d-1} \ll X^{1-\eta}$. By Lemma 20, we can indeed pick such an M because $\frac{4d}{5d+2} < \frac{4}{5}$ for $d \geq 4$. If $d = 3$ then M is essentially $X^{4/11}$ and $8/11 < 1$. This finishes the proof of Theorem 14 and 15.

Chapter 4

Integer Points on Bilinear and Trilinear Equations

4.1 Introduction

In this chapter we will derive an upper bound for the number of projective integer points that satisfy a bilinear or trilinear form. The respective theorems will be Theorem 23 and Theorem 30 below. The advantage of our results is that the bounds depend on the coefficients of the multilinear form and that the main terms in our bounds are essentially optimal. In the trilinear case, we will discuss the irreducibility and singularity of the associated form. We will employ elementary lattice results to prove our claims.

Attention should be given to work by Robbiani [38] and Spencer [42]. In their papers, they use variants of the circle method to derive an asymptotic formula for the number of points on (smooth) bilinear hypersurfaces in the more general bi-projective space $\mathbb{P}^s(\mathbb{Q}) \times \mathbb{P}^s(\mathbb{Q})$ for $s \geq 2$. Their work cannot be directly compared to ours since they use the anticanonical height function. Both papers illustrate the Manin conjecture for bilinear forms.

4.2 Bilinear Forms

We note the following fact about bilinear forms:

Lemma 22. *Let $A = (a_{ij})$ be a 2×2 matrix with associated bilinear form $f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T A \mathbf{y}$. Then f is irreducible if and only if $\det(A) \neq 0$. If f is reducible then it factorizes into a product of two linear factors.*

Proof. This is a well known result and can quickly be verified by direct calculation. □

We will prove the following theorem:

Theorem 23. *Let $A = (a_{ij})$ be a 2×2 matrix with associated bilinear form*

$$f(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T A \mathbf{y}$$

and determinant $\Delta := \det(A)$. Suppose that $\gcd(a_{11}, a_{21}, a_{12}, a_{22}) = 1$. We assume that f is irreducible over $\mathbb{Z}$ so that $\Delta \neq 0$. Let X_1, X_2, Y_1, Y_2 be real numbers ≥ 1 and define

$$\mathcal{N}(\mathbf{X}, \mathbf{Y}) = \#\left\{(\mathbf{x}, \mathbf{y}) : |x_i| \leq X_i, |y_i| \leq Y_i, (x_1, x_2) = (y_1, y_2) = 1, f(\mathbf{x}, \mathbf{y}) = 0\right\}.$$

Then

$$\mathcal{N}(\mathbf{X}, \mathbf{Y}) \ll \min\left\{X_1X_2, Y_1Y_2, \mathrm{d}(\Delta)\left(\sqrt{\frac{X_1X_2Y_1Y_2}{|\Delta|}} + 1\right)\right\},$$

where $\mathrm{d}(\Delta)$ is the number of divisors of Δ.

Proof. We want to count solutions to the equation

$$f(\mathbf{x}, \mathbf{y}) = x_1(a_{11}y_1 + a_{12}y_2) + x_2(a_{21}y_1 + a_{22}y_2) = 0,$$

say. Let us write this equation as

$$f(\mathbf{x}, \mathbf{y}) = x_1 L_1(\mathbf{y}) + x_2 L_2(\mathbf{y}) = 0.$$

First let us consider the case when $L_1(\mathbf{y}) = 0$. Note that $\mathbf{y}$ is a primitive vector and hence in particular, it is non-zero. If furthermore, $L_2(\mathbf{y}) = 0$ then we have a non-zero solution to the equation $A\mathbf{y} = 0$ which is impossible since $\Delta \neq 0$. Thus, we have $x_2 = 0$ which implies that $x_1 = \pm 1$ since $\mathbf{x}$ is a primitive vector. There are at most 4 choices for $\mathbf{y}$ such that $L_1(\mathbf{y}) = 0$. This is easy to see after we divide a_{11} and a_{12} by (a_{11}, a_{12}) in the equation $a_{11}y_1 + a_{12}y_2 = 0$. Thus, the case $L_1(\mathbf{y}) = 0$ contributes $O(1)$ to $\mathcal{N}(\mathbf{X}, \mathbf{Y})$. The case $L_2(\mathbf{y}) = 0$ is analogous. Now, if $x_1 = 0$ then $x_2 = \pm 1$ which reduces to the case $L_2(\mathbf{y}) = 0$. Thus, we may assume that

$$x_1 x_2 L_1(\mathbf{y}) L_1(\mathbf{y}) \neq 0.$$

Since x_1 and x_2 are coprime, we can therefore deduce the existence of a non-zero integer q such that

$$\begin{aligned} -qx_1 &= a_{21}y_1 + a_{22}y_2, \\ qx_2 &= a_{11}y_1 + a_{12}y_2. \end{aligned}$$

If we set

$$P = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

then we have $qP\mathbf{x} = A\mathbf{y}$. Interchanging the roles of $\mathbf{x}$ and $\mathbf{y}$, we can similarly deduce that there is a non-zero integer q' such that $q'P\mathbf{y} = A^T\mathbf{x}$. Combining the two equations, we get

$$qq'\mathbf{x} = -\Delta\mathbf{x}.$$

The vector $\mathbf{x}$ is primitive and therefore non-zero. This allows us to conclude that

$$qq' = -\Delta.$$

Since Δ is non-zero, there are $\mathrm{d}(\Delta)$ choices for q. We now fix one such choice and count the respective contribution to $\mathcal{N}(\mathbf{X}, \mathbf{Y})$. We first note that $q \mid A\mathbf{y}$. This will give us a lattice condition on $\mathbf{y}$, which is described in the following lemma:

Lemma 24. *Fix an integer $m \geq 2$. Let $M = (m_{ij})$ be an $m \times 2$ matrix. Let q be a non-zero integer such that q divides all of the $m(m-1)/2$ minors of size 2×2 of M. Furthermore, assume that there exists no prime $p \mid q$ which divides all the entries of M. Then*

$$\Lambda_q = \{\mathbf{v} \in \mathbb{Z}^2 : q \mid M\mathbf{v}\}$$

is a lattice of determinant q.

Proof. (of Lemma) It is clear that Λ_q is an integer lattice. We proceed to calculate its determinant. We decompose $q = \prod p_i^{e_i}$ into its prime powers and consider the (additive) group homomorphism

$$\phi_i : \mathbb{Z}^2 \to \mathbb{Z}^m / p_i^{e_i}\mathbb{Z}^m$$

given by $\phi_i(\mathbf{v}) = M\mathbf{v} \pmod{p_i^{e_i}}$. By assumption of the lemma, there exists an element of M which is not divisible by p_i. We assume without loss of generality that $p_i \nmid m_{11}$. The other cases are analogous. Let m_{11}^{-1} be the multiplicative inverse of m_{11} modulo $p_i^{e_i}$. Let $\mathbf{w} \equiv m_{11}^{-1}(m_{11}, m_{21}, \ldots, m_{m1})^T \pmod{p_i^{e_i}}$. We claim that $\mathrm{Im}(\phi_i)$ is cyclic with generator $\mathbf{w}$. First note that for any $\lambda \in \mathbb{Z}/p_i^{e_i}\mathbb{Z}$, $\phi_i(\lambda m_{11}^{-1}, 0) \equiv \lambda\mathbf{w} \pmod{p_i^{e_i}}$. Furthermore, assume $\mathbf{u} = M\mathbf{v}$. Then for $j = 2, \ldots, m$:

$$u_1 m_{j1} m_{11}^{-1} = m_{j1}v_1 + m_{12}m_{j1}m_{11}^{-1}v_2 \equiv m_{j1}v_1 + m_{j2}v_2 = u_j,$$

where the last equality follows from the fact that $p_i^{e_i}$ divides the minor $m_{11}m_{i2} - m_{12}m_{i1}$. Hence, we have indeed that $\mathbf{u} = u_1\mathbf{w}$, and $\mathbf{w}$ generates the image of ϕ_i. We now consider the group homomorphism

$$\phi : \mathbb{Z}^2 \to \mathbb{Z}^m/q\mathbb{Z}^m$$

given by $\phi(\mathbf{v}) = M\mathbf{v} \pmod q$. By the Chinese remainder theorem and by what we just showed, we have that $|\operatorname{Im}(\phi)| = q$. We note that $\operatorname{Ker}(\phi) = \Lambda_q$ and it follows by the first Isomorphism Theorem for groups that

$$\det(\Lambda_q) = [\mathbb{Z}^2 : \Lambda_q] = |\operatorname{Im}(\phi)| = q,$$

which proves the lemma. □

We now recall that $q \mid A\mathbf{y}$. Thus, Lemma 24 shows that $\mathbf{y} \in \Lambda_y$, where Λ_y is a lattice of determinant $|q|$. The bounds $|y_1| \leq Y_1$ and $|y_2| \leq Y_2$ let us deduce that $\mathbf{y}$ is inside the ellipse defined by

$$E_y = \left\{ \mathbf{y} \in \mathbb{R}^2 : \left(\frac{y_1}{\sqrt{2}Y_1}\right)^2 + \left(\frac{y_2}{\sqrt{2}Y_2}\right)^2 \leq 1 \right\}.$$

The area of this ellipse is $A(E_y) = 2\pi Y_1 Y_2$. Similarly, $\mathbf{x} \in E_x \cap \Lambda_x$, where E_x is an ellipse of area $A(E_x) = 2\pi X_1 X_2$, and Λ_x is an integer lattice of determinant $|q'|$. Thus, we have reduced the problem to one where we need to count primitive lattice points inside an ellipse. We will employ Lemma 2 of Heath-Brown [26], which we state here for convenience:

Lemma 25. *Let $\Lambda \subseteq \mathbb{R}^2$ be a lattice of determinant $\det(\Lambda)$. Let $E \subseteq \mathbb{R}^2$ be an ellipse, centered at the origin, together with its interior, and let $A(E)$ be the area of E. Then there is a positive number $\alpha = \alpha(\Lambda, E)$ and a basis $\mathbf{b}_1$, $\mathbf{b}_2$ of Λ such that $\lambda_1\mathbf{b}_1 + \lambda_2\mathbf{b}_2 \in E$ implies $|\lambda_1| \leq \alpha$ and $|\lambda_2| \leq A(E)/(\alpha \det(\Lambda))$. Furthermore, the*

number of primitive lattice points in Λ contained in E is at most

$$4\left(\frac{A(E)}{\det(\Lambda)}+1\right).$$

Thus,

$$\mathcal{N}(\mathbf{X},\mathbf{Y}) \ll \sum_{qq'=-\Delta} \min\left\{\frac{X_1X_2}{|q'|},\frac{Y_1Y_2}{|q|}\right\}+\mathrm{d}(\Delta)$$

Since $qq'=-\Delta$, and by using the inequality $\min(A,B)\leq\sqrt{AB}$ we obtain the bound

$$\mathcal{N}(\mathbf{X},\mathbf{Y}) \ll \mathrm{d}(\Delta)\left(\sqrt{\frac{X_1X_2Y_1Y_2}{|\Delta|}}+1\right).$$

The bound

$$\mathcal{N}(\mathbf{X},\mathbf{Y}) \ll \min(X_1X_2,Y_1,Y_2)$$

can be deduced as follows. There are $O(X_1X_2)$ choices for $\mathbf{x}$. Fix one such $\mathbf{x}$. The equation $f(\mathbf{x},\mathbf{y})=0$ cannot be zero identically because $\mathbf{x}$ is a primitive vector and $\Delta\neq 0$. Thus, there are $O(1)$ choices for $\mathbf{y}$. A similar argument yields the bound $O(Y_1Y_2)$. This proves the theorem. □

4.3 Trilinear Forms

Let $A=(a_{ijk})$ be a $2\times2\times2$ hypermatrix. We associate with A its hyperdeterminant

$$\begin{aligned}D :=\ & a_{122}^2a_{211}^2+a_{111}^2a_{222}^2+a_{212}^2a_{121}^2+a_{112}^2a_{221}^2\\ & -2a_{111}a_{122}a_{211}a_{222}-2a_{211}a_{122}a_{112}a_{221}-2a_{211}a_{122}a_{212}a_{121}-2a_{222}a_{111}a_{212}a_{121}\\ & -2a_{222}a_{111}a_{112}a_{221}-2a_{112}a_{121}a_{212}a_{221}+4a_{112}a_{121}a_{211}a_{222}+4a_{111}a_{122}a_{212}a_{221}.\end{aligned}$$

We will give a brief outline of some properties of D below. For some further details on hyperdeterminants, the reader may consult the text by Gel'fand, Kapranov and

Zelevinsky [17]. We define a trilinear form $f = f_A : \mathbb{R}^3 \to \mathbb{R}$ by

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathbf{x}^T (A\mathbf{z})\mathbf{y}.$$

Here, $A\mathbf{z}$ denotes the standard hypermatrix-vector multiplication along the third dimension of A. In particular,

$$A\mathbf{z} = M_{xy}(\mathbf{z}) := z_1 \begin{pmatrix} a_{111} & a_{121} \\ a_{211} & a_{221} \end{pmatrix} + z_2 \begin{pmatrix} a_{112} & a_{122} \\ a_{212} & a_{222} \end{pmatrix}$$

is an ordinary 2x2 matrix depending only on $\mathbf{z}$. We similarly define 2x2 matrixes $M_{yz}(\mathbf{x})$ and $M_{zx}(\mathbf{y})$ by

$$M_{yz}(\mathbf{x}) := x_1 \begin{pmatrix} a_{122} & a_{121} \\ a_{112} & a_{111} \end{pmatrix} + x_2 \begin{pmatrix} a_{222} & a_{221} \\ a_{212} & a_{211} \end{pmatrix}$$

and

$$M_{xz}(\mathbf{y}) := y_1 \begin{pmatrix} a_{111} & a_{112} \\ a_{211} & a_{212} \end{pmatrix} + y_2 \begin{pmatrix} a_{121} & a_{122} \\ a_{221} & a_{222} \end{pmatrix},$$

so that

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \mathbf{x}^T M_{xy}(\mathbf{z})\mathbf{y} = \mathbf{y}^T M_{yz}(\mathbf{x})\mathbf{z} = \mathbf{z}^T M_{zx}(\mathbf{y})\mathbf{x}.$$

By taking transposes on the equation $f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = 0$ it makes sense to define

$$M_{yx}(\mathbf{z}) := M_{xy}(\mathbf{z})^T, \quad M_{zy}(\mathbf{x}) := M_{yz}(\mathbf{x})^T, \quad M_{xz}(\mathbf{y}) := M_{zx}(\mathbf{y})^T.$$

Furthermore, let

$$\begin{aligned}\Delta_{xy} = \Delta_{xy}(\mathbf{z}) &:= \det(M_{xy}(\mathbf{z})),\\ \Delta_{yz} = \Delta_{yz}(\mathbf{x}) &:= \det(M_{yz}(\mathbf{x})),\\ \Delta_{zx} = \Delta_{zx}(\mathbf{y}) &:= \det(M_{zx}(\mathbf{y})).\end{aligned}$$

Then

$$\begin{aligned}\Delta_{xy}(\mathbf{z}) &= (a_{111}a_{221} - a_{121}a_{211})\, z_1^2 + (a_{111}a_{222} + a_{112}a_{221} - a_{212}a_{121} - a_{211}a_{122})\, z_2 z_1\\ &\quad + (a_{112}a_{222} - a_{122}a_{212})\, z_2^2,\\ \Delta_{yz}(\mathbf{x}) &= (a_{111}a_{122} - a_{112}a_{121})\, x_1^2 + (a_{111}a_{222} + a_{211}a_{122} - a_{112}a_{221} - a_{212}a_{121})\, x_2 x_1\\ &\quad + (a_{211}a_{222} - a_{212}a_{221})\, x_2^2,\\ \Delta_{zx}(\mathbf{y}) &= (a_{111}a_{212} - a_{112}a_{211})\, y_1^2 + (a_{111}a_{222} + a_{212}a_{121} - a_{112}a_{221} - a_{211}a_{122})\, y_2 y_1\\ &\quad + (a_{121}a_{222} - a_{122}a_{221})\, y_2^2.\end{aligned}$$

Lemma 26. *The discriminants of the quadratic forms Δ_{xy}, Δ_{yz} and Δ_{zx} are all equal to D.*

Proof. This can be verified by direct calculation. It suffices to show that

$$\begin{aligned}D &= (a_{111}a_{222} + a_{112}a_{221} - a_{212}a_{121} - a_{211}a_{122})^2\\ &\qquad - 4\,(a_{111}a_{221} - a_{121}a_{211})\,(a_{112}a_{222} - a_{122}a_{212})\\ &= (a_{111}a_{222} + a_{211}a_{122} - a_{112}a_{221} - a_{212}a_{121})^2\\ &\qquad - 4\,(a_{111}a_{122} - a_{112}a_{121})\,(a_{211}a_{222} - a_{212}a_{221})\\ &= (a_{111}a_{222} + a_{212}a_{121} - a_{112}a_{221} - a_{211}a_{122})^2\\ &\qquad - 4\,(a_{111}a_{212} - a_{112}a_{211})\,(a_{121}a_{222} - a_{122}a_{221})\,.\end{aligned}$$

□

Lemma 27. *Assume that*

$$Q(\mathbf{x}) = ax_1^2 + bx_1x_2 + cx_2^2 \in \mathbb{Z}[\mathbf{x}]$$

is a binary quadratic form with discriminant $D(Q) = b^2 - 4ac = 0$. *Then,* $D(Q) = 0$ *if and only if* $Q(\mathbf{x}) = CL(\mathbf{x})^2$ *for some (possibly zero)* $C \in \mathbb{Q}$, *and a linear form* $L(\mathbf{x}) \in \mathbb{Z}[\mathbf{x}]$ *with integer coefficients.*

Lemma 28.

i) Assume that Δ_{xy} *vanishes identically. Then* Δ_{yz} *or* Δ_{zx} *also vanishes identically.*

ii) If Δ_{xy} *and* Δ_{yz} *vanish identically then* f *factorizes over* $\mathbb{Q}$ *as*

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = L(\mathbf{y})B(\mathbf{x}, \mathbf{z}), \tag{4.1}$$

where L *is a linear form, and* B *is a bilinear form. Furthermore,* $\Delta_{zx}(\mathbf{y}) = \det(B)L(\mathbf{y})^2$, *where* $\det(B)$ *is the determinant of the matrix associated to* B.

iii) If f *has a linear factor* $L(\mathbf{y})$ *over* $\mathbb{Z}$ *then* Δ_{xy} *and* Δ_{yz} *both vanish identically.*

iv) f *splits in three linear factors over* $\mathbb{Z}$ *if and only if* Δ_{xy}, Δ_{yz} *and* Δ_{zx} *all vanish identically.*

Proof. We prove the first two claims when $a_{111}a_{222} \neq 0$. Assume that Δ_{xy} vanishes identically. Then all the coefficients of Δ_{xy} vanish, that is:

$$\begin{aligned} a_{111}a_{221} - a_{121}a_{211} &= 0 \\ a_{112}a_{222} - a_{122}a_{212} &= 0 \\ a_{111}a_{222} + a_{112}a_{221} - a_{212}a_{121} - a_{211}a_{122} &= 0. \end{aligned} \tag{4.2}$$

Using just the first two equations, we get

$$\Delta_{yz}(\mathbf{x}) = \frac{(a_{111}a_{222} - a_{212}a_{121})\,(x_1a_{122} + x_2a_{222})\,(x_1a_{111} + x_2a_{211})}{a_{111}a_{222}}$$

and

$$\Delta_{zx}(\mathbf{y}) = \frac{(a_{111}a_{222} - a_{211}a_{122})\,(y_1a_{212} + y_2a_{222})\,(y_1a_{111} + y_2a_{121})}{a_{111}a_{222}}.$$

If we substitute the first two equations of (4.2) into the third one, we obtain that

$$\frac{(a_{111}a_{222} - a_{211}a_{122})\,(a_{111}a_{222} - a_{212}a_{121})}{a_{111}a_{222}} = 0.$$

If $a_{111}a_{222} - a_{211}a_{122} = 0$ then $\Delta_{zx}(\mathbf{y})$ vanishes identically and

$$\Delta_{yz}(\mathbf{x}) = \frac{(a_{212}a_{121} - a_{211}a_{122})}{a_{222}a_{122}}\,(x_1a_{122} + x_2a_{222})^2\,.$$

Furthermore, $f(\mathbf{x}, \mathbf{y}, \mathbf{z})$ factorizes as follows:

$$\frac{(x_1a_{122} + x_2a_{222})\,(a_{122}a_{212}z_2y_1 + a_{122}y_1z_1a_{211} + a_{122}y_2z_2a_{222} + y_2z_1a_{121}a_{222})}{a_{222}a_{122}}.$$

This proves i) and ii) in the case under consideration. In the case $a_{111}a_{222} - a_{212}a_{121} = 0$, we note that $\Delta_{yz}(\mathbf{x})$ vanishes identically and the calculations are similar. It is not difficult to verify i) and ii) if $a_{111}a_{222} = 0$.

We now prove iii). If

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (b_1y_1 + b_2y_2)\,(c_1x_1z_1 + c_2x_1z_2 + c_3x_2z_1 + c_4x_2z_2)$$

then

$$a_{111} = b_1c_1,\ a_{112} = b_1c_2,\ a_{121} = b_2c_1,\ a_{122} = b_2c_2,$$
$$a_{211} = b_1c_3,\ a_{221} = b_2c_3,\ a_{212} = b_1c_4,\ a_{222} = b_2c_4,$$

and it can easily be verified by direct calculation that Δ_{xy} and Δ_{yz} both vanish identically. The statement iv) follows directly from ii) and iii). □

Lemma 29. *The following are equivalent*

i) $D = 0$.

ii) There exists a non-trivial point in $(\mathbb{P}^1)^3$ *at which all partial derivatives of* f *vanish.*

iii) f *is singular in* $(\mathbb{P}^1)^3$.

Proof.

ii) ⇒ i) Assume for a contradiction that all partial derivatives of f vanish at a point in $(\mathbb{P}^1)^3$ and that $D \neq 0$. Thus, by Lemma 27, there are precisely two distinct solutions $\mathbf{z_1}, \mathbf{z_2} \in \mathbb{P}$ to the equation $\Delta_{xy}(\mathbf{z}) = 0$. If $M_{xy}(\mathbf{z_1})$ is identically zero, then

$$M_{xz}(\mathbf{y})\mathbf{z_1} = M_{xy}(\mathbf{z_1})\mathbf{y} = \mathbf{0},$$

for all $\mathbf{y} \in \mathbb{P}$. This means that for all $\mathbf{y} \in \mathbb{P}$, there is a non-zero vector in the kernel of $M_{xz}(\mathbf{y})$. Thus, $\Delta_{xz}(\mathbf{y})$ vanishes identically and therefore $D = 0$, which contradicts our assumption. Therefore, $M_{xy}(\mathbf{z_1})$ cannot vanish identically and there must be $\mathbf{y_2} \in \mathbb{P}$ such that $M_{xy}(\mathbf{z_1})\mathbf{y_2} = 0$. We note that $\mathbf{y_2}$ is unique (up to a scalar multiple), since otherwise $M_{xy}(\mathbf{z_1})$ would vanish identically. Similarly, there exists a unique $\mathbf{y_1} \in \mathbb{P}$ such that $M_{xy}(\mathbf{z_2})\mathbf{y_1} = 0$. If $\mathbf{y_1} = \mathbf{y_2}$ then

$$M_{xz}(\mathbf{y_1})\mathbf{z_1} = M_{xz}(\mathbf{y_1})\mathbf{z_2}.$$

But similarly to the above argument, there must be a unique $\mathbf{z} \in \mathbb{P}$ such that $M_{xz}(\mathbf{y_1})\mathbf{z} = 0$. But, by assumption we have that $\mathbf{z_1} \neq \mathbf{z_2}$. Therefore, $\mathbf{y_1} \neq \mathbf{y_2}$. Similarly, we can find $\mathbf{x_1}, \mathbf{x_2} \in \mathbb{P}$ with $\mathbf{x_1} \neq \mathbf{x_2}$ such that $M_{yx}(\mathbf{z_1})\mathbf{x_2} = 0$ and $M_{yx}(\mathbf{z_2})\mathbf{x_1} = 0$. We can now write an arbitrary $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in (\mathbb{P}^1)^3$ as

$$(a_1\mathbf{x_1} + a_2\mathbf{x_2}, b_1\mathbf{y_1} + b_2\mathbf{y_2}, c_1\mathbf{z_1} + c_2\mathbf{z_2}),$$

say. This is possible since $\mathbf{x_1}, \mathbf{x_2}$ and $\mathbf{y_1}, \mathbf{y_2}$ and $\mathbf{z_1}, \mathbf{z_2}$ are all bases for $\mathbb{P}^1$. We can then see that

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = a_1b_1c_1f(\mathbf{x_1}, \mathbf{y_1}, \mathbf{z_1}) + a_2b_2c_2f(\mathbf{x_2}, \mathbf{y_2}, \mathbf{z_2}).$$

Now we observe that $\mathbf{x} = a_1\mathbf{x_1} + a_2\mathbf{x_2}$. Since $\mathbf{x_1}$ and $\mathbf{x_2}$ are linearly independent, we can invert the transformation and get that $a_1 = L_1(\mathbf{x})$ and $a_2 = L_1'(\mathbf{x})$, say, where L_1 and L_1' are linear forms with coefficients in $\mathbb{Q}$, depending on $\mathbf{x_1}$ and $\mathbf{x_2}$. We find similar expressions for b_1, b_2 and c_1, c_2 to deduce that

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = L_1(\mathbf{x})L_2(\mathbf{y})L_3(\mathbf{z}) + L_1'(\mathbf{x})L_2'(\mathbf{y})L_3'(\mathbf{z}).$$

From this expression we can see directly that if f has a singular point (X, Y, Z) then it must have a linear factor, without loss of generality, $L(\mathbf{x})$, say. This linear factor must vanish at a point $\mathbf{p} \in \mathbb{P}$. We would then have for all $\mathbf{y}, \mathbf{z} \in \mathbb{P}$ that

$$0 = f(\mathbf{p}, \mathbf{y}, \mathbf{z}) = \mathbf{y}^T M_{yz}(\mathbf{p})\mathbf{z}.$$

This then gives that $M_{yz}(\mathbf{p}) = 0$ which implies as above that $D = 0$.

i) $\Rightarrow$ ii) Conversely, assume that $D = 0$. By Lemma 27, $\Delta_{xy}(\mathbf{z}) = cL(\mathbf{z})^2$. We first consider the case when $c = 0$. In this case f factorizes by Lemma 28. We

assume without loss of generality that f splits as in (4.1). But in this case the gradient of f is zero when $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ is picked such that $L(\mathbf{y})$ and $B(\mathbf{x}, \mathbf{z})$ simultaneously vanish. By this argument, we may assume that neither of the three determinants $\Delta_{xy}(\mathbf{z})$, $\Delta_{yz}(\mathbf{x})$, or $\Delta_{zx}(\mathbf{y})$ vanishes identically. Next, we pick a primitive $\mathbf{z}$ such that $\Delta_{xy}(\mathbf{z}) = 0$. Similarly, we pick primitive $\mathbf{x}$ and $\mathbf{y}$ such that $\Delta_{yz}(\mathbf{x}) = 0$ and $\Delta_{zx}(\mathbf{y}) = 0$. This implies that there are primitive vectors $\mathbf{x_1}$, $\mathbf{x_2}$, $\mathbf{y_1}$, $\mathbf{y_2}$, and $\mathbf{z_1}$, $\mathbf{z_2}$ such that

$$\begin{aligned}
\mathbf{x_1}^T M_{xy}(\mathbf{z}) &= M_{xy}(\mathbf{z})\mathbf{y_1} = 0, \\
\mathbf{y_2}^T M_{yz}(\mathbf{x}) &= M_{yz}(\mathbf{x})\mathbf{z_1} = 0, \\
\mathbf{z_2}^T M_{zx}(\mathbf{y}) &= M_{zx}(\mathbf{y})\mathbf{x_2} = 0.
\end{aligned}$$

Note that $\mathbf{x_1}^T M_{xy}(\mathbf{z}) = \mathbf{z}^T M_{zy}(\mathbf{x_1}) = 0$. Thus, $\Delta_{yz}(\mathbf{x_1}) = 0$. We recall that the discriminant Δ_{yz} is $D = 0$ and that Δ_{yz} does not vanish identically. Therefore, $\mathbf{x_1} = \mathbf{x}$. By using the same idea, we can show

$$\mathbf{x_1} = \mathbf{x_2} = \mathbf{x}, \quad \mathbf{y_1} = \mathbf{y_2} = \mathbf{y}, \quad \mathbf{z_1} = \mathbf{z_2} = \mathbf{z},$$

which proves that all partial derivatives of f are simultaneously zero at the non-trivial point $(\mathbf{x}, \mathbf{y}, \mathbf{z})$.

ii) $\Leftrightarrow$ iii) The fact that ii) $\Rightarrow$ iii) follows from Euler's theorem for homogeneous polynomials. It states in particular that for a homogeneous function $g(x_1, \ldots, x_d)$ of order n:

$$\sum_{i=1}^{d} x_i \frac{\partial g}{\partial x_i} = n g(\mathbf{x}).$$

In our case, we may apply this result with $g = f$, $d = 6$ and $n = 3$. It is then clear that ii) $\Rightarrow$ iii). The converse is trivial.

□

Let $X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be real numbers ≥ 1. Our goal is to find an upper bound for the quantity

$$\mathcal{N}'(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \#\{(\mathbf{x}, \mathbf{y}, \mathbf{z}) : |x_i| \leq X_i, |y_i| \leq Y_i, |z_i| \leq Z_i, \\ (x_1, x_2) = (y_1, y_2) = (z_1, z_2) = 1, f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = 0\}.$$

By Theorem 23, it suffices to study the case when f is irreducible. We note that if f factorizes then $D = 0$ but the converse may not necessarily be true as the family of examples

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = y_1 x_1 z_1 a_{111} + y_1 x_2 z_1 a_{211} + y_1 x_2 z_2 + y_2 x_2 z_1$$

shows. Here, $D = 0$ but f is irreducible if $a_{111} \neq 0$. Let

$$s = s(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \Delta_{xy}(\mathbf{z}) \Delta_{yz}(\mathbf{x}) \Delta_{zx}(\mathbf{y}).$$

It turns out that the number of points counted by $\mathcal{N}'$ for which $s = 0$ may be large, even if $D \neq 0$. For example, consider

$$f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = y_1 x_1 z_1 a_{111} + y_1 x_2 z_2 + y_2 x_2 z_1 + y_2 x_2 z_2$$

for $a_{111} \neq 0$. Then, f is irreducible, $D = a_{111}^2 \neq 0$ and

$$s(\mathbf{x}, \mathbf{y}, \mathbf{z}) = a_{111}^2 x_2 y_1 z_1 \left(z_1 + z_2\right) \left(y_1 + y_2\right) \left(a_{111} x_1 - x_2\right).$$

Furthermore, it is easy to see that the number of points contributing to $\mathcal{N}'$ for which $s = 0$ is $\gg X_1 X_2 + Y_1 Y_2 + Z_1 Z_2$. Lemma 33 shows that this is in general also the best upper bound. We therefore exclude points for which $s = 0$ in the remaining argument.

We now state the main theorem of this section:

Theorem 30. *Let $A = (a_{ijk})$ be a $2 \times 2 \times 2$ hypermatrix with associated trilinear form $f = f_A$ and hyperdeterminant $D := \det(A)$. We assume that f is irreducible over $\mathbb{Z}$ and that $D \neq 0$. Let $X_1, X_2, Y_1, Y_2, Z_1, Z_2$ be real numbers ≥ 1 and define*

$$\mathcal{N}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) = \#\{(\mathbf{x}, \mathbf{y}, \mathbf{z}) : |x_i| \leq X_i, |y_i| \leq Y_i, |z_i| \leq Z_i, \\ (x_1, x_2) = (y_1, y_2) = (z_1, z_2) = 1, f(\mathbf{x}, \mathbf{y}, \mathbf{z}) = 0, s(\mathbf{x}, \mathbf{y}, \mathbf{z}) \neq 0\}.$$

Let $T = \|f\| X_1 X_2 Y_1 Y_2 Z_1 Z_2$. Then

$$\mathcal{N}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) \ll T^{\epsilon} \left(\frac{\sqrt{X_1 X_2 Y_1 Y_2 Z_1 Z_2}}{D^{1/4}} + \sqrt{X_1 X_2 Y_1 Y_2} + Z_1 Z_2 \right).$$

We note in particular, that the condition $D \geq 1$ yields the estimate

$$\mathcal{N}(\mathbf{X}, \mathbf{Y}, \mathbf{Z}) \ll T^{\epsilon} \sqrt{X_1 X_2 Y_1 Y_2 Z_1 Z_2}.$$

This can easily be obtained by permuting $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ in the theorem and then taking the minimum of the resulting estimates.

We define for any primitive vector $\mathbf{z}$:

$$f_{\mathbf{z}}(\mathbf{x}, \mathbf{y}) := f(\mathbf{x}, \mathbf{y}, \mathbf{z}).$$

With this notation, we think of $f_{\mathbf{z}}$ as a bilinear form in the variables $\mathbf{x}, \mathbf{y}$. Let the coefficients of $f_{\mathbf{z}}$ be the linear forms $L_z^{(i)} = L_z^{(i)}(\mathbf{z})$, where $i = 1, \ldots, 4$. We may think of $L_z^{(i)}$ as a 1×2 row vector, the elements of $L_z^{(i)}$ being the coefficients of the form $L_z^{(i)}(\mathbf{z})$. Let $i, j \in \{1, \ldots, 4\}$. We consider a 2×2 matrix which has $L_z^{(i)}$ as its first row and $L_z^{(j)}$ as its second row. Let $D_z^{(i,j)}$ be the absolute value of the determinant of this matrix. We define analogously $f_{\mathbf{y}}, L_y^{(i)}, D_y^{(i,j)}$ and $f_{\mathbf{x}}, L_x^{(i)}, D_x^{(i,j)}$.

Lemma 31. *Let q be a non-zero integer. Assume that there exists a primitive vector $\mathbf{z}$ such that $q \mid L_z^{(i)}(\mathbf{z})$ for all i. Then $q^2 \mid D$.*

Proof. Let

$$g_z = \gcd_{i,j} D_z^{(i,j)}.$$

Our first aim is to prove that $q \mid g_z$. We fix i and j and want to show that $q \mid D_z^{(i,j)}$. If $D_z^{(i,j)} = 0$ then we are done. Thus, we assume that $D_z^{(i,j)} \neq 0$. Let $L_z^{(i)}(\mathbf{z}) = az_1 + bz_2$ and $L_z^{(j)}(\mathbf{z}) = cz_1 + dz_2$ so that $D_z^{(i,j)} = ad - bc$. There exists integers k_1 and k_2 such that

$$az_1 + bz_2 = k_1 q \quad \text{and} \quad cz_1 + dz_2 = k_2 q.$$

So that

$$(bc - ad)z_2 = q(ck_1 - ak_2),$$
$$(bc - ad)z_1 = -q(dk_1 - bk_2)$$

We observe that $q \mid (bc - ad)z_1$ and that $q \mid (bc - ad)z_2$. Since z_1 and z_2 are coprime, we therefore get that $q \mid (ad - bc)(z_1, z_2) = ad - bc$. This proves that $q \mid D_z^{(i,j)}$ and since i and j were arbitrary, we may deduce that $q \mid g_z$. It can be shown by direct calculations that g_z is the greatest common factor of the following six 2x2 determinants:

$$a_{111}a_{122} - a_{112}a_{121}, \qquad a_{111}a_{212} - a_{112}a_{211}, \qquad a_{111}a_{222} - a_{112}a_{221},$$
$$a_{212}a_{121} - a_{211}a_{122}, \qquad a_{121}a_{222} - a_{122}a_{221}, \qquad a_{211}a_{222} - a_{212}a_{221}$$

From this it follows at once that $q^2 \mid D$. □

Lemma 32. *Assume that there exists a primitive vector* $\mathbf{z}$ *such that* $L_z^{(i)}(\mathbf{z}) = 0$ *for all* i*. Then* f *factorizes or vanishes identically.*

Proof. Let $L_z^{(i)}(\mathbf{z}) = a_i z_1 + b_i z_2$ $(i = 1, \ldots, 4)$, say and define $a_i' = a_i/(a_i, b_i)$ and

$b_i' = b_i/(a_i, b_i)$ in the case when $(a_i, b_i) \neq 0$. We recall that z_1 and z_2 are co-prime. We assume that all $L_z^{(i)}$ vanish simultaneously for the same $\mathbf{z}$. If $z_1 = 0$ then $z_2 = \pm 1$ and therefore $b_i' = 0$ and $a_i' = \pm 1$ for all i. This implies that $b_i = 0$ for all i, which means that f has a linear factor z_1 and the conclusion in the lemma is valid. Thus we may assume that $z_1 \neq 0$ and similarly $z_2 \neq 0$. If $z_1 z_2 \neq 0$ and $L_z^{(i)}(\mathbf{z}) = 0$ then either $a_i = b_i = 0$ or $\mathbf{z} = \pm(b_i', -a_i')$. This implies that either all $L_z^{(i)}$ are identically 0 or that all the $L_z^{(i)}$ are pairwise proportional. In the first case, f vanishes identically and in the second case, f has a linear factor. This proves the lemma. □

Lemma 33. *Assuming that f is irreducible over $\mathbb{Z}$, the number of points $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ counted by $\mathcal{N}$ for which $\Delta_{xy}(\mathbf{z}) = 0$ is $O(X_1X_2 + Y_1Y_2)$.*

Proof. We first note that Δ_{xy} cannot vanish identically by Lemma 28. Thus, there are $O(1)$ choices for $\mathbf{z}$. We fix one such $\mathbf{z}$ and consider the equation $f_{\mathbf{z}}(\mathbf{x}, \mathbf{y}) = 0$ as a bilinear equation with coefficients $L_z^{(i)}(\mathbf{z}) = a_i z_1 + b_i z_2$ $(i = 1, \dots, 8)$, say. By Lemma 32, the function $f_{\mathbf{z}}(\mathbf{x}, \mathbf{y})$ cannot vanish identically. The equation $f_{\mathbf{z}}(\mathbf{x}, \mathbf{y}) = 0$ is therefore saying that a non-zero bilinear form vanishes. This bilinear form will factorize as a product of linear forms $f_{\mathbf{z}}(\mathbf{x}, \mathbf{y}) = L_{1,\mathbf{z}}(\mathbf{x})L_{2,\mathbf{z}}(\mathbf{y})$ because $\Delta_{xy}(\mathbf{z}) = 0$. It is clear that the equation $L_{1,\mathbf{z}}(\mathbf{x})L_{2,\mathbf{z}}(\mathbf{y}) = 0$ has $\ll X_1X_2 + Y_1Y_2$ solutions. □

Fix a primitive integer vector $\mathbf{z}$. We want to apply Theorem 23 for bilinear equations to $f_{\mathbf{z}}$. By assumption, $\Delta(f_{\mathbf{z}}) \neq 0$. If there exists an integer q dividing all $L_z^{(i)}$ then $q^2 \mid D$ by Lemma 31. Let $L_i' = L_z^{(i)}/q$. We divide the equation $f_{\mathbf{z}}(\mathbf{x}, \mathbf{y}) = 0$ by q so that we get $f'(\mathbf{x}, \mathbf{y}) = 0$, where f' is a bilinear form with coprime coefficients and non-zero determinant $\Delta(f') = \Delta_{xy}(\mathbf{z})/q^2$. Thus, we may deduce that:

$$\mathcal{N} \ll \sum_{q^2 \mid D} \sum_{\substack{\mathbf{z}:|z_i| \leq Z_i \\ (z_1,z_2)=1 \\ q \mid L_z^{(j)}(\mathbf{z}) \\ |\Delta_{xy}(\mathbf{z})| \geq 1}} \mathrm{d}(\Delta_{xy}(\mathbf{z})) \left(\frac{q\sqrt{X_1X_2Y_1Y_2}}{\sqrt{|\Delta_{xy}(\mathbf{z})|}} + 1 \right).$$

Next, we process the condition that $q \mid L_z^{(j)}(\mathbf{z})$ for all j. Let C be the 4×2 matrix having the $L_z^{(j)}$ as rows. Since f is irreducible, there exists no prime p that divides all elements of C. Since $q \mid L_z^{(j)}(\mathbf{z})$, we have as in the proof of of Lemma 31 that q divides all 2x2 minors of C. Therefore, we may apply Lemma 24 and deduce that the elements $\mathbf{z}$ counted by the above inner sum are in a lattice Λ_q of determinant q. We further observe that the points $\mathbf{z}$ counted by the inner sum are also in the ellipse $E(Z_1, Z_2)$ given by $(z_1/Z_1)^2 + (z_2/Z_2)^2 \ll 1$. This ellipse has area $A(E(Z_1, Z_2)) \asymp Z_1 Z_2$. By Lemma 25, there exists a basis $\mathbf{b}_1$, $\mathbf{b}_2$ of the lattice Λ_q and a positive number α such that if we write $\mathbf{z} \in E(Z_1, Z_2)$ as $\mathbf{z} = G\mathbf{z}'$ then $|z_1'| \leq \alpha$ and $|z_2'| \ll Z_1 Z_2/(\alpha q)$. Here, G is a 2×2 matrix with columns $\mathbf{b}_1$ and $\mathbf{b}_2$. Note that Δ_{xy} is a quadratic form of discriminant D and thus, the discriminant of the new quadratic form $\Delta'_{xy}(\mathbf{z}') = \Delta_{xy}(G\mathbf{z}')$ is $q^2 D$. We further note that if $\Delta'_{xy}(\mathbf{z}') = 0$ then $\Delta_{xy}(\mathbf{z}) = 0$, and thus it is safe to assume that $|\Delta'_{xy}(\mathbf{z}')| \geq 1$. By following the proof of Lemma 25, we can see that

$$\|\Delta'_{xy}\| \ll \|\Delta_{xy}\| P(D, Z_1, Z_2),$$

where $P(D, Z_1, Z_2)$ is a finite power of DZ_1Z_2. Thus, after a change of variables $\mathbf{z} = G_q \mathbf{z}'$ for each q, we arrive at the estimate

$$\mathcal{N} \ll \sum_{q^2 \mid D} \sum_{\substack{\mathbf{z}' : |z_i'| \leq Z_i' \\ (z_1', z_2') = 1 \\ |\Delta'_{xy}(\mathbf{z}')| \geq 1}} d(\Delta'_{xy}(\mathbf{z}')) \left(\frac{q\sqrt{X_1 X_2 Y_1 Y_2}}{\sqrt{|\Delta'_{xy}(\mathbf{z}')|}} + 1 \right),$$

where $Z_1' Z_2' \ll Z_1 Z_2/q$. If $Z_1' < 1$ then $z_1' = 0$ and $z_2' = \pm 1$. A similar argument holds if $Z_2' < 1$. Thus, we note that

$$1 \leq |\Delta'_{xy}(\mathbf{z}')| \ll \|\Delta_{xy}\| P(D, Z_1, Z_2),$$

where again $P(D, Z_1, Z_2)$ denotes some finite power of DZ_1Z_2. We may therefore

deduce the trivial estimate

$$\sum_{q^2|D} \sum_{\substack{\mathbf{z}':|z_i'|\le Z_i' \\ (z_1',z_2')=1 \\ |\Delta_{xy}'(\mathbf{z}')|\ge 1}} d(\Delta_{xy}'(\mathbf{z}')) \ll T^\epsilon Z_1 Z_2$$

and it remains to find an upper bound for the remaining sum. Thus, we may split the sum over $\mathbf{z}'$ into dyadic ranges for $|\Delta_{xy}'(\mathbf{z}')|$. In particular, there exists an integer R such that $1 \le R \ll \|\Delta_{xy}\| P(D, Z_1, Z_2)$ and

$$\mathcal{N} \ll T^\epsilon \sqrt{X_1 X_2 Y_1 Y_2} \sum_{q^2|D} q \sum_{\substack{\mathbf{z}':|z_i'|\le Z_i' \\ (z_1',z_2')=1 \\ R\le|\Delta_{xy}'(\mathbf{z}')|<2R}} \frac{1}{\sqrt{|\Delta_{xy}'(\mathbf{z}')|}} + T^\epsilon Z_1 Z_2.$$

We proceed to attack the inner sum. For $q, n > 0$ with $q^2 \mid D$, let

$$a_{n,q} := \#\left\{\mathbf{z}' \in \mathbb{Z}^2 : |z_i'| \le Z_i', (z_1', z_2') = 1, |\Delta_{xy}'(\mathbf{z}')| = n\right\}.$$

Then

$$\mathcal{N} \ll T^\epsilon \sqrt{X_1 X_2 Y_1 Y_2} \sum_{q^2|D} q S_q(R) + T^\epsilon Z_1 Z_2,$$

where

$$S_q(R) = \sum_{R\le n<2R} \frac{a_{n,q}}{\sqrt{n}}.$$

We now need to find an upper bound for $S_q(R)$. For $t \ge 1$, let

$$A_q(t) := \sum_{1\le m<t} a_{m,q}.$$

By partial summation, we obtain

$$S_q(R) \ll \frac{A_q(2R)}{\sqrt{R}} + \frac{A_q(R)}{\sqrt{R}} + \int_R^{2R} \frac{A_q(t)}{t^{3/2}}\, dt.$$

It remains to find an upper bound for $A_q(t)$. We prove the following lemma:

Lemma 34. *The following upper bound holds:*

$$A_q(t) \ll \min\left\{\frac{Z_1 Z_2}{q} + 1, \left(\frac{t}{qD^{1/2}} + 1\right)(Tt)^{\epsilon}\right\}$$

Proof. Note that

$$A_q(t) = \#\left\{\mathbf{z} \in \mathbb{Z}^2 : |z_i| \leq Z_i', (z_1, z_2) = 1, 1 \leq |\Delta_{xy}'(\mathbf{z})| \leq t\right\},$$

where we recall that Z_1' and Z_2' are positive numbers such that $Z_1'Z_2' \ll Z_1Z_2/q$ and Δ_{xy}' is a quadratic form with integer coefficients such that $D(\Delta_{xy}') = q^2D$. If $Z_1' < 1$ then $z_1 = 0$ and $z_2 = \pm 1$. Thus, the case when $Z_1' < 1$ or $Z_2' < 1$ contributes $O(1)$ to $A_q(t)$. If $Z_1' \geq 1$ and $Z_2' \geq 1$ then

$$A_q(t) \ll (Z_1' + 1)(Z_2' + 1) \ll \frac{Z_1 Z_2}{q} + 1.$$

This proves the first bound. Next, let us consider the case when

$$\Delta_{xy}'(\mathbf{z}) = \alpha(z_1 - \beta_1 z_2)(z_1 - \beta_2 z_2) = \alpha L_1(\mathbf{z})L_2(\mathbf{z}),$$

say, for some $\alpha \in \mathbb{Z} \setminus \{0\}$ and $\beta_i \in \mathbb{C}$. Note that in general $D(\Delta_{xy}') = |\alpha|^2|\beta_1 - \beta_2|^2$. Such a factorization exists if and only if the coefficient of z_1^2 in Δ' is non-zero. We first consider the case when $\beta_1 = \beta_2$. In this case we can deduce that $q^2D = D(\Delta_{xy}') = 0$, which is impossible since $D \neq 0$.

Next consider the case when $\beta_1 = \bar{\beta_2} = a + bi$, with $a, b \in \mathbb{R}$ and $b \neq 0$. Then

$$|\Delta_{xy}'(\mathbf{z})| = |\alpha|((x - ay)^2 + (by)^2).$$

We set $r = x - ay$ and $s = by$. Then the point (r, s) is inside a real lattice Λ given by the matrix

$$\begin{pmatrix} 1 & -a \\ 0 & b \end{pmatrix}.$$

We note that $\det(\Lambda) = |b|$ and that the point (r, s) also lies in the circle given by

$$r^2 + s^2 \leq t/|\alpha|.$$

This circle has area $\pi t/|\alpha|$. Thus, by Lemma 25, the number of possibilities for (r, s) is

$$\ll \frac{t}{|\alpha||b|} + 1 \ll \frac{t}{qD^{1/2}} + 1,$$

where in the last line we used that $q^2 D = D(\Delta'_{xy}) = 4b^2\alpha^2$. Each choice of (r, s) gives at most one choice for $\mathbf{z}$ since $b \neq 0$.

We may therefore assume that β_1 and β_2 are real. By the solution formula for quadratic polynomials, we observe that $\beta_i \ll \|\Delta'\|/|\alpha|$ and therefore, $\alpha L_i(\mathbf{z}) \ll \|\Delta'\|Z$, where $Z = \max\{Z'_1, Z'_2\}$. Since $1 \leq |\Delta'_{xy}(\mathbf{z}')|$, we also note that $|L_i(\mathbf{z})| \gg 1/(\|\Delta'\|Z)$. We therefore conclude that

$$\frac{1}{\|\Delta'\|Z} \ll |L_i(\mathbf{z})| \ll \|\Delta'\|Z.$$

We proceed by splitting the ranges of $L_1(\mathbf{z})$ and $L_2(\mathbf{z})$ into dyadic ranges so that

$$K \leq |L_1(\mathbf{z})| < 2K \text{ and } L \leq |L_2(\mathbf{z})| < 2L$$

for some integers K and L. The dyadic subdivision comes at the cost of a factor $(\|\Delta_{xy}\|DZ_1Z_2t)^\epsilon$ in the estimate for $A_q(t)$ By setting $r = L_1(\mathbf{z})$ and $s = L_2(\mathbf{z})$ we can again see that the points (r, s) are in a real lattice Λ with $|\det(\Lambda)| = |\beta_1 - \beta_2|$ and

they are in an ellipse of shape

$$(r/K)^2 + (s/L)^2 \ll 1$$

and area $\ll KL \ll \frac{t}{|\alpha|}$. And thus, we obtain once again by Lemma 25 that the number of possibilities for the points (r, s) is

$$\ll (\|\Delta_{xy}\| D Z_1 Z_2 t)^{\epsilon} (t/(qD^{1/2}) + 1).$$

The linear transformation defining (r, s) is invertible because $\beta_1 \neq \beta_2$. Thus, for each choice (r, s) there is again at most one possible value for $\mathbf{z}$. This finishes the proof of the lemma if the coefficient of z_1^2 in Δ' is non-zero. The case when the coefficient of z_2^2 is non-zero is similar.

Therefore, we may now concentrate on the last case when $\Delta'_{xy}(\mathbf{z}) = bz_1z_2$ for some integer $b \neq 0$. We recall that $D(\Delta'_{xy}) = q^2D = b^2$. In particular, $b = qD^{1/2}$. We observe that

$$A_q(t) \ll \#\left\{\mathbf{z} \in \mathbb{Z}^2 : 1 \leq |bz_1z_2| \leq t\right\} \ll t^{\epsilon}\left(\frac{t}{b} + 1\right) \ll t^{\epsilon}\left(\frac{t}{qD^{1/2}} + 1\right).$$

□

We note that $q < \sqrt{R}$ because $q^2 \mid \Delta_{xy} \ll R$. This gives

$$S_q(R) \ll (TR)^{\epsilon}\left(\frac{1}{q}\min\left\{\frac{Z_1Z_2}{\sqrt{R}}, \frac{\sqrt{R}}{D^{1/2}}\right\} + \frac{1}{\sqrt{R}}\right) \ll \frac{T^{\epsilon}}{q}\left(\frac{\sqrt{Z_1Z_2}}{D^{1/4}} + 1\right),$$

where the critical value is obtained when $R = Z_1Z_2D^{1/2}$. This proves the theorem.

Chapter 5

Counting Monomials for Cubic Varieties

5.1 Introduction

Let $F(x_1, x_2, x_3, x_4)$ be an irreducible form of degree 3 in 4 variables. We are interested in an upper bound for

$$N(F, B) = \#\left\{\mathbf{x} \in \mathbb{Z}^4, (x_1, x_2, x_3, x_4) = 1, |x_i| \leq B, F(\mathbf{x}) = 0\right\}.$$

Using a generalization of Heath-Brown's p-adic determinant method, Salberger [40] has shown that

$$N(F, B) \ll_\epsilon B^{12/7+\epsilon},$$

provided F is smooth. Heath-Brown's method shows that the points counted by $N(F, B)$ must lie on one of $k \ll_\epsilon B^{\sqrt{3}+\epsilon}$ auxiliary varieties (see Theorem 1). Our aim is to improve the bound in Theorem 1 by proving that

Theorem 35. *In the case $n = 4$ and $d = 3$ we can replace the bound on k in Theorem 1 by $k \ll_\epsilon B^{12/7+\epsilon}$.*

Our method generalizes to any $n \geq 3$ but given the technical complexity, we restrict ourselves to the case when $n = 3$. We note that $\sqrt{3} \approx 1.73$ and that $12/7 \approx 1.71$.

We follow a variant of the p-adic determinant method by Heath-Brown [18]. Our argument seems to be similar to parts of the argument in Ellenberg and Venkatesh [12]. We only sketch our argument in the parts where it is similar to Heath-Brown's approach. Let $p \asymp P$ be a suitably large prime. Let $\mathbf{t} \in \mathbb{F}_p^4$ be a projective representative for the non-singular points of $F(\mathbf{t}) = 0$ over $\mathbb{F}_p$. We consider points $\mathbf{x} \in \mathbb{Z}^4$ such that such that $F(\mathbf{x}) = 0$ and $\mathbf{x} \equiv \lambda \mathbf{t} \pmod{p}$ for some $\lambda \in \mathbb{Z}$ and such that $|x_i| \leq B$ for all i. We assume without loss of generality that $t_1 = 1$. Furthermore, we only consider points $\mathbf{x}$ with $p \nmid \nabla F(\mathbf{x})$. Following Heath-Brown's notation, we define $S_p(\mathbf{t})$ to be the set consisting of all these points $\mathbf{x}$.

As in Heath-Brown's argument, we can then use Hensel's Lemma to lift $\mathbf{t}$ to a p-adic solution $\mathbf{u} \in \mathbb{Z}_p^4$ of $F(\mathbf{u}) = 0$ such that $u_1 = 1$. Let $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(J)}$ be the (distinct) elements of $S_p(\mathbf{t})$ and let A be a suitably large positive integer. Let $m_1(\mathbf{x}), \ldots, m_{H(A)}(\mathbf{x})$ be the list of monomials

$$x_1^{e_1} x_2^{e_2} x_3^{e_3} x_4^{e_4}, \qquad \sum_i e_i = A,$$

where

$$H := H(A) = \frac{1}{6}(A+1)(A+2)(A+3).$$

Let $\mathcal{M}$ be the $J \times H$ matrix with (i,j)-th entry $m_j(\mathbf{x}^{(i)})$. We then use a version of the Implicit Function Theorem as in Heath-Brown so that we can assume that all $\mathbf{x}^j$ belong to the same projective class as $\mathbf{u}$ modulo p. That is, we can write $\mathbf{x}^{(j)}$ as $\mathbf{u} + \mathbf{y}^{(j)}$, where $\mathbf{y}^{(j)} \in p\mathbb{Z}_p^4$.

Let $\mathbb{Q}_d[\mathbf{x}]$ denote the set of forms of degree d with rational coefficients in the variables

$\mathbf{x}$. Define the vector spaces

$$V = \mathrm{Ker}(\mathcal{M}) = \{\mathbf{c} \in \mathbb{Q}^H : \mathcal{M}\mathbf{v} = \mathbf{0}\}$$

and

$$V_1 = \{\mathbf{c} \in \mathbb{Q}_A[\mathbf{x}] : c(\mathbf{x}) = F(\mathbf{x})g(\mathbf{x}) \text{ for some } g(\mathbf{x}) \in \mathbb{Q}_{A-3}[x]\}.$$

Our aim is now to construct an auxiliary equation $F_p(\mathbf{x}; \mathbf{t})$ which is not a multiple of F such that $F_p(\mathbf{x}^{(i)}; \mathbf{t}) = 0$ for all i. This is equivalent to finding a non-zero vector which is in V but the corresponding form is not in V_1. Such a vector exists if $\dim V > \dim V_1$, which is the same as

$$\mathrm{rank}(\mathcal{M}) < H - H_1,$$

where $H_1 = \dim(V_1) = H(A-3)$. We will now consider the matrix $\mathcal{M}$ and show that we can perform column operations so that the last $H(A-3)$ rows of $\mathcal{M}$ are zero. We then delete the zero columns and consider the determinant Δ of the remaining matrix We then proceed with the usual p-adic methods to show that $\Delta = 0$ by showing that $\|\Delta\|_p$ is large.

5.2 Linear Changes

We write F as

$$F(X_1, X_2, X_3, X_4) = f_0 X_1^3 + f_1 X_1^2 + f_2 X_1 + f_3,$$

where the f_i are forms of degree i in the variables X_2, X_3, X_4. We may assume that $S_p(\mathbf{t}) \neq \emptyset$ and thus, by performing a linear change of variables (over $\mathbb{Z}_p$), we may assume without loss of generality that $f_0 = 0$. By performing a further linear change

of variables, we may assume that the non-singular point $\mathbf{u}$ is the point $(1,0,0,0)$. Note that

$$\nabla F(1,0,0,0) = \left(0, \frac{\partial f_1}{\partial x_2}, \frac{\partial f_1}{\partial x_3}, \frac{\partial f_1}{\partial x_4}\right)$$

and $p \nmid \nabla F(1,0,0,0)$. Thus, the linear form f_1 does not vanish identically modulo p. We therefore make the invertible (over $\mathbb{Z}_p$) linear change $Y_2 = f_1(X_2, X_3, X_4)$ and $Y_i = X_i$ for all $i \neq 2$. Hence,

$$F(Y_1, Y_2, Y_3, Y_4) = Y_2 Y_1^2 + f_2' Y_1 + f_3',$$

where the f_i' are forms of degree i in the variables Y_2, Y_3, Y_4. Next, we perform a further $\mathbb{Z}_p$-linear change of variables as follows: Let $Y_1 = Z_1 + l(Z_3, Z_4)$ and $Z_i = Y_i$ for all $i \neq 1$. Then,

$$F(Z_1, Z_2, Z_3, Z_4) = Z_2 Z_1^2 + q(Z_2, Z_3, Z_4) Z_1 + c(Z_2, Z_3, Z_4),$$

where $q = 2lZ_2 + f_2'$ is a quadratic form and $c = f_3' + l^2 Z_2 + l f_2'$ is a cubic form, the coefficients being in $\mathbb{Z}_p$. We note that

$$c(0, Z_3, Z_4) = f_3'(0, Z_3, Z_4) + l(Z_3, Z_4) f_2'(0, Z_3, Z_4),$$

and

$$q(0, Z_3, Z_4) = f_2'(0, Z_3, Z_4).$$

We have thus transformed F to the following equation

$$r = Q(r, s, t) + C(r, s, t),$$

where $r = z_2/z_1$, $s = z_3/z_1$ and $t = z_4/z_1$ with $p \nmid z_1$, say. We can further see that if $Q(0, s, t)$ does not vanish identically then we can pick l such that $p \nmid C(0, s, t)$,

say. By performing a further linear change in s, t we can then assume without loss of generality that $p \nmid C(0, 1, 0)$.

5.3 Notation

1. We will work with multisets of polynomials in our proof. Informally, a multiset is a set where elements can occur multiple times, but the order of the elements is irrelevant. We denote the cardinality of a multiset $\mathcal{L}$ by $|\mathcal{L}|$. For example, $|\{1, 1, 2, 2, 3\}| = 5$. We also use the union of two multisets in the obvious way. For example, $\{1, 2, 3\} \cup \{1, 1\} = \{1, 2, 3, 1, 1\}$.

2. We define the (weighted) degree of a monomial $m = r^a s^b t^c$ by $\delta(m) = 2a+b+c$. We define the lowest degree of a polynomial p in r, s, t to be

$$\delta(p) = \min_m \delta(m),$$

   where the minimum ranges over all monomials m occurring in p with non-zero coefficient. If $\mathcal{L}$ is a multiset of polynomials then

$$\nu_p(\mathcal{L}) = \sum_{p \in \mathcal{L}} \delta(p).$$

3. Let $P(r, s, t)$ be a polynomial in r, s, t The notation PM_k denotes the list containing $(k + 1)$ polynomials $Ps^k, Ps^{k-1}t, \ldots Pt^k$. We use this notation when we want to make a statement about all the expressions in PM_k at once. Here M_k can be seen as the list of monomials of degree k in s, t. Note that M_k is always independent of r, whereas m_k which will denote one particular monomial may depend on r.

4. The notation $PM_k^{(m)}$ denotes a subset of PM_k of size m, that is m (distinct)

elements of PM_k but we don't care what they are (though they can always be determined explicitly in our algorithm).

5. Let $\mathcal{G}$ be a list of polynomials in r, s, t. We write $\langle \mathcal{G} \rangle$ to denote all the $\mathbb{Z}_p$-linear combinations of polynomials in $\mathcal{G}$ and for a polynomial p we write $p \in \langle \mathcal{G} \rangle$ if p can be written as a $\mathbb{Z}_p$-linear combination of elements in $\mathcal{G}$.

6. We will not distinguish between a polynomial $p(r, s, t)$ and the column of the matrix corresponding to it. Let $\mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ be multisets of polynomials such that $|\mathcal{G}_1| = |\mathcal{G}_2|$. By the notation $\mathcal{G}_1 \equiv \mathcal{G}_2 \pmod{\mathcal{G}_3}$ we mean that by adding linear combinations of columns corresponding to the elements of $\mathcal{G}_3$ to the columns corresponding to elements of $\mathcal{G}_1$, we can transform the columns corresponding to $\mathcal{G}_1$ to the columns corresponding to $\mathcal{G}_2$. This notation helps to keep track of what columns are needed in each step for the column operations.

5.4 Eliminating zero Columns

As explained above we now assume that our matrix $\mathcal{M}$ has entries in the rational variables r, s, t and that $p \mid r, s, t$. Furthermore, the following equation holds:

$$r = Q(r, s, t) + C(r, s, t),$$

and the columns of $\mathcal{M}$ correspond to the monomials

$$r^a s^b t^c, a + b + c \leq A,$$

where A is for simplicity of calculations an even integer, $A = 2A_1$, say. Our target now is to show that $\nu_p(\Delta)$ is large. More precisely, we want to show that

$$\nu_p(\Delta) \geq \frac{7}{4}A^3 + O(A^2). \tag{5.1}$$

We write the cubic form C as

$$C = C_3 + C_2 r + C_1 r^2 + C_0 r^3$$

and the quadratic form Q as

$$Q = Q_2 + Q_1 r + Q_0,$$

such that C_i and Q_i are forms of degree i, only depending on s and t. In particular, C_0 and Q_0 are constants. We recall that $H(A)$ is the number of columns of $\mathcal{M}$. As a first step, want to show that after performing column operations,

$$H(A-3) = \frac{1}{6}(A-2)(A-1)A$$

columns of the matrix are zero. Let $\mathcal{L}_1$ be the multiset of monomials

$$\begin{aligned} s^a t^b, &\qquad a+b \leq A \\ r^a s^b t^c, &\qquad a+b+c \in \{A, A-1\}, a \geq 1. \end{aligned}$$

and let $\mathcal{L}_0$ be the multiset of monomials

$$r^{a+1} s^b t^c, a+b+c \leq A-3, a \geq 0.$$

Note that $\mathcal{L}_0$ and $\mathcal{L}_1$ together contain exactly the monomials we started with. We will now prove that the monomials in $\mathcal{L}_0$ can we written as linear combinations of monomials in $\mathcal{L}_1$, and therefore all monomials in $\mathcal{L}_0$ can be transformed by column operations to zero columns, while the columns corresponding to $\mathcal{L}_1$ stay unchanged. Note that $|\mathcal{L}_0| = H(A-3)$, which is what we wanted. We prove the following claim by induction:

Lemma 36. *For $k = 1, 2, \ldots, A$, all monomials of the form rm_{A-k} are in $\langle \mathcal{L}_1 \rangle$.*

Proof. If $k = 1, 2$ then $rm_{A-k} \in \mathcal{L}_1$ and hence in particular $rm_{A-k} \in \langle \mathcal{L}_1 \rangle$. Now assume $k \geq 3$ and that $rm_{A-k+1} \in \langle \mathcal{L}_1 \rangle$ and $rm_{A-k+2} \in \langle \mathcal{L}_1 \rangle$. Since all elements of M_{A-k+2} and M_{A-k+3} are in $\mathcal{L}_1$, we may conclude that all monomials of degree $A-k+2$ and all monomials of degree $A-k+3$ in r, s, t are in $\langle \mathcal{L}_1 \rangle$. By using the equation for r, we note that

$$rm_{A-k} = Q(r,s,t)m_{A-k} + C(r,s,t)m_{A-k}.$$

The monomials of $Q(r,s,t)m_{A-k}$ are of degree $A-k+2$ and the monomials occurring in $C(r,s,t)m_{A-k}$ are of degree $A-k+3$. Thus, $rm_{A-k} \in \langle \mathcal{L}_1 \rangle$ and by induction, the lemma follows. □

This proves that $\mathcal{L}_0 \equiv [0, \ldots, 0] \pmod{\mathcal{L}_1}$. Now consider the monomials in $\mathcal{L}_1$ of the shape rm_{A-2}. Consider as above, $rm_{A-2} = Q(r,s,t)m_{A-2} + C(r,s,t)m_{A-2}$. Note that the monomials in $Q(r,s,t)m_{A-2}$ are of degree A. Hence, after performing column operations within $\mathcal{L}_1$, we may assume that $\mathcal{L}_1$ consists of the monomials

$$\begin{aligned} s^a t^b, &\qquad a+b \leq A \\ r^a s^b t^c, &\qquad a+b+c = A, \qquad a \geq 1 \\ C r^a s^b t^c, &\qquad a+b+c = A-2, \qquad a \geq 0. \end{aligned} \tag{5.2}$$

Next, we need the following result:

Lemma 37. *We can assume without loss of generality that $Q_2(s,t)$ does not vanish identically modulo p.*

Proof. We note that $p \mid s,t$ by assumption. From the equation for r it is clear that $p^2 \mid r$ and if p divides all coefficients of $Q_2(s,t)$ then $p^3 \mid Q(r,s,t)$ and hence p^3 divides r. In this case the work we have done so far is enough to prove the Lemma. Indeed, if $p \mid s$, $p \mid t$ and $p^3 \mid r$ then

$$\nu_p(\Delta) \geq \sum_{a+b\leq A} (a+b) + 2 \sum_{a+b+c=A, a\geq 1} (3a+b+c) = 2A^3 + O(A^2).$$

This is strictly better than the inequality (5.1) we are aiming for. Thus, we may assume that one coefficient of Q_2 is not divisible by p. □

Therefore, we may now assume in particular that $p \nmid C(0,1,0)$, as outlined before.

5.5 Calculating $\nu_p(\Delta)$

Recall that we want to find ν as large as possible so that $p^\nu \mid \Delta$. We will prove the following crucial lemma for the column operations we are going to perform:

Lemma 38. *Let $l \in \{1,2,\dots A_1-1\}$: (Recall $A = 2A_1$) and let $k \in \{l,\dots,A-l-2\}$. Furthermore, assume that $m = m_{A-l-k-2}$ is a monomial in s,t of degree $A-l-k-2$,*

not depending on r. Then

$$\begin{aligned} C^{l+1}r^{k-l}m - C^{l-1}r^{k-l+1}C_3m \in \langle & C^l r^{k-l} M_{A-k-l}, \\ & C^{l-1}r^{k-l+2}M_{A-k-l}, \\ & C^{l-1}r^{k-l+3}M_{A-k-l-1}, \\ & C^{l-1}r^{k-l+4}M_{A-k-l-2}, \\ & C^l r^{k-l+1}M_{A-k-l-1}, \\ & C^l r^{k-l+2}M_{A-k-l-2}\rangle. \end{aligned}$$

Proof. First note that the following identity holds

$$C^2 - C_3 r = -Q_2 C + r(C - C_3) - C(Q - Q_2)$$

because it is equivalent to $C^2 = rC - QC$ which is true because $r = Q + C$. Let $m = m_{A-k-l-2}(s,t)$ be any monomial of degree $A-k-l-2$ which does not contain r. Multiplying the identity by $C^{l-1}r^{k-l}m$, we get

$$\begin{aligned} C^{l+1}r^{k-l}m - C^{l-1}r^{k-l+1}C_3m = & -C^l r^{k-l}Q_2 m \\ & +C^{l-1}r^{k-l+1}(C - C_3)m \\ & -C^l r^{k-l}(Q - Q_2)m. \end{aligned}$$

Next, observe that

$$C^l r^{k-l}Q_2 m \in C^l r^{k-l} M_{A-k-l}.$$

Note that $C - C_3 = rC_2 + r^2C_1 + r^3C_0$ and $Q - Q_2 = rQ_1 + r^2Q_0$ which gives the last five expressions on the right-hand side of the lemma. □

We now regroup the elements of $\mathcal{L}_1$ as follows:

$$\begin{aligned}
\mathcal{L}_{1,0} :=& M_0 \cup M_1 \cup \ldots \cup M_A \\
\mathcal{L}_{1,k} :=& (r^k M_{A-k} \cup C r^{k-1} M_{A-k-1}) \qquad (k = 1, \ldots, A-1), \\
\mathcal{L}_{1,A} :=& \{r^A\}.
\end{aligned}$$

Next, we define lists of polynomials $\mathcal{L}_{l,k}$ for $1 \leq l \leq A_1$ and $1 \leq k \leq A$ as follows: For $l \leq k \leq A - l$, let:

$$\begin{aligned}
\mathcal{L}_{l,k} :=& C^l r^{k-l} M_{A-k-l} \\
& \cup C^{l-1} r^{k-l+1} M_{A-k-l+1} \\
& \bigcup_{m=2}^{l} C^{l-m} r^{k-l+m} M^{(3)}_{A-k-l+m}.
\end{aligned}$$

For $k = l - 1$, let:

$$\begin{aligned}
\mathcal{L}_{l,k} :=& C^{l-1} M_{A-2l+2} \\
& \bigcup_{m=2}^{l} C^{l-m} r^{m-1} M^{(3)}_{A-2l+m+1}.
\end{aligned}$$

and for all other k and l define $\mathcal{L}_{l,k}$ recursively by:

$$\mathcal{L}_{l,k} := \mathcal{L}_{l-1,k}.$$

We set $\mathcal{L}_{l,0} := \mathcal{L}_{1,0}$ for all $1 \leq l \leq A_1$. Finally, we define for $1 \leq l \leq A_1$:

$$\mathcal{L}_l := \mathcal{L}_{l,0} \cup \mathcal{L}_{l,1} \cup \ldots \cup \mathcal{L}_{l,A}.$$

Note that the definition of $\mathcal{L}_1$ agrees precisely with the polynomials we already have in $\mathcal{L}_1$ (see (5.2)). Furthermore, observe that for $k \neq 0$ and any l, all the polynomials

in $\mathcal{L}_{l,k}$ have lowest degree $\geq k + A$. In particular,

$$\nu(\mathcal{L}_{l,k}) \geq |\mathcal{L}_{l,k}|(k + A). \tag{5.3}$$

if $k \neq 0$. Also, note that $|\mathcal{L}_l| = N(A)$ for all l. Let Δ_l be the determinant corresponding to the monomials $\mathcal{L}_l$. We will prove the following:

Lemma 39. *We have that*

$$\nu_p(\Delta_1) = \nu_p(\Delta_{A_1}).$$

Proof. The idea of the algorithm can be explained as follows. The algorithm has $A_1 - 1$ steps. We start at $l = 1$ and then proceed successively to $l = A_1$. In each step we perform column operations to transform the elements from $\mathcal{L}_l$ into the elements of $\mathcal{L}_{l+1}$. The key ingredient is the identity in Lemma 38. The identity allows us to replace the columns $C^{l-1}r^{k-l+1}s^3m$ by $C^{l+1}r^{k-l}m$. (Here we use that the coefficient of s^3 in $C_3(s,t)$ is not divisible by p). We only know that $p^{A+k} \mid C^{l-1}r^{k-l+1}s^3m$ but that $p^{A+k+1} \mid C^{l+1}r^{k-l}m$, so the replacement of the column is a strict improvement. The details are now as follows:

Assume $1 \leq l \leq A_1 - 1$ and let us start with the determinant Δ_l corresponding to the columns from $\mathcal{L}_l$. We will now perform column operations to transform the determinant to Δ_{l+1}.

First, we note that for $k = l, \ldots, A - l - 2$,

$$C^{l-1}r^{k-l+1}C_3M_{A-k-l-2} \subseteq \langle \mathcal{L}_{l,k} \rangle,$$
$$C^{l}r^{k-l}M_{A-k-l} \subseteq \mathcal{L}_{l,k},$$
$$C^{l-1}r^{k-l+2}M_{A-k-l} \subseteq \mathcal{L}_{l,k+1},$$
$$C^{l-1}r^{k-l+3}M_{A-k-l-1} \subseteq \mathcal{L}_{l,k+2},$$
$$C^{l}r^{k-l+1}M_{A-k-l-1} \subseteq \mathcal{L}_{l,k+1},$$
$$C^{l}r^{k-l+2}M_{A-k-l-2} \subseteq \mathcal{L}_{l,k+2},$$
$$C^{l-1}r^{k-l+4}M_{A-k-l-2} \subseteq \mathcal{L}_{l,k+3}.$$

The first six of these statements follow directly from the definition of $\mathcal{L}_{l,k}$ when $l \leq k \leq A - l$. When $k + 3 \leq A - l$ then it also follows straight from the definition that

$$C^{l-1}r^{k-l+4}M_{A-k-l-2} \subseteq \mathcal{L}_{l,k+3}.$$

If $k + 3 = A - l + 1$ then $\mathcal{L}_{l,k+3} = \mathcal{L}_{l-1,k+3}$ and then $(l-1) \leq k + 3 \leq A - (l-1)$ and $C^{l-1}r^{k-l+4}M_{A-k-l-2} \in \mathcal{L}_{l-1,k+3}$. We can verify the last claim directly when $l = 1$.

Now we aim to repeatedly apply the identity of Lemma 38. We execute the following procedure successively for For $k = l, \ldots, A - l - 2$. Let $m_a = s^b t^a$ denote a monomial of degree $a + b = A - k - l - 2$ in s, t not depending on r. One element of $\mathcal{L}_{l,k}$ will be $C^{l-1}r^{k-l+1}s^3m_a \in C^{l-1}r^{k-l+1}M_{A-k-l+1}$. Call the corresponding column $\mathcal{C}$. We now multiply this column by $C_3(1, 0)$. This does not change $\nu_p(\Delta_l)$ since $p \nmid C_3(1, 0)$. Next, we add a linear combination of the columns $C^{l-1}r^{k-l+1}s^2tm_a$, $C^{l-1}r^{k-l+1}st^2m_a$ and $C^{l-1}r^{k-l+1}t^3m_a$ to $\mathcal{C}$ so that $\mathcal{C}$ becomes $C^{l-1}r^{k-l+1}C_3m_a$. Next we add scalar multiples of columns from $\mathcal{L}_{l,k}$, $\mathcal{L}_{l,k+1}$, $\mathcal{L}_{l,k+2}$ and $\mathcal{L}_{l,k+3}$ to the column $\mathcal{C}$, according to Lemma 38 so that $\mathcal{C}$ becomes $C^{l+1}r^{k-l}m_a$. We have thus replaced the column $C^{l-1}r^{k-l+1}s^3m_a$ by the column $C^{l+1}r^{k-l}m_a$. We can do this successively

for all $a = 0, \ldots, A-k-l-2$. In particular, we should note that no column operation to replace any $C^{l-1}r^{k-l+1}s^3m_{a_0}$ uses any of the previously replaced columns $C^{l-1}r^{k-l+1}s^3m_a$ with $a < a_0$.

Therefore, we have replaced $(A-k-l-1)$ of the $(A-k-l+2)$ monomials $C^{l-1}r^{k-l+1}M_{A-k-l+1}$ by the monomials $C^{l+1}r^{k-l}M_{A-l-k-2}$ and we denote the remaining 3 monomials of $C^{l-1}r^{k-l+1}M_{A-k-l+1}$ by $C^{l-1}r^{k-l+1}M^{(3)}_{A-k-l+1}$. (We note that explicitly $M^{(3)}_{A-k-l+1} = \{t^{A-k-l+1}, t^{A-k-l}s, t^{A-k-l-1}s^2\}$). To phrase this in terms of our sets $\mathcal{L}_{l,k}$: For $k = l, \ldots, A-l-2$, we replace the $C^{l-1}r^{k-l+1}M_{A-k-l+1}$ in $\mathcal{L}_{l,k}$ by $C^{l-1}r^{k-l+1}M^{(3)}_{A-k-l+1}$. Furthermore, we add $C^{l+1}r^{k-l}M_{A-l-k-2}$ to $\mathcal{L}_{l,k+1}$. The result of this process will then be $\mathcal{L}_{l+1}$.

After we have carried out this algorithm for all k, we realize that

$$\nu_p(\Delta_l) = \nu_p(\Delta_{l+1}).$$

Successively carrying out this algorithm for all l, we conclude that

$$\nu_p(\Delta_1) = \nu_p(\Delta_{A_1}).$$

□

Thus, it suffices to calculate $\nu_p(\Delta_{A_1})$. We have

$$\nu_p(\Delta_{A_1}) \geq \nu(\mathcal{L}_{1,0}) + \sum_{l=2}^{A_1} \nu(\mathcal{L}_{l,l-1}) + \sum_{l=1}^{A_1} \nu(\mathcal{L}_{l,A-l}) + \nu([r^A]).$$

We note that

$$\nu(\mathcal{L}_{1,0}) = \sum_{a+b \leq A} (a+b) = \frac{1}{3}A^3 + O(A^2).$$

For the remaining sums we use the estimate (5.3). Observe that for appropriate l,

$$|\mathcal{L}_{l,l-1}| = A - 2l + 3 + 3(l-1) = A + l$$

and that

$$|\mathcal{L}_{l,A-l}| = 1 + 2 + 3(l-1) = 3l.$$

Therefore,

$$\sum_{l=2}^{A_1} \nu(\mathcal{L}_{l,l-1}) \geq \sum_{l=2}^{A_1} (A+l)(A+l-1) = \frac{19}{24}A^3 + O(A^2),$$

and

$$\sum_{l=1}^{A_1} \nu(\mathcal{L}_{l,A-l}) \geq \sum_{l=1}^{A_1} 3l(2A-l) = \frac{5}{8}A^3 + O(A^2).$$

Altogether we obtain the desired estimate (5.1). Note that

$$|\Delta| \ll X^{AH}$$

and that $AH = \frac{3}{2}A^3 + O(A^2)$. So, we may pick $P = X^{6/7}$ which gives a number of auxiliary varieties $O(X^{12/7+\epsilon})$.

Bibliography

[1] A. Axer, Über einige Grenzwertsätze, *S.-B. Math.-Natur. K1. Akad. Wiss. Wien (2a)*, 120 (1911), 1253–1298.

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

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

[4] J. Brandes, Twins of s-free numbers, Diploma Thesis, Institute for Algebra and Number Theory University of Stuttgart (2009).

[5] N. Broberg, A note on a paper by R. Heath-Brown: The density of rational points on curves and surfaces, *J. Reine Angew. Math.*, 571 (2004), 159-178.

[6] T. D. Browning, Power-free values of polynomials, *Archiv der Math. (2)*, 96 (2011), 139–150.

[7] L. Carlitz, On a problem in additive arithmetic, *Quart. J. Math. Oxford Ser. 3*, 1 (1932), 273–290.

[8] D. Mendes da Costa, Integral points on elliptic curves and the Bombieri–Pila bounds, preprint (2013), *arXiv:1301.4116v2*.

[9] H. Davenport, Analytic Methods for Diophantine Equations and Diophantine Inequalities, *Cambridge University Press*, 1962.

[10] H. Davenport, Cubic forms in 16 variables, *Proc. Roy. Soc. A*, 272 (1963), 285–303.

[11] R. Dietmann, O. Marmon, The density of twins of k-free numbers, *arXiv:1307.2481*, to appear in Bulletin of the London Mathematical Society.

[12] J. Ellenberg, A. Venkatesh, On uniform bounds for rational points on nonrational curves, *International Mathematics Research Notices*, 5 (2005), 2163–81.

[13] P. Erdös, Arithmetical properties of polynomials, *J. London Math. Soc.*, 28 (1953), 416–425.

[14] T. Estermann, Einige Sätze über quadratfreie Zahlen, *Math. Ann.*, 105 (1931), 653–662.

[15] É. Fouvry, F. Jouve, Size of regulators and consecutive squarefree numbers, *Mathematische Zeitschrift*, 273 (2012), 869-882.

[16] É. Fouvry, F. Jouve, A positive density of fundamental discriminants with large regulator. *Pacific J. Math.*, 262, no. 1 (2013), 81-107.

[17] I. M Gel'fand, M. M. Kapranov, A. V. Zelevinsky, Discriminants, Resultants and Multidimensional Determinants, Birkhauser, 1994.

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

[19] D.R. Heath-Brown, Counting Rational Points on Algebraic Varieties, *Analytic Number Theory*, Springer Lecture Notes Vol. 1891,

[20] D.R. Heath-Brown, Cubic forms in ten variables, *Proc. London Math. Soc. (3)*, 47 (1983), 225–257. Springer Verlag, Berlin-Heidelberg, 2006.

[21] D.R. Heath-Brown, Sums and differences of three k-th powers, *J. Number Theory*, 129 (2009), 1579–1594.

[22] D.R. Heath-Brown, Square-Free Values of $n^2 + 1$, *Acta arith.*, 155 (2012), 1–13.

[23] D.R. Heath-Brown, Power-free values of polynomials, *Quart. J. Math.*, 64 (2013), 177-188.

[24] D.R. Heath-Brown, The Square-Sieve and Consecutive Square-Free Numbers, *Math. Ann.*, 266 (1984), 251–259.

[25] D.R. Heath-Brown, The number of primes in a short interval, *Journal für die reine und angewandte Mathematik 1988*, 389 (1988), 22–63.

[26] D.R. Heath-Brown, Diophantine approximation with square-free numbers, *Mathematische Zeitschrift*, 187 (1984), 335–344.

[27] H. Helfgott, Power-free values, large deviations and integer points on irrational curves, *J. Théor. Nombres Bordeaux*, 19 (2007), 433–472.

[28] H. Helfgott, Power-free values, repulsion between points, differing beliefs and the existence of error, *Anatomy of integers*, 81–88, CRM Proc. Lecture Notes 46, Amer. Math. Soc., 2008.

[29] C. Hooley, On the power-free values of polynomials, *Mathematika*, 14 (1967), 21–26.

[30] C. Hooley, On power-free numbers and polynomials II, *J. reine angew. Math.*, 295 (1977), 1–21.

[31] C.-H. Jia, The distribution of square-free numbers, *China Ser. A 36*, 2 (1993), 154–169.

[32] E. Landau, Sur quelques inégalités dans la théorie de la fonction $\zeta(s)$ de Riemann, *Bull. Soc. Math. France*, 33 (1905), 229–241.

[33] D.J. Lewis, K. Mahler, Representation of integers by binary forms, *Acta Arith.*, 6 (1961), 333–363.

[34] M. Nair, Power free values of polynomials. *Mathematika*, 23 (1976), 159–183.

[35] M. Nair, Power free values of polynomials II, *Proc. London Math. Soc.*, 38 (1979), 353–368.

[36] J. Pila, Density of integral and rational points on varieties, *Astérisque*, 228 (1995), 183–187.

[37] G. Ricci, Ricerche aritmetiche sui polinomi, *Rend. Circ. Mat. Palermo*, 57 (1933), 433–475.

[38] M. Robbiani, On the number of rational points of bounded height on smooth bilinear hypersurfaces in biprojective space, *J. London. Math. Soc. (2)* 63 (2001), 33–51.

[39] P. Salberger, Counting rational points on projective varieties, Submitted, 2010.

[40] P. Salberger, Uniform bounds for rational points on cubic hypersurfaces, preprint, 2014.

[41] W. Schmidt, Equations Over Finite Fields, An Elementary Approach, *Springer Verlag*, 1976.

[42] C. V. Spencer, The Manin Conjecture for $x_0y_0 + \ldots + x_sy_s = 0$, *J. Number Theory*, 129 (2009), 1505–1521.

[43] A. Thue, Über Annäherungswerte algebraischer Zahlen, *J. reine angew. Math.*, 135 (1909), 284–305.

[44] K.-M. Tsang, The distribution of r-tuples of square-free numbers, *Mathematika*, 32 (1985), 265–275.

[45] A. Walfisz, Weylsche Exponentialsummen in der neueren Zahlentheorie, *Mathematische Forschungsberichte, XV.* (VEB Deutscher Verlag der Wissenschaften, Berlin, 1963).

[46] M. N. Walsh, Bounded Rational Points on Curves, *International Mathematics Research Notices*, 2014.

[47] E. Weiss, Algebraic Number Theory, *International Series In Pure and Applied Mathematics*, McGraw-Hill, New York (1963).