Topics in Sieve Theory

Oliver McGrath
Magdalen College
University of Oxford

A thesis submitted for the degree of
Doctor of Philosophy
Trinity 2022

For Tim and Jack.

Acknowledgements

I would like to thank my supervisor James Maynard for being a constant source of guidance throughout my time in Oxford. I greatly appreciate that he was always available to answer any questions I had, no matter how trivial, and for making our weekly meetings so enjoyable.

I am grateful to the EPSRC for funding the first three and a half years of my research. I would like to thank James and the ERC for their generous financial support which covered the remaining few months.

I am thankful to all my friends who have supported me over the past few years, along with my colleagues in the department and the number theory research group. Special thanks go to Liam. At times it felt like we were both a long way from the Shire, and your company in Oxford made darker times immeasurably brighter.

I am thankful for my partner, Ndi, whose strength and resilience inspires me everyday. This thesis wouldn't have been possible without your unconditional love and support. I look forward to many more adventures with you in the future.

Finally, I am thankful for my family and their endless support over the years. In particular, I owe so much to my parents. They are my greatest teachers, and this thesis is dedicated to them.

Abstract

This thesis is concerned with applications of sieve methods to two Diophantine problems.

The first problem requires us to prove the existence of a certain infinite configuration of sums of two squares. Namely, the aim is to exhibit two increasing sequences of integers a_i and m_j such that $m_j - a_i = \square + \square$ for every $1 \leq i \leq j$. This set-up has a geometric interpretation which arises naturally in the field of quantum chaos. We tackle this problem using a modified half-dimensional Maynard-Tao sieve, and present details of the argument in Chapter 2.

The second problem asks us to show that a certain Diophantine equation has few integer solutions. We approach this problem by adapting the polynomial sieve developed by Browning and using the work of Weil and Deligne to obtain appropriate estimates for various exponential sums which naturally arise. As a corollary to the main result, we will deduce that polynomials with integer coefficients have "small asymmetric additive energy," a result which has various applications in the literature. We give the details of this argument in Chapter 3.

Contents

Chapter 1

Introduction

The most fundamental objects in mathematics are the prime numbers. These elementary objects have fascinated mathematicians since the time of Euclid, and have proved to be an exceptionally good source of simple-to-state, yet seemingly intractable, mathematical problems.

In recent times, the field of prime number theory has enjoyed immense progress. The development of powerful sieve methods has enabled analytic number theorists to shed new light on these elementary, yet mysterious, objects. In particular, in the last two decades there has been a flurry of activity concerning small gaps between primes. Although plenty of questions continue to elude us - are there infinitely many twin primes? - we now have a much greater understanding of the local statistics of primes.

The story by now is familiar; it begins in 2005, when Goldston, Pintz and Yıldırım [11] (henceforth referred to collectively as GPY) succeeded in showing that there exist consecutive primes which are closer than any arbitrarily small multiple of the average spacing. This was a huge breakthrough, which brought us ever closer to answering questions about prime numbers which have confounded us for millennia. Moreover, GPY could obtain bounded gaps between primes provided one could go slightly beyond the square-root barrier in the Bombieri-Vinogradov theorem. Later, in 2013, Zhang [29] spectacularly succeeded in doing this exactly this, for a special type of moduli. This weaker result proved to be sufficient to establish, for the first time, bounded gaps between primes.

Later that same year, Maynard [21] (and independently Tao, unpublished) pushed the theory in another direction. They developed the so-called Maynard-Tao sieve;

a powerful new sieve method which was considerably more flexible than the sieve method inherent in the work of GPY and Zhang. Using this, Maynard was able to establish vastly superior results (even without requiring one to extend the Bombieri-Vinogradov theorem).

As is well known, sieve methods are very flexible tools, and so the same methodologies inherent in the works above can be transferred to other problems which may look superficially quite different. Thus, although the work in this thesis is not directly related to bounded gaps between primes, to convey the ideas accurately it is instructive to begin by reflecting on some of the main ideas underlying the works above. In particular, the work of GPY and Maynard is directly relevant and applicable to the problems I will focus on in later chapters.

Thus, the contents of this introductory chapter are as follows: in Section 1.1 we will give a broad overview of what sieves are, and how they are used in analytic number theory. In Section 1.2 we will describe a particular sieve method called the Selberg sieve. In Section 1.3 we will describe the GPY method for detecting small gaps between primes, and in Section 1.4 we will discuss the Maynard-Tao sieve. Finally, in Section 1.5 we will look at how sieves can be used to count solutions to Diophantine equations.

1.1 Sieves

Sieves are tools used by analytic number theorists to count prime numbers and more generally patterns in prime numbers. As mentioned above, sieves are flexible tools and may also count patterns in other sets of arithmetic interest. For example, we may use sieves to count numbers representable as a sum of two squares; a case of particular interest to us in this thesis. As observed by Hooley [15], we may also use sieves to count solutions to Diophantine equations. We will discuss this in more detail in Section 1.5.

The first sieve technique on record can be traced back to a Greek polymath by the name of Eratosthenes of Cyrene, who was active in the third century BC. We note the trivial fact that any composite integer less than X (say) necessarily has a prime factor less than $\sqrt{X}$. Using this, Eratosthenes realised that one could compute prime numbers up to X by writing all the integers up to X in a long list and "crossing

off" the multiples of primes less than $\sqrt{X}$. The terminology arises as this algorithm clearly resembles a "sieving process" in which only the prime numbers survive.

An analytic implementation of this process is due to the French mathematician Legendre. We can realise the above algorithm as an inclusion-exclusion process. Let us introduce the *Möbius function* $\mu(n)$, defined to be

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \dots p_k \text{ is square-free,} \\ 0 & \text{otherwise} \end{cases} \tag{1.1.1}$$

and satisfying the important convolution identity

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases} \tag{1.1.2}$$

We begin with a finite set of integers $\mathcal{A} \subset \mathbb{Z}$, a set of primes $\mathcal{P} \subseteq \mathbb{P}$, and a parameter $z \geq 1$. From this data we form the product

$$P(z) = \prod_{\substack{p<z \\ p\in\mathcal{P}}} p. \tag{1.1.3}$$

We would like to count the elements of $\mathcal{A}$ which are free from prime factors less than z. Let us call this count $S(\mathcal{A}, z)$, the *sifted set*. We may express this quantity succintly as

$$S(\mathcal{A}, z) = \#\{n \in \mathcal{A} : (n, P(z)) = 1\}. \tag{1.1.4}$$

Using (1.1.2), one immediately derives the following identity, which is often referred to as the *Legendre identity*:

$$S(\mathcal{A}, z) = \sum_{d|P(z)} \mu(d) \#\{n \in \mathcal{A} : d|n\}. \tag{1.1.5}$$

For special choices of parameters, it would be desirable to obtain good estimates for the sifted set. For example, up to negligible errors, we have the following:

1. *Primes:* if $\mathcal{A} = \{n \leq X\}$ and $\mathcal{P} = \mathbb{P}$ then $S(\mathcal{A}, X^{1/2})$ counts primes up to X.

2. *Patterns in primes:* if $\mathcal{A} = \{n(n+2) \leq X\}$ and $\mathcal{P} = \mathbb{P}$ then $S(\mathcal{A}, X^{1/2})$ counts twin primes up to X.

3. *Sums of two squares:* if $\mathcal{A} = \{n \leq X\}$ and $\mathcal{P} = \{p \in \mathbb{P} : p \equiv 3 \pmod 4\}$ then $S(\mathcal{A}, X^{1/2})$ counts sums of two squares up to X.

Legendre's identity tells us that we can can get a handle on these sets provided that we can understand $\mathcal{A}$ well in arithmetic progressions; in modern parlance, we call this *Type I information* about $\mathcal{A}$.

To proceed, we typically make the assumption that we have estimates of type

$$\#\{n \in \mathcal{A} : d|n\} = \#\mathcal{A}\, g(d) + r_d \tag{1.1.6}$$

available. Here, g is a multiplicative function and r_d is a remainder term which we think of as being small. Such an approximation is true for most sets $\mathcal{A}$ which arise naturally. One should have in mind the example $g(d) = 1/d$ and $r_d = \{X/d\}$, which is the case of interest when we sieve for primes less than X like in example (1) above.

Typically we cannot use any information about the numbers r_d other than their size; in particular, exploiting cancellation with sign changes of the Möbius function is assumed to be out of the question. Thus, with assumption (1.1.6) we rewrite Legendre's identity as follows:

$$S(\mathcal{A}, z) = \#\mathcal{A} \sum_{d|P(z)} \mu(d)g(d) + O\Big(\sum_{d|P(z)} |r_d| \Big). \tag{1.1.7}$$

Unfortunately this means, in practice, to control the error terms we are forced to take z to be quite small. In particular, for the three interesting examples considered above, we are taking z substantially larger than any error term estimates would allow us to, and we cannot conclude anything non-trivial about $S(\mathcal{A}, z)$ via equation (1.1.7).

In some sense, this simple identity is the starting point for modern sieve theory. One now attempts to come up with alternative set-ups which allow one to obtain estimates valid for larger ranges of z, by modifying the underlying inclusion-exclusion process and introducing various auxiliary parameters. Typically, this involves finding majorants and minorants to the convolution identity (1.1.2). We call such objects *sieve weights*. In the next section I will introduce a particularly elegant upper bound sieve method due to Selberg, which is a vital building block for the theory which will follow.

1.2 The Selberg sieve

Let $(\lambda_d)_{d=1}^{\infty}$ be any sequence of real-valued weights such that $\lambda_1 = 1$ and $\lambda_d = 0$ whenever $d \geq R$ (say). From equation (1.1.2) it is clear that we have an upper bound

$$\sum_{d|n} \mu(d) \leq \Big(\sum_{d|n} \lambda_d \Big)^2. \tag{1.2.1}$$

All we are using here is the fact squares of real numbers are non-negative. This simple observation, due to Selberg [25], allows one to obtain upper bounds on the sifted set $S(\mathcal{A}, z)$. Indeed, we have

$$\begin{aligned} S(\mathcal{A}, z) &\leq \sum_{n \in \mathcal{A}} \Big(\sum_{d|(n, P(z))} \lambda_d \Big)^2 = \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} \#\{n \in \mathcal{A} : [d_1, d_2] | n\} \\ &= \#\mathcal{A} \sum_{d_1, d_2 | P(z)} \lambda_{d_1} \lambda_{d_2} g([d_1, d_2]) + O\Big(\sum_{d_1, d_2 \leq R} |\lambda_{d_1}||\lambda_{d_2}||r_{[d_1, d_2]}| \Big), \end{aligned} \tag{1.2.2}$$

where we have used assumption (1.1.6) to estimate $\mathcal{A}$ in arithmetic progressions.

Provided the function g is suitably regular, the main term can be viewed as a quadratic form in the coefficients λ_d, which can then be minimised using standard techniques (with the idea being the error term takes care of itself and is suitably small). For example, if the function g satisfies the natural regularity hypothesis

$$\sum_{\substack{w \leq p < y \\ p \in \mathcal{P}}} g(p) \log p = \kappa \log \frac{y}{w} + O(1) \tag{1.2.3}$$

for all $2 \leq w < y$ and some constant $\kappa \geq 0$, called the *sieve dimension*, one can show the optimal weights λ_d are (asymptotically) of the form

$$\lambda_d = \mu(d)(\log R/d)^{\kappa} \tag{1.2.4}$$

i.e. a smoothed Möbius function.

For instance, in the example where we sieve for primes, we take our sieving function to be $g(p) = 1/p$ and hence, by standard Mertens-type estimates for sums over primes, we satisfy (1.2.3) with $\kappa = 1$. In view of the convolution identity

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d, \tag{1.2.5}$$

where here $\Lambda(n)$ denotes the von Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \\ 0 & \text{otherwise,} \end{cases} \tag{1.2.6}$$

we can interpret this smoothing as dampening the contribution from highly composite integers, and hence a natural weight in light of the (arithmetic) sifted set we are trying to estimate.

When we sieve for sums of two squares - a case of particular importance in this thesis - our sieving function satisfies (1.2.3) with $\kappa = 1/2$. Thus, from the point of view of sieve theory, primes form a "one-dimensional" (or simply "linear") problem whereas sums of two squares form a "half-dimensional" problem. This reduction in the size of κ has some benefits which we will discuss later.

1.3 The GPY set-up

The authors GPY [11] employed a variant of the Selberg sieve in order to detect primes which are close together. To frame things in a slightly more general context which will be useful later, we first recall the following conjecture due to Hardy and Littlewood, which completely describes the small-scale structure of the prime numbers.

Conjecture (Hardy-Littlewood prime k-tuple conjecture)**.** *Fix a k-tuple of integers $\mathcal{H} = \{h_1, \dots, h_k\}$. We have*

$$\#\{n \leq X : n + h_1, \dots, n + h_k \text{ are prime}\} \sim \mathfrak{S}(\mathcal{H}) \frac{X}{(\log X)^k} \tag{1.3.1}$$

where

$$\mathfrak{S}(\mathcal{H}) = \prod_p \left(1 - \frac{v_{\mathcal{H}}(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-k} \tag{1.3.2}$$

and

$$v_{\mathcal{H}}(p) = \#\{1 \leq x \leq p : \prod_{i=1}^{k}(x + h_i) \equiv 0 \ (mod\ p)\}. \tag{1.3.3}$$

We recall that $\mathcal{H}$ is called *admissible* if $v_{\mathcal{H}}(p) < p$ for every prime p. In particular, this conjecture implies that whenever $\mathcal{H}$ is admissible, there exist infinitely many integers n for which the translates $n + h_i$ are simultaneously prime. In the special case when our admissible set is $\mathcal{H} = \{0, 2\}$, this conjecture reduces to the famous *twin prime conjecture.*

In order to analyse this conjecture, GPY considered the following set-up: let us examine the sum

$$S = \sum_{N<n\leq 2N} \Big(\sum_{i=1}^{k} 1_{\mathbb{P}}(n+h_i) - m \Big) w_n \tag{1.3.4}$$

where w_n are non-negative weights. If one could show S was positive for all sufficiently large N, then, by positivity, one obtains infinitely many integers n for which at least $m+1$ of the linear forms $n+h_i$ are simultaneously prime. Thus, one would like to choose weights concentrated on when "many" of the translates $n+h_i$ are prime, whilst being analytically tractable enough so one can handle the sieve sums which arise. (This last point should not be understated!)

Naturally, this led GPY to consider using sieve weights. In clear reference to the optimal Selberg sieve weights (of dimension k), GPY chose their weights to be of the form

$$w_n = \Big(\sum_{d \mid \prod_{i=1}^{k}(n+h_i)} \lambda_d \Big)^2 \tag{1.3.5}$$

where

$$\lambda_d = \mu(d)(\log R/d)^{k+l}. \tag{1.3.6}$$

The GPY weights are slightly more general than the optimal Selberg sieve weights (of dimension k). Here $0 \leq l \leq k$ is a parameter which they were free to optimise, subject to the constraint $l = o(k)$. This extra degree of freedom is in fact important for their argument, and arises because the GPY set-up is not a pure k-dimensional sieving problem (as one may expect when sieving for primes in a k-tuple). In actuality it is slightly more complicated, due to the fact there is a optimising step in the argument: one must balance the sieve estimates coming from the terms corresponding to primes and the terms corresponding to integers.

As mentioned at the beginning of this section, these weights *just* missed being able to prove bounded gaps between primes, yet were still able to prove interesting and novel results such as

$$\liminf_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0. \tag{1.3.7}$$

Here, by the prime number theorem, $\log p_n$ is understood to be the size of the average gap near the n'th prime. This result was then improved upon in subsequent papers.

Having said this, any improvement on the range of moduli allowable in the Bombieri-Vinogradov theorem would yield bounded gaps between primes via this method. This is the aspect of the GPY method which Zhang [29] improved upon: it turns out one can improve the range of moduli in certain special situations which is sufficient for the GPY argument to go through as before. This important work goes in a somewhat orthogonal direction to the rest of this thesis, and so we will not discuss Zhang's insightful contributions to the subject any further; suffice to say, the main result proved, namely

$$\liminf_{n\to\infty}(p_{n+1}-p_n)\leq 70 \text{ million}, \tag{1.3.8}$$

was a landmark achievement in analytic number theory.

Before moving on, we remark here that there exists a famous fundamental obstruction to producing primes via sieves called the *parity problem*, which informally says that sieves cannot distinguish between numbers with an even or odd number of prime factors solely using Type I information. The GPY method circumvents this issue by producing primes via the pigeonhole principle. In this context, the parity problem manifests itself as saying the expected "main term" contribution from the $1_{\mathbb{P}}(n+h)$ terms can be at most the contribution from the constant term $1/2$. (In particular, one could never prove the existence of infinitely many twin primes via the GPY method as presented above.)

1.4 The Maynard-Tao sieve

The key insight of Maynard [21] (and Tao independently, unpublished) was to consider more general sieve weights in the GPY set-up which were considerably more flexible. The Maynard-Tao sieve weights take the form

$$w_n=\Bigg(\sum_{d_i|n+h_i\ \forall i}\lambda_{d_1,\dots,d_k}\Bigg)^2 \tag{1.4.1}$$

where now

$$\lambda_{d_1,\dots,d_k}\approx\prod_{i=1}^{k}\mu(d_i)F\bigg(\log\frac{R}{d_1},\dots,\log\frac{R}{d_k}\bigg) \tag{1.4.2}$$

and F is a suitably smooth function which one is free to optimise at the end of the argument.

It is the extra flexibility afforded by considering divisors of each translate $n+h_i$

individually which allows the Maynard-Tao sieve to go much further than the GPY sieve considered above. For instance, it is shown that

$$\liminf_{n\to\infty}(p_{n+1}-p_n)\leq 600, \tag{1.4.3}$$

and, more generally, for any integer $m\geq 2$ we have

$$\liminf_{n\to\infty}(p_{n+m}-p_n)\ll m^3e^{4m}. \tag{1.4.4}$$

These bounds were subsequently improved by the Polymath8b project [24] which introduced lots of fine refinements to the Maynard-Tao sieve and optimised many minor arguments. They can also be improved further, conditionally, if one assumes extensions to the Bombieri-Vinogradov theorem (such as the Elliot-Halberstam conjecture) hold.

In Chapter 2 we will look at a problem which is reminiscent of the prime k-tuples conjecture, except we are now interested in sums of two squares rather than primes. Hence, from the perspective of sieve theory, the sieving dimension is halved and our problem becomes easier. A natural tool to use in this context is the half-dimensional Maynard-Tao sieve. For our purposes, this means that one can obtain quantitatively far superior results when dealing with sums of two squares instead of primes.

For example, let us fix an admissible set $\{h_1,\dots,h_k\}$. Then the (standard) Maynard-Tao sieve, applied as in [21], can be used to show that $\gg \log k$ of the translates $n+h_1,\dots,n+h_k$ are simultaneously prime, infinitely often. On the other hand, the *half-dimensional* Maynard-Tao sieve, applied in exactly the same way, can be used to show that $\gg k^{1/2}$ of the translates $n+h_1,\dots,n+h_k$ are simultaneously sums of two squares, infinitely often - a substantial improvement.

However, it should be emphasised that this boost in the numerics is *not* the reason why our argument works for sums of two squares and not for primes. Rather, crucially, it relies on the fact that one can estimate two-point correlations of sums of two squares. Such estimates are of course not available for primes.

Our problem additionally requires us to have some extra control over which elements survive the sieving process. This necessitates a modification of the sieve and a second moment estimate (thus going beyond the GPY set-up, which is a first moment method). This problem will be described fully in Chapter 2.

1.5 Detecting solutions to Diophantine equations with sieves

As a further indication to their versatility, one can use sieves to count solutions to Diophantine equations. The philosophy is straightforward and reminiscent of the famous "local-global" principle: one can attempt to show that a certain Diophantine equation has few integer solutions by showing that it doesn't have lots of local solutions for "many" primes p.

This idea was first observed by Hooley [15] in the 1980s, who used a generalised Selberg sieve to count solutions to the equation

$$x_1^3 + x_2^3 = x_3^3 + x_4^3 \tag{1.5.1}$$

where $x_i \in [1, B] \cap \mathbb{Z}$ for each i. This degree 3 equation has 4 variables, and thus lands awkwardly outside the range of Diophantine equations treatable via traditional methods such as the circle method or the determinant method. In this regime, one notes that there are $2B^2$ "trivial" solutions of the form (a, b, a, b) and (a, b, b, a), and one would expect there to be very few (if any) other solutions (an expectation supported by standard heuristics in the field of arithmetic geometry). Indeed, Hooley showed that there are at most $o(B^2)$ "non-trivial" solutions, and in later work [16, 18], he generalised his method to work for equal sums of two k'th powers for any $k \geq 3$.

Today, a particularly clean sieve method in this context has been developed by Browning [4], known as the polynomial sieve. This sieve method extends the square sieve of Heath-Brown [12] and the power sieve of Munshi [22], and will be presented in Chapter 3. In particular, it allows us to take a set $\mathcal{A} \subset \mathbb{Z}^m$ and a polynomial $F \in \mathbb{Z}[x_0, x_1, \ldots, x_m]$, and detect solutions to the equation $F(y_0, y_1, \ldots, y_m) = 0$ where $y_0 \in \mathbb{Z}$ and $(y_1, \ldots, y_m) \in \mathcal{A}$.

We will apply the polynomial sieve to count solutions to the equation

$$f(x_1) + f(x_2) = f(x_3) + f(x_4) + k \tag{1.5.2}$$

where f is a polynomial with integer coefficients, and k is a fixed non-zero integer. We call this the *asymmetric additive energy of the polynomial f (with respect to k)*, and recently it has been realised by various authors that estimates for this quantity would have applications in the literature. We will discuss this in more detail in Chapter 3.

To demonstrate how the sieve method works in this context, it is instructive to study the cubic equation (1.5.1) considered by Hooley in more detail. One first makes a change of variables which allows us to easily isolate the trivial solutions described above: rewriting our equation in the factorised form

$$(x_1 - x_3)(x_1^2 + x_1x_3 + x_3^2) = (x_4 - x_2)(x_4^2 + x_2x_4 + x_2^2), \tag{1.5.3}$$

an appropriate substitution of variables yields the equivalent equation

$$y_1(y_1^2 + 3y_2^2) = y_3(y_3^2 + 3y_4^2). \tag{1.5.4}$$

We now fix $y_3 \neq 0$ and count solutions to the simpler equation which remains. There are some extra complications which arise whenever y_1 and y_3 have a large gcd, relating to "trivial" solutions modulo the gcd which we have to work a bit harder to rule out. For simplicity, let us suppose that these variables are coprime. The benefit of this set-up is that we can restrict our attention to the set

$$\{(y_1, y_2) \in ([1, B] \cap \mathbb{Z})^2 : y_1^2 + 3y_2^2 \equiv 0 \pmod{y_3}\}, \tag{1.5.5}$$

thereby retaining the trivial bound of $O(B^{2+\epsilon})$ when we apply the sieve. This means we only need to win a tiny amount via the sieve to show the desired estimate of $o(B^2)$ for the number of non-trivial solutions. (Typically, one obtains power-savings via this method.)

The sieve method works in this context provided one has good estimates available for the local counts of solutions. These local counts manifest as exponential sums over certain algebraic varieties, such as

$$\sum_{\substack{x,y \in \mathbb{F}_p \\ x^2+3y^2=0}} e\left(\frac{Mx + Ny}{p}\right) \tag{1.5.6}$$

(here, M and N are integers reduced modulo p). One requires square-root cancellation for these exponential sums (in the generic case). Hence, to continue, it is necessary to invoke the work of Weil [28] and Deligne [9] concerning the Riemann Hypothesis for varieties over finite fields. Thus, although the sieve method as presented is ostensibly a tool belonging to the realm of analysis, to execute it effectively one has recourse to deep methods in algebraic geometry.

Chapter 2

A variation of the prime k-tuples conjecture with applications to quantum limits

Let $\mathcal{H}^* = \{h_1, h_2, \ldots\}$ be an ordered set of integers. We give sufficient conditions for the existence of increasing sequences of natural numbers a_j and n_k such that $n_k + h_{a_j}$ is a sum of two squares for every $k \geq 1$ and $1 \leq j \leq k$. Our method uses a novel modification of the Maynard-Tao sieve together with a second moment estimate. As a special case of our result, we deduce a conjecture due to D. Jakobson which has several implications for quantum limits on flat tori.

2.1 Introduction

We say that a set $\mathcal{H} = \{h_1, \ldots, h_k\}$ of distinct integers is *admissible* if $\#\{\mathcal{H} \pmod p\} < p$ for every prime p. An outstanding problem in analytic number theory is the prime k-tuples conjecture, which asserts the following.

Conjecture 2.1.1. *Let $\mathcal{H} = \{h_1, \ldots, h_k\}$ be admissible. Then there exists infinitely many integers n such that the translates $n + h_1, \ldots, n + h_k$ are prime.*

A proof of this conjecture is far out of reach of current techniques. However, we have been successful in establishing various weak versions of this result using sieve methods. For example, the Maynard-Tao sieve can be used to show that $\gg \log k$ of the translates are simultaneously prime infinitely often, when k is sufficiently large (cf. [21, 24]).

We extend the definition of admissibility to infinite ordered sets and say $\mathcal{H}^* =$

$\{h_1, h_2, \ldots\}$ is admissible if the finite truncation $\{h_1, \ldots, h_k\} \subseteq \mathcal{H}^*$ is admissible for every $k \geq 1$. In this chapter, we are interested in the following variation of this conjecture, for numbers representable as a sum of two squares.

Conjecture 2.1.2. *Let $\mathcal{H}^* = \{h_1, h_2, \ldots\}$ be admissible. Then there exists an increasing sequence of integers n_k such that, for every $k \geq 1$, the translates $n_k+h_1, \ldots, n_k+h_k$ are sums of two squares.*

We remark that if we replaced "sums of two squares" with "prime" here, then this would simply be a reformulation of Conjecture 2.1.1. (It is easy to show that any finite admissible set can be extended to an infinite admissible set.)

Our interest in this version of the conjecture stems from a problem which appears towards the end of D. Jakobson's *"Quantum limits on flat tori"* paper [19]. In this paper Jakobson is concerned with characterising the possible quantum limits that can arise on the standard flat d-dimensional torus $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$. A complete classification of such objects is established in two dimensions, with possible behaviours in higher dimensions described unconditionally for $d \geq 4$, and conditionally for $d = 3$ on a weak version of Conjecture 2.1.2 (cf. [19, Conjecture 8.2]).

In this chapter, we establish Jakobson's conjecture.

Theorem 2.1.3. *There exists increasing sequences of natural numbers a_j and M_k such that $M_k - a_j^2$ is a sum of two squares for $1 \leq j \leq k$. Moreover, the sequence a_j is such that:*

1. *$r_2(a_j) < r_2(a_{j+1})$ for all $j \geq 1$.*
2. *The even parts are uniformly bounded; that is to say, if we write $a_j = 2^{b_j} m_j$ where $(m_j, 2) = 1$, then $b_j = O(1)$ uniformly for $j \geq 1$.*

Here, $r_2(n)$ denotes the number of representations of n as a sum of two squares. We deduce Theorem 2.1.3 from the following general result.

Theorem 2.1.4. *Let $\mathcal{H}^* = \{h_1, h_2, \ldots\}$ be admissible such that each h_i is divisible by 4. Then there exists increasing sequences of natural numbers a_j and n_k such that $n_k + h_{a_j}$ is a sum of two squares for every $k \geq 1$ and $1 \leq j \leq k$.*

For example, Theorem 2.1.4 applied to the admissible set $\mathcal{H}^* = \{h_1, h_2, \ldots\}$ with elements $h_i = -(2 \cdot 5^i)^2$, yields a solution to Theorem 2.1.3.

As mentioned above, Theorem 2.1.3 allows us conclude results about quantum limits on flat tori. Let $(\lambda_j)_{j\geq 1}$ be a sequence of eigenvalues of the Laplace operator ∇ on $\mathbb{T}^d$ such that $\lambda_j \to \infty$, and let φ_j be corresponding eigenfunctions with $\|\varphi_j\|_2 = 1$. If the sequence of probability measures $\mathrm{d}\mu_j = |\varphi_j|^2 \mathrm{d}x$ has a weak-$*$ limit $\mathrm{d}v$, then we call $\mathrm{d}v$ a *quantum limit*. (Here $\mathrm{d}x$ is the normalised Riemannian volume.)

It can be shown that all limits of such sequences $\mathrm{d}\mu_j$ are absolutely continuous with respect to the Lebesgue measure on $\mathbb{T}^d$ (cf. [19, Theorem 1.3]), and so one can consider the Fourier expansion

$$\mathrm{d}v = \sum_{\tau \in \mathbb{Z}^d} c_\tau e^{2\pi i \langle \tau, x \rangle} \mathrm{d}x. \tag{2.1.1}$$

Among other things, Jakobson shows that in two dimensions all quantum limits are necessarily trigonometric polynomials (cf. [19, Theorem 1.2]). The same result isn't true for $d \geq 4$, and conjecturally not true for $d = 3$ either (cf. [19, Conjecture 8.2] and the following discussion). With Theorem 2.1.3, we can now complete this aspect of the classification of quantum limits on flat tori.

Theorem 2.1.5. *There exists quantum limits on $\mathbb{T}^3$ that are not trigonometric polynomials.*

As further consequences to Theorem 2.1.3 we are able to show the following results for quantum limits whose Fourier expansions are described as in (2.1.1).

Theorem 2.1.6. *Let $\epsilon > 0$. We have the following.*

(i) For $d \geq 4$ there exists quantum limits $\mathrm{d}v$ on $\mathbb{T}^d$ with densities that are not in $l^{2-\epsilon}$ (i.e. for which $\sum_\tau |c_\tau|^{2-\epsilon}$ diverges).

(ii) For $d \geq 5$ there exists quantum limits $\mathrm{d}v$ on $\mathbb{T}^d$ for which

$$\limsup_{\rho \to \infty} \frac{\Sigma(\rho)}{\rho^{d-4-\epsilon}} = +\infty,$$

where $\Sigma(\rho)$ is defined as

$$\Sigma(\rho) = \sum_{\substack{\tau \in \mathbb{Z}^d \\ |\tau| < \rho}} |c_\tau|. \tag{2.1.2}$$

The results contained in Theorem 2.1.6 improve upon various results found in [19]. Part (i) was previously shown for $d \geq 5$, and has now been extended to the case $d = 4$ where it is now optimal (cf. [19, Theorem 1.4]). Part (ii) improves on the weaker lower bound

$$\limsup_{\rho \to \infty} \frac{\Sigma(\rho)}{\rho^{d-5-\epsilon}} = +\infty$$

which was shown for $d \geq 6$. The lower bound we prove is believed to be optimal for all $d \geq 5$ (cf. [19, Proposition 1.2] and comments shortly after).

Remark 2.1.7. It is well-known that the eigenvalues of ∇ on $\mathbb{T}^d$ are the numbers $4\pi^2 k$ for non-negative integers k, and they occur with multiplicity $r_d(k)$ (the number of representations of k as the sum of d squares). This means various constructions associated to quantum limits on flat tori can be translated to problems in number theory involving sums of squares.

Remark 2.1.8. Jakobson shows how Theorem 2.1.3 follows from weak form of the prime k-tuples conjecture, essentially by using the fact primes $p \equiv 1 \pmod 4$ are the sum of two squares (cf. discussion at the end of [19, Section 8]). We note that the weak form of the conjecture Jakobson uses is still far out of reach of current methods.

2.2 Outline of new sieve ideas

In this section, let $\mathcal{A} \subseteq \mathbb{N}$ denote a set of arithmetic interest, which for our purposes is the set of numbers representable as a sum of two squares (but the following discussion holds more generally). We will denote random variables by boldfaced letters, for example $\mathbf{X}$. We will let $\mathbb{P}(\cdot)$ denote a probability measure and by $\mathbb{E}[\cdot]$ the expectation operator.

2.2.1 A model problem

Our aim is to prove Theorem 2.1.4. By a pigeonhole argument (see Proposition 2.5.1), it suffices to consider the following model problem.

Model Problem. *Fix an admissible set $\mathcal{H}^* = \{h_1, h_2, \ldots\}$ of integers and a partition $\mathcal{H}^* = B_1 \cup B_2 \cup \ldots$ where each bin B_i is a fixed, finite size k_i. Is it the case that for every $M \geq 1$ there exists elements $h_{a_1}, \ldots, h_{a_M}$ and infinitely many integers n such that $h_{a_j} \in B_j$ and $n + h_{a_j} \in \mathcal{A}$ for $1 \leq j \leq M$?*

We realise the above set-up as the output of a sieving process. For notational purposes we order $B_i = \{h_{k_0+\ldots+k_{i-1}+1}, \ldots, h_{k_0+\ldots+k_i}\}$ for $i \geq 1$, with the convention that $k_0 = 0$. Let $k = k_0 + \ldots + k_M$ for some large M. Given $n \in [N, 2N)$ for some large N, let $\mathbf{X}_i$ denote the random variable that counts the number of $h \in B_i$ such that $n + h \in \mathcal{A}$, and let $\mathbf{X} = \mathbf{X}_1 + \ldots \mathbf{X}_M$. The current method we use to detect primes in k-tuples is the GPY method. For general sets $\mathcal{A}$, the aim is to show the first moment inequality

$$S_{\mathcal{A}} = \sum_{N \leq n < 2N} \Big(\sum_{i=1}^{k} \mathbb{1}_{\mathcal{A}}(n + h_i) - m \Big) w(n) > 0 \tag{2.2.1}$$

holds for some integer $m \geq 1$, where $\mathbb{1}_{\mathcal{A}}$ denotes the indicator function of the set $\mathcal{A}$ and $w(n)$ are non-negative weights (cf. [11, 21, 24]). If we normalise the weights to sum to 1, then this is saying "if we choose n randomly from the interval $[N, 2N)$ with probability $w(n)$, then $\mathbb{E}[\mathbf{X}] > m$." From this we can deduce the existence of an $n \in [N, 2N)$ for which $m + 1$ of the translates $n + h_i \in \mathcal{A}$. We say such a translate has been "accepted." Exactly which translates are accepted is unknown. This is a limitation of the first moment method.

It is clear that for our model problem, we require more information about which translates $n + h$ appear. Namely, we need to be obtaining an accepted translate from each of the M bins $B_1, \ldots, B_M$ (recall $k = k_0 + \ldots + k_M$). This presents two obvious difficulties.

1. For any $1 \leq i \leq k$ the probability of the event $n + h_i \in \mathcal{A}$ depends on k, and tends to 0 as $k \to \infty$. This would mean any bin of *fixed* size expects to get fewer and fewer elements as k gets large. In particular, we cannot hope the hypotheses hold for every $M \geq 1$.

2. Even in the situation where $\mathbb{E}[\mathbf{X}_i] > 1$ holds for each $1 \leq i \leq M$, we cannot conclude anything about $\mathbb{P}((\mathbf{X}_1 > 0) \cap \ldots \cap (\mathbf{X}_M > 0))$ unless we input some information about the joint distribution of the bins.

We are able to overcome these issues by modifying the sieve weights and using a second moment estimate.

2.2.2 Choice of sieve weights

We solve the first problem by modifying the sieve weights to put more emphasis on the earlier bins. This way, we can guarantee that $\mathbb{P}(n + h \in \mathcal{A} | h \in B_i) = c_i$ where

the constant c_i depends solely on the bin. This also means that we can guarantee $\mathbb{E}[\mathbf{X}_i]$ is large for each i (provided k_i is large enough in terms of c_i). We will consider Maynard-Tao sieve weights with a fixed factorisation

$$w(n) = \Bigg(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i}} \prod_{i=1}^{M} \lambda^{(i)}_{d_{k_0+\dots+k_{i-1}+1},\dots,d_{k_0+\dots+k_i}} \Bigg)^2, \tag{2.2.2}$$

where

$$\lambda^{(i)}_{d_{k_0+\dots+k_{i-1}+1},\dots,d_{k_0+\dots+k_i}} \approx \Bigg(\prod_{j=k_0+\dots+k_{i-1}+1}^{k_0+\dots+k_i} \mu(d_j) \Bigg) f_i(d_{k_0+\dots+k_{i-1}+1}, \dots, d_{k_0+\dots+k_i}), \tag{2.2.3}$$

and f_i is a suitable smooth function supported on the simplex

$$R_{B_i,\beta_i} = \{(x_{k_0+\dots+k_{i-1}+1}, \dots, x_{k_0+\dots+k_i}) \in [0,1]^{k_i} : 0 \leq \sum_{j=k_0+\dots+k_{i-1}+1}^{k_0+\dots+k_i} x_j \leq \beta_i\}. \tag{2.2.4}$$

Here $(\beta_i)_{i\geq 1}$ is a sequence of real numbers such that $\sum_{i=1}^{\infty} \beta_i \leq 1$ (cf. the sieve weights defined in [21, Proposition 4.1]). We will take $\beta_i = 2^{-i}$, and in this instance one might say "we have allocated 50% of the sieve power to B_1."

2.2.3 Concentration of measure

We can deal with the second problem by showing the random variables $\mathbf{X}_i$ exhibit "enough" independence. This is precisely what concentration of measure arguments are used for. For example, an application of the union bound and Chebychev's inequality tells us that

$$\mathbb{P}(|\mathbf{X}_i - \mathbb{E}[\mathbf{X}_i]| < t_i \text{ for all } i) \geq 1 - \sum_{i=1}^{M} \frac{\mathbb{E}[\mathbf{X}_i - \mathbb{E}[\mathbf{X}_i]]^2}{t_i^2} \tag{2.2.5}$$

where $t_i \geq 1$ are concentration parameters. Thus, if we can show the variances $\mathbb{E}[\mathbf{X}_i - \mathbb{E}[\mathbf{X}_i]]^2$ are small, then we should be able to show each random variable concentrates in a (small) interval about its mean with high probability. In particular, we should be able to show that we get (at least) one accepted translate coming from each bin after the sieving process. We implement this analytically by using a second moment estimate (see Proposition 2.5.2).

Remark 2.2.1. A similar second moment estimate was considered by Banks, Freiberg and Maynard in their paper [2]. They showed a partition result (for primes), where the bins are allowed to grow with k. A key aspect of our work is that the bin sizes are fixed. Moreover they only needed upper bounds of the correct order of magnitude for the sieve sums, whereas we require precise asymptotics.

2.2.4 Hooley's ρ function.

In practice, utilising a second moment estimate requires an understanding of the two-point correlations

$$\sum_{N\leq n<2N} \rho_{\mathcal{A}}(n+h)\rho_{\mathcal{A}}(n+h') \tag{2.2.6}$$

where $\rho_{\mathcal{A}}$ is a non-negative function supported on $\mathcal{A}$. This means our methods are limited to cases in which estimates of the above type are known. In particular we cannot deal with the case of primes, as evaluating the above sum asymptotically with $\mathbb{1}_{\mathbb{P}}$ or the von Mangoldt function Λ (say) is equivalent to the twin prime conjecture.

One can do much better when working with sums of two squares. We cannot evaluate (2.2.6) asymptotically using the indicator function, but we can if we work with the representation function $r_2(n)$ instead. Unfortunately $r_2(n)$ is too large for our purposes, and it proves necessary to consider a weighted version instead. In Hooley's work [14] on the distribution of numbers representable as the sum of two squares, he considers a weighted representation function $\rho(n) = t(n)r_2(n)$ where

$$t(n) = t_{N,\theta_1}(n) = \sum_{\substack{a|n,\ a\leq v \\ p|a\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)}{g_2(a)}\left(1-\frac{\log a}{\log v}\right), \quad (v = N^{\theta_1}) \tag{2.2.7}$$

and θ_1 is a suitably small, fixed constant (for example Hooley takes $\theta_1 = 1/20$). Here $g_2(p)$ is the multiplicative function defined on primes by

$$g_2(p) = \begin{cases} 2-\frac{1}{p} & \text{if } p\equiv 1 \pmod 4, \\ \frac{1}{p} & \text{if } p\equiv 3 \pmod 4. \end{cases} \tag{2.2.8}$$

The $t(n)$ factor acts to dampen down the oscillations due to $r_2(n)$. Thus $\rho(n)$ acts a proxy for the indicator function $\mathbb{1}_{n=\square+\square}$ and moreover asymptotics for (2.2.6) are available for $\rho(n)$. This is the function we will be working with.

2.2.5 Outline of the chapter.

In Section 2.3 we deduce the results about quantum limits contained in Theorem's 2.1.5 and 2.1.6 from Theorem 2.1.3. In Section 2.5 we state a few preliminary lemmas that will be needed in the sieve calculations. We defer the proofs of these results to the Appendix. In Section 2.6 we state our main sieve results, and from them we deduce Theorem 2.1.4. We isolate a key lemma (see Lemma 2.6.6) from which all of our sieve estimates follow. Section 2.7 and Section 2.8 are dedicated to proving this lemma.

2.3 Proofs of quantum limit results

In this section we deduce the results of Theorem 2.1.5 and Theorem 2.1.6 from Theorem 2.1.3. Following [19], we note that φ_k is an eigenfunction of the Laplacian on $\mathbb{T}^d$ with eigenvalue $\lambda_k = 4\pi^2 n_k$ for some $n_k \in \mathbb{N}$ if and only if its Fourier expansion is of the form

$$\varphi_k(x) = \sum_{\substack{\xi \in \mathbb{Z}^d \\ |\xi|^2 = n_k}} a_\xi e^{2\pi i \langle \xi, x \rangle}, \tag{2.3.1}$$

for $a_\xi \in \mathbb{C}$. Moreover $\|\varphi_k\|_2 = 1$ if and only if $\sum_\xi |a_\xi|^2 = 1$. It follows that

$$\begin{aligned} |\varphi_k(x)|^2 &= \sum_{\tau \in \mathbb{Z}^d} b_\tau(k) e^{2\pi i \langle \tau, x \rangle}, \\ b_\tau(k) &= \sum_{\substack{\xi - \eta = \tau \\ |\xi|^2 = |\eta|^2 = n_k}} a_\xi \overline{a_\eta}. \end{aligned} \tag{2.3.2}$$

Let $\mathrm{d}v$ be a quantum limit on $\mathbb{T}^d$ with Fourier expansion as in (2.1.1). By $|\varphi_k|^2 \mathrm{d}x \to \mathrm{d}v$ weak-$*$ as $k \to \infty$ we mean that for every $\tau \in \mathbb{Z}^d$ we have $c_\tau = \lim_{k \to \infty} b_\tau(k)$.

Fix $a_1 < a_2 < \ldots$ and $M_1 < M_2 < \ldots$ as in the statement of Theorem 2.1.3, and let $b_j^{(k)}, c_j^{(k)} \in \mathbb{Z}$ be such

$$M_k = a_j^2 + (b_j^{(k)})^2 + (c_j^{(k)})^2, \quad (1 \leq j \leq k). \tag{2.3.3}$$

Let $\epsilon > 0$ be sufficiently small, and let $F = F_\epsilon : \mathbb{N} \to \mathbb{N}$ be a rapidly increasing function whose rate of growth will be specified later. As we are assuming both $a_i \to \infty$ and $r(a_i) \to \infty$, by passing to a subsequence if necessary (and relabelling the indices of the sequence M_k), we may suppose $a_i, r(a_i) \gg F(i)$.

We will require information about the number of integer points on the surface of the d-dimensional sphere. For this we recall the following results: writing $n = 2^k m$ and letting $\sigma(n) = \sum_{d|n} d$ denote the sum-of-divisors function, we have the identities

$$\begin{aligned} r_3(n^2) &= 6 \prod_{p^a || m} (\sigma(p^a) - (-1)^{\frac{p-1}{2}} \sigma(p^{a-1})), \\ r_4(n^2) &= 24\sigma(m^2), \\ r_d(n^2) &= C_d(n^2) n^{d-2} \quad \text{for} \quad d \geq 5. \end{aligned}$$

Here $C_d(n^2)$ is a singular series which satisfies $C_d(n^2) \asymp_d 1$.

We prove each statement similarly - in each case we consider a suitable sequence of L^2-normalised eigenfunctions with eigenvalues $\lambda_k = 4\pi^2 M_k$ and show that the limit has the desired property.

Proof of (Theorem 2.1.3 $\Rightarrow$ Theorem 2.1.5). Consider the sequence of L^2-normalised eigenfunctions on $\mathbb{T}^3$ that arise by choosing coefficients

$$a_\xi = \begin{cases} \sqrt{\frac{2^k}{2^k-1}} \cdot \frac{1}{2^{(j+1)/2}} & \text{if } \xi = (\pm a_j, b_j^{(k)}, c_j^{(k)}) \text{ for some } j, \\ 0 & \text{otherwise.} \end{cases}$$

Fix $i \geq 1$. With this choice, for any $k \geq i$ we obtain

$$b_{(2a_i,0,0)}(k) = \sum_{\substack{\xi-\eta=(2a_i,0,0) \\ |\xi|^2=|\eta|^2=M_k}} a_\xi \overline{a_\eta} = \frac{2^k}{2^k-1} \cdot \frac{1}{2^{i+1}},$$

because the a_i are distinct and so the only contribution to the sum comes from $\xi = (a_i, b_i^{(k)}, c_i^{(k)})$ and $\eta = (-a_i, b_i^{(k)}, c_i^{(k)})$. Hence

$$c_{(2a_i,0,0)} = \lim_{k\to\infty} b_{(2a_i,0,0)}(k) = \frac{1}{2^{i+1}} > 0,$$

which proves the theorem. □

Proof of (Theorem 2.1.3 $\Rightarrow$ Theorem 2.1.6). It suffices to prove part (i) for $d = 4$, by identifying the eigenfunctions on $\mathbb{T}^d$ with the eigenfunctions on $\mathbb{T}^{d+l}$ all of whose non-zero frequencies lie in the subspace $\{(x_1, \ldots, x_{d+l}) : x_{d+1} = \ldots = x_{d+l} = 0\} \subseteq \mathbb{Z}^{d+l}$.

Consider the sequence of L^2-normalised eigenvectors on $\mathbb{T}^4$ that arise by choosing

$$a_\xi = \begin{cases} \sqrt{\frac{2^k}{2^k-1}} \cdot \frac{1}{(2^j r(a_j^2))^{1/2}} & \text{if } \xi = (X, Y, b_j^{(k)}, c_j^{(k)}) \text{ for some } j \text{ and } X^2 + Y^2 = a_j^2, \\ 0 & \text{otherwise.} \end{cases}$$

Fix i and suppose $k \geq i$. From (2.3.2), and using positivity of the coefficients, we see that

$$b_\tau(k) \geq \frac{2^k}{2^k-1} \cdot \frac{1}{2^i r(a_i^2)} \cdot \sum_{\substack{\xi,\eta\in\mathbb{Z}^d \\ \xi-\eta=\tau \\ \xi=(X,Y,b_i^{(k)},c_i^{(k)}) \\ \eta=(X',Y',b_i^{(k)},c_i^{(k)})}} 1,$$

where $X^2+Y^2=(X')^2+(Y')^2=a_i^2$. Hence

$$|b_\tau(k)|^{2-\epsilon} \geq \left(\frac{2^k}{2^k-1}\right)^{2-\epsilon} \cdot \frac{(2^i r(a_i^2))^\epsilon}{4^i r(a_i^2)^2} \cdot \Bigg(\sum_{\substack{\xi,\eta\in\mathbb{Z}^d \\ \xi-\eta=\tau \\ \xi=(X,Y,b_i^{(k)},c_i^{(k)}) \\ \eta=(X',Y',b_i^{(k)},c_i^{(k)})}} 1 \Bigg)^{2-\epsilon}$$

$$\geq \left(\frac{2^k}{2^k-1}\right)^{2-\epsilon} \cdot \frac{(2^i r(a_i^2))^\epsilon}{4^i r(a_i^2)^2} \cdot \sum_{\substack{\xi,\eta\in\mathbb{Z}^d \\ \xi-\eta=\tau \\ \xi=(X,Y,b_i^{(k)},c_i^{(k)}) \\ \eta=(X',Y',b_i^{(k)},c_i^{(k)})}} 1.$$

Given two non-zero coefficients $a_\xi, a_{\xi'}$, corresponding to vectors of the form $\xi = (X, Y, b_i^{(k)}, c_i^{(k)})$ and $\xi' = (X', Y', b_i^{(k)}, c_i^{(k)})$, we see the difference vector is

$$\xi - \xi' = (X - X', Y - Y', 0, 0),$$

and the norm of this vector is $\leq 2a_i$ by the triangle inequality. It follows that if we sum $b_\tau(k)$ over all $|\tau| \leq 2a_i$ then we pick up all such differences, and there are $r(a_i^2)^2$ of them. From the lower bound above, we conclude that

$$\sum_{\substack{\tau\in\mathbb{Z}^d \\ |\tau|\leq 2a_i}} |b_\tau(k)|^{2-\epsilon} \geq \left(\frac{2^k}{2^k-1}\right)^{2-\epsilon} \cdot \frac{(2^i r(a_i^2))^\epsilon}{4^i}.$$

Taking the limit as $k \to \infty$ we conclude that

$$\sum_{\substack{\tau\in\mathbb{Z}^d \\ |\tau|\leq 2a_i}} |c_\tau|^{2-\epsilon} \geq \frac{(2^i r(a_i^2))^\epsilon}{4^i} \geq \frac{(2^i r(a_i))^\epsilon}{4^i} \gg \frac{(2^i F(i))^\epsilon}{4^i}.$$

Now we can choose $F = F_\epsilon$ so that the expression on the right hand side is unbounded as $i \to \infty$. It follows that $\sum_\tau |c_\tau|^{2-\epsilon}$ doesn't converge, proving part (i).

For part (ii), fix $d \geq 5$. We proceed as in part (i), except this time because $d \geq 5$ we have the lower bound $r_{d-2}(a_i^2) \gg_d a_i^{d-4}$. We remark that to obtain this bound for $d \in \{5, 6\}$ we are using property (2) given by Theorem 2.1.3. For $d \geq 7$ the bound holds without this extra assumption on our sequence.

Now consider the sequence of eigenvectors on $\mathbb{T}^d$ with densities

$$a_\xi = \begin{cases} \sqrt{\frac{2^k}{2^k-1}} \cdot \frac{1}{(2^j r_{d-2}(a_j^2))^{1/2}} & \text{if } \xi = (X_1, \ldots, X_{d-2}, b_j^{(k)}, c_j^{(k)}) \text{ for some } j \text{ and } X_1^2 + \\ & \ldots X_{d-2}^2 = a_j^2, \\ 0 & \text{otherwise.} \end{cases}$$

Fix i and suppose $k \geq i$. As above we can conclude

$$\sum_{\substack{\tau \in \mathbb{Z}^d \\ |\tau| \leq 2a_i}} |b_\tau(k)| \geq \left(\frac{2^k}{2^k - 1} \right) \cdot \frac{r_{d-2}(a_i^2)}{2^i}.$$

Taking the limit as $k \to \infty$ we conclude that

$$\sum_{\substack{\tau \in \mathbb{Z}^d \\ |\tau| \leq 2a_i}} |c_\tau| \geq \frac{r_{d-2}(a_i^2)}{2^i} \gg_d \frac{a_i^{d-4}}{2^i}.$$

It follows that

$$\frac{\sum_{|\tau| \leq 2a_i} |c_\tau|}{(2a_i)^{d-4-\epsilon}} \gg_d \frac{(2a_i)^\epsilon}{2^i} \gg_d \frac{(2F(i))^\epsilon}{2^i}.$$

Choosing $F = F_\epsilon$ appropriately and letting $i \to \infty$, we see that for this choice of quantum limit we have

$$\limsup_{\rho \to \infty} \frac{\Sigma(\rho)}{\rho^{d-4-\epsilon}} = +\infty,$$

where $\Sigma(\rho)$ is defined as in (2.1.2). This proves part (ii). □

2.4 Notation

We will use both Landau and Vinogradov asymptotic notation throughout this chapter. N will denote a large integer, and all asymptotic notation is to be understood as referring to the limit as $N \to \infty$. Any dependencies of the implied constants on other parameters A will be denoted by a subscript, for example $X \ll_A Y$ or $X = O_A(Y)$, unless stated otherwise. We let ϵ denote a small positive constant, and we adopt the convention it is allowed to change at each occurrence, and even within a line.

We will denote the non-trivial Dirichlet character (mod 4) by χ_4, and we may omit the subscript and simply write χ. As usual, we let $\varphi(n)$ denote the Euler-Totient function, $\tau_r(n)$ denote the number of ways of writing n as the product of r natural numbers, $\mu(n)$ denote the Möbius function, and $r_d(n)$ denote the number of representations of n as the sum of d squares. For the rest of the chapter we will write $r(n)$ when $d = 2$. For integers a, b we let (a, b) denote their highest common factor, and $[a, b]$ denote their lowest common multiple.

We define the Ramanujan-Landau constant

$$A = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \tag{2.4.1}$$

which will appear in many of our results.

2.5 Preliminaries

In this section, we formalise some of the notions discussed in Section 2, and state a few key estimates that will be required later in the sieve calculations.

2.5.1 A pigeonhole argument

The following proposition allows us to go from the set-up in Theorem 2.1.4 to the model problem discussed in Section 2.

Proposition 2.5.1 (Pigeonhole argument for infinite bin set-up)**.** *Fix $\mathcal{A} \subseteq \mathbb{N}$ and a set $\mathcal{H}^* = \{h_1, h_2, \ldots\}$ of integers. Suppose that there exists a partition $\mathcal{H}^* = B_1 \cup B_2 \cup \ldots$ where each bin B_i is a fixed, finite size, such that for every $M \geq 1$, there exists infinitely many n and M translates $n + h_{i,M} \in \mathcal{A}$ with $h_{i,M} \in B_i$ for $1 \leq i \leq M$. Then there exists increasing sequences a_j and n_k such that for every $k \geq 1$ we have $n_k + h_{a_j} \in \mathcal{A}$ for $1 \leq j \leq k$ and moreover $h_{a_j} \in B_j$ for all j.*

Proof. With the above set-up, obtain translates $n + h_{i,M} \in \mathcal{A}$ with $h_{i,M} \in B_i$ for $1 \leq i \leq M$ for each $M \geq 1$. Record this process in the following infinite table:

B_1	B_2	B_3	$\ldots$	B_M	B_{M+1}	$\ldots$
$h_{1,1}$			$\ldots$			
$h_{1,2}$	$h_{2,2}$		$\ldots$			
$h_{1,3}$	$h_{2,3}$	$h_{3,3}$	$\ldots$			
$\vdots$	$\vdots$	$\vdots$	$\vdots$			
$h_{1,M}$	$h_{2,M}$	$h_{3,M}$	$\ldots$	$h_{M,M}$		
$h_{1,M+1}$	$h_{2,M+1}$	$h_{3,M+1}$	$\ldots$	$h_{M,M+1}$	$h_{M+1,M+1}$	
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\vdots$	$\vdots$

Look at the first column. By the pigeonhole principle, since B_1 is finite, there must exist an element $h_{a_1} \in B_1$ which appears infinitely many times. Choose the smallest such h_{a_1}, and choose any $n_1 \in \mathbb{N}$ for which $n_1 + h_{a_1} \in \mathcal{A}$. Now erase all the rows that do not start with h_{a_1}, and look at the remaining (infinite) table. Again, since B_2 is finite, some element $h_{a_2} \in B_2$ must occur infinitely many times in the second column. Choose the smallest such h_{a_2}, and choose any $n_2 > n_1$ such that $n_2 + h_{a_2} \in \mathcal{A}$ (which we can do because there are infinitely many such n_2). By construction this n_2 will be such that $n_2 + h_{a_1} \in \mathcal{A}$. Now erase all rows that don't start with h_{a_1}, h_{a_2}, and repeat this process for B_3, and so on. We will end up with increasing sequences a_j and n_k which by construction satisfy the required conditions. □

2.5.2 A second moment estimate

As discussed in Section 2, our work will require input about the joint distribution of the bins, which we will achieve via concentration of measure arguments. The following second moment estimate will suffice for our purposes.

Proposition 2.5.2 (Second moment estimate)**.** *Fix $\mathcal{A} \subset \mathbb{N}$ and $\mathcal{H} = \{h_1, \dots, h_k\}$ a set of integers. Suppose we have a partition $\mathcal{H} = B_1 \cup \dots \cup B_M$. Let $\mu_i, t_i \geq 1$ be real numbers for $1 \leq i \leq M$. Let $\rho_{\mathcal{A}}$ be a non-negative function supported on $\mathcal{A}$ and $w(n)$ be non-negative weights for each integer n. If*

$$\sum_{N \leq n < 2N} \left[\min_{j=1,\dots,M} \frac{\mu_j^2}{t_j^2} - \sum_{i=1}^{M} \left(\frac{\sum_{h \in B_i} \rho_{\mathcal{A}}(n+h) - \mu_i}{t_i} \right)^2 \right] w(n) > 0, \tag{2.5.1}$$

then there exists an $n \in [N, 2N)$ and elements $h_{a_i} \in B_i$ such that $n + h_{a_i} \in \mathcal{A}$ for $1 \leq i \leq M$.

Proof. By positivity we deduce the existence of an $n \in [N, 2N)$ such that

$$\sum_{i=1}^{M} \left(\frac{\sum_{h \in B_i} \rho_{\mathcal{A}}(n+h) - \mu_i}{t_i} \right)^2 < \min_{j=1,\dots,M} \frac{\mu_j^2}{t_j^2}.$$

If $n + h \notin \mathcal{A}$ for all $h \in B_i$, then by assumption on the support of $\rho_{\mathcal{A}}$ the left hand side of the above expression is $\geq \mu_i^2/t_i^2$, a contradiction. □

Thus, if the second moment estimate (2.5.1) holds for all $M \geq 1$ and sufficiently large N, then we are in a situation where the hypotheses of Proposition 2.5.1 are satisfied.

2.5.3 Estimates in arithmetic progressions

We require an understanding of how $\rho(n)$ and $\rho(n)\rho(n+h)$ behaves in arithmetic progressions for our sieve calculations. Essentially this reduces down to understanding the corresponding sums for $r(n)$ and $r(n)r(n+h)$, where the estimates we need are known with power-saving error terms. This means that the error terms in the sieve calculations can be bounded trivially (cf. with the case of primes [21, 11], where we have to use equi-distribution results such as the Bombieri-Vinogradov theorem to bound the error terms that arise).

We have the following lemmas. We note that the functions $g_1, \dots, g_7$ defined in this section will be used frequently throughout the rest of the chapter.

Lemma 2.5.3. *Suppose $(a,q)=(d,q)=1$ where d,q are square-free and odd, of size $\ll N^{O(1)}$. Then we have*

$$\sum_{\substack{n\leq N\\ n\equiv a\ (mod\ q)\\ n\equiv 1\ (mod\ 4)\\ d|n}} r(n)=\frac{g_1(q)g_2(d)}{2qd}\pi N+R_1(N;d,q),$$

where g_2 is defined as in (2.2.8), g_1 is the multiplicative function defined on primes by $g_1(p)=1-\chi(p)/p$, and

$$R_1(N;d,q)\ll_\epsilon ((qd)^{\frac{1}{2}}+N^{\frac{1}{3}})d^{\frac{1}{2}}N^\epsilon$$

Lemma 2.5.4. *Suppose that $(a,q)=(a+h,q)=(d_1,q)=(d_2,q)=(d_1,d_2)=1$ and $4|h$, where d_1,d_2,q are square-free and odd, of size $\ll N^{O(1)}$. Moreover suppose $h>0$ is fixed such that $p|h\Rightarrow p|2q$. Then we have*

$$\sum_{\substack{n\leq N\\ n\equiv a\ (mod\ q)\\ n\equiv 1\ (mod\ 4)\\ d_1|n\\ d_2|n+h}} r(n)r(n+h)=\frac{g_1(q)^2\Gamma(d_1,d_2,q)}{q}\pi^2N+R_2(N;d_1,d_2,q),$$

where

$$\Gamma(d_1,d_2,q)=\frac{g_2(d_1)g_2(d_2)}{d_1d_2}\sum_{(r,2q)=1}\frac{\mu(r)(d_1,r)(d_2,r)\chi[(d_1^2,r)]\chi[(d_2^2,r)]}{r^2},$$

and

$$R_2(N;d_1,d_2,q)\ll_\epsilon q^{\frac{1}{2}}d_1d_2N^{\frac{3}{4}+\epsilon}+d_1^{\frac{1}{2}}d_2^{\frac{1}{2}}N^{\frac{5}{6}+\epsilon}.$$

Lemma 2.5.5. *Let $(a,q)=(d,q)=1$ where d,q are square-free and odd, of size $\ll N^{O(1)}$. Then we have*

$$\sum_{\substack{n\leq N\\ n\equiv a\ (mod\ q)\\ n\equiv 1\ (mod\ 4)\\ d|n}} r^2(n)=\frac{g_3(q)g_4(d)}{qd}\bigg(\log N+A_2+2\sum_{p|q}g_5(p)-2\sum_{p|d}g_6(p)\bigg)N+O_\epsilon(qN^{\frac{3}{4}+\epsilon}),$$

where

$$A_2=2\gamma-1+2\frac{L'(1,\chi_4)}{L(1,\chi_4)}-2\frac{\zeta'(2)}{\zeta(2)}+\frac{4}{3}\log 2.$$

Here g_3,g_4 are the multiplicative functions defined on primes by

$$g_3(p)=\begin{cases}\frac{(p-1)^2}{p(p+1)} & \text{if } p\equiv 1\ (mod\ 4),\\ g_1(p) & \text{if } p\equiv 3\ (mod\ 4),\end{cases}\qquad g_4(p)=\begin{cases}\frac{4p^2-3p+1}{p(p+1)} & \text{if } p\equiv 1\ (mod\ 4),\\ g_2(p) & \text{if } p\equiv 3\ (mod\ 4),\end{cases}$$

and $g_5(p), g_6(p)$ *are defined by*

$$g_5(p) = \begin{cases} \frac{(2p+1)\log p}{p^2-1} & \text{if } p \equiv 1 \ (mod\ 4), \\ \frac{\log p}{p^2-1} & \text{if } p \equiv 3 \ (mod\ 4), \end{cases} \qquad g_6(p) = \begin{cases} \frac{(p-1)^2(2p+1)\log p}{(p+1)(4p^2-3p+1)} & \text{if } p \equiv 1 \ (mod\ 4), \\ \log p & \text{if } p \equiv 3 \ (mod\ 4). \end{cases}$$

We will prove each of these results in Appendix A. Lemma 2.5.3 follows from two known results. Lemma 2.5.4 follows by adapting the method used by Plaksin in [23], where a similar sum is considered. Finally Lemma 2.5.5 can be shown using standard Perron's formula arguments, together with a fourth moment estimate for Dirichlet L-functions.

When finding the corresponding estimates for $\rho(n)$ the following sums naturally appear (for the definitions of W, W_1 and D_0 see (2.6.1) below the fold):

$$X_{N,W} = \sum_{\substack{a \leq v \\ (a,W)=1 \\ p|a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)}{a} \log \frac{v}{a}, \tag{2.5.2}$$

$$Y_{N,W} = \sum_{\substack{a,b \leq v \\ (a,W)=(b,W)=1 \\ (a,b)=1 \\ p|a,b \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)}{g_7(a)g_7(b)} \log \frac{v}{a} \log \frac{v}{b}, \tag{2.5.3}$$

$$Z^{(1)}_{N,W} = \sum_{\substack{a,b \leq v \\ (a,W)=(b,W)=1 \\ p|a,b \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log \frac{v}{a} \log \frac{v}{b}, \tag{2.5.4}$$

$$Z^{(2)}_{N,W} = \sum_{\substack{a,b \leq v \\ (a,W)=(b,W)=1 \\ p|a,b \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log \frac{v}{a} \log \frac{v}{b} \sum_{p|[a,b]} g_6(p). \tag{2.5.5}$$

Here g_7 is the multiplicative function defined on primes by $g_7(p) = p+1$. The following lemma evaluates the auxiliary sums above.

Lemma 2.5.6 (Auxiliary estimates for $\rho(n)$)**.** *We have*

$$X_{N,W} = (1+o(1))\frac{8A\log^{\frac{1}{2}} v}{\pi g_1(W_1)},$$

$$Y_{N,W} = (1+o(1))\frac{64A^2\log v}{\pi^2 g_1(W_1)^2},$$

$$Z^{(1)}_{N,W} = (1+o(1))\frac{32A^3\log^{\frac{1}{2}} v}{\pi^2 g_1(W_1)^3},$$

$$Z^{(2)}_{N,W} = -(1+o(1))\frac{16A^3\log^{\frac{3}{2}} v}{\pi^2 g_1(W_1)^3},$$

where A is defined as in (2.4.1). In each case one may take the $o(1)$ term to be $O(D_0^{-1})$.

We remark that the estimate for $X_{N,1}$ appears in Hooley's work (after correcting a misprint - cf. [14, Lemma 5] and note his slightly different definition of A). We prove Lemma 2.5.6 in Appendix B. Each sum can be evaluated by the Selberg-Delange method.

2.6 The sieve set-up

We now state our sieve results and use them to deduce Theorem 2.1.4. For the rest of the chapter, k is fixed, $\mathcal{H} = \{h_1, \dots, h_k\}$ is a fixed admissible set such that $4|h_i$ for each i, and N is sufficiently large in terms of any fixed quantity. We allow any of the constants hidden in the Landau notation to depend on k, without explicitly specifying so.

We will employ a $4W$-trick in our sieve calculations. Let

$$W = \prod_{2<p\leq D_0} p, \tag{2.6.1}$$

where $D_0 = (\log\log N)^3$, so that $W \ll (\log N)^{2(\log\log N)^2} \ll_\epsilon N^\epsilon$ for any fixed $\epsilon > 0$ by the prime number theorem. It will prove useful to define

$$W_1 = \prod_{\substack{p\leq D_0 \\ p\equiv 1 \pmod 4}} p, \qquad W_3 = \prod_{\substack{p\leq D_0 \\ p\equiv 3 \pmod 4}} p, \tag{2.6.2}$$

so that $W = W_1 W_3$.

By admissibility of $\mathcal{H}$ there exists a fixed residue class $v_0 \pmod W$ such that $(v_0 + h_i, W) = 1$ for each i. Fix $1 \leq m, l \leq k$ with $m \neq l$. We consider four types of

sums:

$$S_1 = \sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W \\ n\equiv 1 \pmod 4}} \Big(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i \ \forall i}} \lambda_{d_1,\dots,d_k} \Big)^2, \tag{2.6.3}$$

$$S_2^{(m)} = \sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W \\ n\equiv 1 \pmod 4}} \rho(n+h_m) \Big(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i \ \forall i}} \lambda_{d_1,\dots,d_k} \Big)^2, \tag{2.6.4}$$

$$S_3^{(m,l)} = \sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W \\ n\equiv 1 \pmod 4}} \rho(n+h_m)\rho(n+h_l) \Big(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i \ \forall i}} \lambda_{d_1,\dots,d_k} \Big)^2, \tag{2.6.5}$$

$$S_4^{(m)} = \sum_{\substack{N\le n<2N \\ n\equiv v_0 \pmod W \\ n\equiv 1 \pmod 4}} \rho^2(n+h_m) \Big(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i \ \forall i}} \lambda_{d_1,\dots,d_k} \Big)^2. \tag{2.6.6}$$

Because k is fixed, we may assume that D_0 is sufficiently large so that

$$p|h_i - h_j \Rightarrow p|2W. \tag{2.6.7}$$

Remark 2.6.1. For the second moment estimate, it proves important to control the residue classes of the translates $n+h \pmod 4$, hence the condition $n \equiv 1 \pmod 4$ in our sieve sums and also the assumption $4|h$ for our admissible set. This is because of the inherent bias numbers representable as a sum of two squares have modulo 4.

Our first Proposition evaluates these sums for general half-dimensional Maynard-Tao sieve weights. Fix $0 < \theta_1 < 1/18$ in the definition of $\rho(n)$ (see (2.2.7)). We also define the normalisation constant

$$B = \frac{A}{\Gamma(1/2)\sqrt{L(1,\chi_4)}} \cdot \frac{\varphi(W_3)(\log R)^{\frac{1}{2}}}{W_3} = \frac{2A}{\pi} \cdot \frac{\varphi(W_3)(\log R)^{\frac{1}{2}}}{W_3}. \tag{2.6.8}$$

Proposition 2.6.2 (Half-dimensional Maynard-Tao sieve estimates)**.** *Let $R = N^{\theta_2/2}$ for some small fixed positive constant θ_2 such that $0 < \theta_1 + \theta_2 < 1/18$. Let $\lambda_{d_1,\dots,d_k}$ be defined in terms of a fixed smooth function F by*

$$\lambda_{d_1,\dots,d_k} = \Big(\prod_{i=1}^k \mu(d_i) d_i \Big) \sum_{\substack{r_1,\dots,r_k \\ d_i \mid r_i \forall i \\ (r_i,W)=1 \forall i \\ p\mid r_i \Rightarrow p\equiv 3 \ (mod\ 4) \forall i}} \frac{\mu(\prod_{i=1}^k r_i)^2}{\prod_{i=1}^k \varphi(r_i)} F\Big(\frac{\log r_1}{\log R}, \dots, \frac{\log r_k}{\log R} \Big),$$

whenever $\prod_{i=1}^k d_i \leq R$ *is squarefree,* $(\prod_{i=1}^k d_i, W) = 1$ *and* $p|\prod_{i=1}^k d_i \Rightarrow p \equiv 3 \ (mod\ 4)$*, and let* $\lambda_{d_1,\dots,d_k} = 0$ *otherwise. Moreover let* F *be supported on* $R_k = \{(x_1,\dots,x_k) \in [0,1]^k : \sum_{i=1}^k x_i \leq 1\}$*. Then we have*

$$\begin{aligned}
S_1 &= (1+o(1))\frac{B^k N}{4W} L_k(F),\\
S_2^{(m)} &= (1+o(1))\frac{4\sqrt{\frac{\log R}{\log v}} B^k N}{\pi W} L_{k;m}(F),\\
S_3^{(m,l)} &= (1+o(1))\frac{64(\frac{\log R}{\log v}) B^k N}{\pi^2 W} L_{k;m,l}(F),\\
S_4^{(m)} &= (1+o(1))\frac{2\sqrt{\frac{\log R}{\log v}}(\frac{\log N}{\log v}+1) B^k N}{\pi W} L_{k;m}(F)
\end{aligned}$$

provided $L_k(F), L_{k;m}(F)$ *and* $L_{k;m,l}(F)$ *are non-zero, where*

$$\begin{aligned}
L_k(F) &= \int_0^1 \dots \int_0^1 \Big[F(x_1,\dots,x_k)\Big]^2 \prod_{i=1}^k \frac{\mathrm{d}x_i}{\sqrt{x_i}}\\
L_{k;m}(F) &= \int_0^1 \dots \int_0^1 \Big[\int_0^1 F(x_1,\dots,x_k)\frac{\mathrm{d}x_m}{\sqrt{x_m}}\Big]^2 \prod_{\substack{i=1\\ i\neq m}}^k \frac{\mathrm{d}x_i}{\sqrt{x_i}},\\
L_{k;m,l}(F) &= \int_0^1 \dots \int_0^1 \Big[\int_0^1 \Big(\int_0^1 F(x_1,\dots,x_k)\frac{\mathrm{d}x_m}{\sqrt{x_m}}\Big)\frac{\mathrm{d}x_l}{\sqrt{x_l}}\Big]^2 \prod_{\substack{i=1\\ i\neq m,l}}^k \frac{\mathrm{d}x_i}{\sqrt{x_i}}.
\end{aligned}$$

From this, one can deduce the corresponding results for the modification of the Maynard-Tao sieve described in Section 2.

Proposition 2.6.3 (Modified Maynard-Tao sieve estimates)**.** *Suppose in addition to the hypotheses of Proposition 2.6.2 we have a partition* $\mathcal{H} = \{h_1,\dots,h_k\} = B_1 \cup \dots \cup B_M$ *into bins* B_i *of fixed and finite size* k_i*. Write* $B_i = \{h_{k_0+\dots+k_{i-1}+1},\dots,h_{k_0+\dots+k_i}\}$ *with the convention that* $k_0 = 0$*. Suppose further we have a corresponding factorisation*

$$F(x_1,\dots,x_k) = \prod_{i=1}^M F_i(x_{k_0+\dots+k_{i-1}+1},\dots,x_{k_0+\dots+k_i}),$$

where each F_i *is smooth and supported on the simplex*

$$R_{B_i,\beta_i} = \{(x_{k_0+\dots+k_{i-1}+1},\dots,x_{k_0+\dots+k_i}) \in [0,1]^{k_i} : 0 \leq \sum_{j=k_0+\dots+k_{i-1}+1}^{k_0+\dots+k_i} x_j \leq \beta_i\}.$$

Here $(\beta_i)_{i=1}^{\infty}$ is a sequence of real numbers such that $\sum_{i=1}^{\infty}\beta_i \leq 1$. Then for $h_m, h_l \in B_j$ we have

$$\begin{aligned}
S_1 &= (1+o(1))\frac{B^k N}{4W}\Big(\prod_{i=1}^{M} L_{|B_i|}(F)\Big),\\
S_2^{(m)} &= (1+o(1))\frac{4\sqrt{\frac{\log R}{\log v}}B^k N}{\pi W}\Big(\prod_{i=1}^{M} L_{|B_i|}(F_i)\Big)\frac{L_{|B_j|;m}(F_j)}{L_{|B_j|}(F_j)},\\
S_3^{(m,l)} &= (1+o(1))\frac{64(\frac{\log R}{\log v})B^k N}{\pi^2 W}\Big(\prod_{i=1}^{M} L_{|B_i|}(F_i)\Big)\frac{L_{|B_j|;m,l}(F_j)}{L_{|B_j|}(F_j)},\\
S_4^{(m)} &= (1+o(1))\frac{2\sqrt{\frac{\log R}{\log v}}(\frac{\log N}{\log v}+1)B^k N}{\pi W}\Big(\prod_{i=1}^{M} L_{|B_i|}(F_i)\Big)\frac{L_{|B_j|;m}(F_j)}{L_{|B_j|}(F_j)}.
\end{aligned}$$

Proof. The hypotheses imply $F = \prod_{i=1}^{M} F_i$ is also smooth and supported on R_k, and hence the results of Proposition 2.6.2 apply. It suffices to to show the functionals factorise in the forms stated. Because our set-up ensures that $\mathrm{supp}(F) = \mathrm{supp}(F_1) \times \ldots \times \mathrm{supp}(F_M)$ one can easily check that if $h_m, h_l \in B_j$ then

$$\begin{aligned}
L_k(F) &= \prod_{i=1}^{M} L_{|B_i|}(F_i),\\
L_{k;m}(F) &= \Big(\prod_{i=1}^{M} L^{(0)}_{|B_i|}(F_i)\Big)\frac{L_{|B_j|:m}(F_j)}{L_{|B_j|}(F_j)},\\
L_{k;m,l}(F) &= \Big(\prod_{i=1}^{M} L^{(0)}_{|B_i|}(F_i)\Big)\frac{L_{|B_j|:m,l}(F_j)}{L_{|B_j|}(F_j)}.
\end{aligned}$$

□

With the following lemma we will be in a position to prove Theorem 2.1.4.

Lemma 2.6.4 (Evaluation of sieve functionals)**.** *Let $F(t_1,\ldots,t_k) = \prod_{i=1}^{k} g(kt_i)$ where*

$$g(t) = \begin{cases} \frac{1}{1+\frac{t}{\beta}}, & \text{if } t \leq \beta,\\ 0, & \text{otherwise.}\end{cases}$$

Then for any m, l we have

$$\begin{aligned}
\frac{L_{k;m}(F)}{L_k(F)} &= \frac{\pi^2}{\pi+2}\cdot\sqrt{\frac{\beta}{k}},\\
\frac{L_{k:m,l}(F)}{L_k(F)} &= \Big(\frac{\pi^2}{\pi+2}\Big)^2\cdot\frac{\beta}{k}.
\end{aligned}$$

Proof. The definition implies F is supported on the cube $[0, \frac{\beta}{k}]^k \subseteq R_{k,\beta}$. In this case the functionals factorise completely and the lemma follows from the fact

$$\int_0^{\frac{\beta}{k}} \frac{\mathrm{d}t}{\sqrt{t}(1+\frac{kt}{\beta})^2} = \frac{\pi+2}{4} \cdot \sqrt{\frac{\beta}{k}},$$
$$\int_0^{\frac{\beta}{k}} \frac{\mathrm{d}t}{\sqrt{t}(1+\frac{kt}{\beta})} = \frac{\pi}{2} \cdot \sqrt{\frac{\beta}{k}}.$$

□

Remark 2.6.5. We have restricted the support of our functions to the cube $[0, \frac{\beta}{k}]^k \subseteq R_{k,\beta}$ so that the integrals can be evaluated exactly. This essentially means we are using weights of similar strength to the original GPY weights (cf. [11]). For the half-dimensional case one can show that for large k these weights are essentially optimal. (In particular, following a similar optimisation process as in [21, Section 7] one arrives at the same results as above.)

We are now in a position to prove Theorem 2.1.4.

Proof of Theorem 2.1.4. Let $\mathcal{H} = \{h_1, h_2, \ldots\}$ be a fixed admissible set. Fix real numbers θ_1, θ_2 subject to $0 < \theta_1 + \theta_2 < 1/18$ and define the constant

$$\Delta = \Delta(\theta_1, \theta_2) = \frac{\sqrt{2}(\pi+2)}{32\pi} \frac{1+\theta_1}{\sqrt{\theta_1\theta_2}}.$$

With notation as above, consider a partition $\mathcal{H} = B_1 \cup B_2 \cup \ldots$ where $k_1 > 2\Delta^3$ and for $i \geq 2$ we choose B_i such that $k_i > 2^{7i}$. By Proposition 2.5.2 we will be done if we can show, for every $M \geq 1$, the inequality

$$\sum_{\substack{N \leq n < 2N \\ n \equiv v_0 \pmod W \\ n \equiv 1 \pmod 4}} \Big[\min_{j=1,\ldots,M} \frac{\mu_j^2}{t_j^2} - \sum_{i=1}^{M} \Big(\frac{\sum_{h \in B_i} \rho(n+h) - \mu_i}{t_i} \Big)^2 \Big] \Big(\sum_{\substack{d_1,\ldots,d_k \\ d_i \mid n+h_i \ \forall i}} \lambda_{d_1,\ldots,d_k} \Big)^2 > 0 \tag{2.6.9}$$

for all sufficiently large N and some choice of real numbers $\mu_i, t_i \geq 1$. Choose weights $\lambda_{d_1,\ldots,d_k}$ as in Proposition 2.6.2, and let $F(x_1, \ldots, x_k) = \prod_{i=1}^M F_i(x_{k_0+\ldots+k_{i-1}+1}, \ldots, x_{k_0+\ldots+k_i})$ where each F_i is supported on $R_{B_i, 2^{-i}}$. Let $F_i(x_{k_0+\ldots+k_{i-1}+1}, \ldots, x_{k_0+\ldots+k_i}) = \prod_{j=k_0+\ldots+k_{i-1}+1}^{k_0+\ldots+k_i} g(k_i x_j)$ where for $j \in \{b_{2i-1}, \ldots, b_{2i}\}$ we define

$$g(x_j) = \begin{cases} \frac{1}{1+2^i x_j}, & \text{if } x_j \leq 2^{-i} \\ 0, & \text{otherwise} \end{cases}$$

Expanding out (2.6.9), we have to evaluate the expression

$$\Big(\min_{j=1,\dots,M}\frac{\mu_j^2}{t_j^2}\Big)S_1-\sum_{i=1}^{M}\frac{1}{t_i^2}\Big[\sum_{\substack{h,h'\in B_i\\ h\neq h'}}S_3^{(h,h')}+\sum_{h\in B_i}S_4^{(h)}-2\mu_i\sum_{h\in B_i}S_2^{(h)}+\mu_i^2S_1\Big]$$

(where by abuse of notation we have written $S_2^{(h)}$ for $S_2^{(i)}$ where $h=h_i$ say). A convenient choice of μ_i,λ_i is

$$\mu_i=c\Big(\frac{k_i}{2^i}\Big)^{\frac{1}{2}},\quad t_i=c\Big(\frac{k_i}{2^i}\Big)^{\frac{1}{3}},$$

where

$$c=c(\theta_1,\theta_2)=\frac{16\sqrt{\theta_2/2\theta_1}}{\pi}\Big(\frac{\pi^2}{\pi+2}\Big).$$

Evaluating these sums using Proposition 2.6.3 and Lemma 2.6.4 we see that this is asymptotically

$$\frac{B^kN}{4W}\Big(\prod_{i=1}^{M}L^{(0)}_{|B_i|}(F)\Big)\Big\{\Big(\frac{k_1}{2}\Big)^{\frac{1}{3}}-\sum_{i=1}^{M}\Big[\Delta\Big(\frac{2^i}{k_i}\Big)^{\frac{1}{6}}-\frac{1}{2^i}\Big(\frac{2^i}{k_i}\Big)^{\frac{2}{3}}\Big]\Big\}.$$

Hence (2.6.9) will be satisfied for all sufficiently large N provided

$$\Delta\sum_{i=1}^{M}\Big(\frac{2^i}{k_i}\Big)^{\frac{1}{6}}<\Big(\frac{k_1}{2}\Big)^{\frac{1}{3}}. \tag{2.6.10}$$

But now our choice of bins ensures that

$$\Delta\sum_{i=1}^{M}\Big(\frac{2^i}{k_i}\Big)^{\frac{1}{6}}\leq\Delta\sum_{i=1}^{M}\frac{1}{2^i}\leq\Delta<\Big(\frac{k_1}{2}\Big)^{\frac{1}{3}},$$

and so (2.6.10) is satisfied for all $M\geq 1$. □

It remains to prove Proposition 2.6.2. Each sum can be treated similarly. The following lemma handles all of them at once. First, given a function F satisfying the hypotheses of Proposition 2.6.2, we define

$$F_{\max}=\sup_{(t_1,\dots,t_k)\in[0,1]^k}\Big(|F(t_1,\dots,t_k)|+\sum_{i=1}^{k}|\frac{\partial F}{\partial t_i}(t_1,\dots,t_k)|\Big). \tag{2.6.11}$$

The lemma can now be stated as follows.

Lemma 2.6.6 (General sieve lemma)**.** *Let $J \subseteq \{1,\dots,k\}$ (possibly empty) and $p_1, p_2 \in \mathbb{P} \cup \{1\}$ be fixed. Write $I = \{1,\dots,k\}\backslash J$. Define the sieve sum $S_{J,p_1,p_2,m} = S_{J,p_1,p_2,m,f,g}$ by*

$$S_{J,p_1,p_2,m} = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime} \\ p_1 | d_m, p_2 | e_m}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\in I} f([d_i,e_i]) \prod_{j\in J} g([d_j,e_j]),$$

with weights $\lambda_{d_1,\dots,d_k}$ defined as in Proposition 2.6.2. If $J = \emptyset$ we define $f(p) = 1/p$ (and there is no dependence on g in the sum). Otherwise, f and g are non-zero multiplicative functions defined on primes by

$$f(p) = \frac{1}{p} + O\left(\frac{1}{p^2}\right), \;\; g(p) = \frac{1}{p^2} + O\left(\frac{1}{p^3}\right),$$

and moreover we assume that $f(p) \neq 1/p$. We write S_J for $S_{J,1,1,m}$. Suppose $\lambda_{d_1,\dots,d_k}$ satisfy the same hypotheses as in Proposition 2.6.2. Then for $|J| \in \{0,1,2\}$ we have the following:

(i) If $m \in J$ then

$$S_{J,p_1,p_2,m} \ll \frac{F_{max}^2 B^{k+|J|}(\log\log R)^2}{(p_1p_2/(p_1,p_2))^2}.$$

(ii) If $m \notin J$ then

$$S_{J,p_1,p_2,m} \ll \frac{F_{max}^2 B^{k+|J|}(\log\log R)^2}{p_1p_2/(p_1,p_2)}.$$

(iii) We have

$$S_J = (1+o(1))B^{k+|J|}L_J(F),$$

where the integral operators are defined by Proposition 2.6.2 above, and we write $L_J(F)$ as shorthand for $L_{k;j\in J}(F)$.

We now show how this implies Proposition 2.6.2.

Proof of (Lemma 2.6.6 ⇒ Proposition 2.6.2). We consider each sum in turn. First we note that using the definition of $\lambda_{d_1,\dots,d_k}$, the exact same calculation as in [21, p. 394] gives

$$\sup_{d_1,\dots,d_k} |\lambda_{d_1,\dots,d_k}| \ll F_{\max} \sum_{\substack{u\leq R \\ p|u \Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)\tau_k(u)}{\varphi(u)} \ll F_{\max}(\log R)^{\frac{k}{2}},$$

and so we have a trivial bound[1]

$$\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} |\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}| \ll \Big(\sup_{d_1,\dots,d_k} |\lambda_{d_1,\dots,d_k}|\Big)^2 \Big(\sum_{\substack{d\le R\\ p|d\Rightarrow p\equiv 3 \pmod 4}} \tau_k(d)\Big)^2$$
$$\ll F_{\max}^2 R^2 (\log R)^{2k} \ll_\epsilon F_{\max}^2 N^{\theta_2+\epsilon}. \tag{2.6.12}$$

As mentioned in Section 4, because we can obtain power-saving in the error terms for the formulae stated there, this trivial bound will suffice for our purposes.

(i) Rewrite S_1 in the form

$$S_1 = \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N\le n<2N\\ n\equiv v_0 \pmod W\\ n\equiv 1 \pmod 4\\ n\equiv -h_i \pmod{[d_i,e_i]}}} 1.$$

We may assume $W, [d_1, e_1], \dots, [d_k, e_k]$ are pairwise coprime, as otherwise the inner sum is empty. In this case, by the Chinese Remainder Theorem, these congruences are equivalent to a single congruence (mod q) where $q = 4W\prod_{i=1}^k [d_i, e_i]$. The inner sum evaluates to

$$\frac{N}{q} + O(1).$$

The error term contributes $O_\epsilon(F_{\max}^2 N^{\theta_2+\epsilon})$ which is negligible. The main term is

$$\frac{N}{4W} \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime}}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i=1}^k \frac{1}{[d_i,e_i]}.$$

This is of the form S_J where $|J| = 0$. Evaluating it according to Lemma 2.6.6 we obtain

$$S_1 = (1+o(1))\frac{B^k N}{4W} L_k^{(0)}(F).$$

[1]By Rankin's trick we have

$$\sum_{\substack{d\le R\\ p|d\Rightarrow p\equiv 3 \pmod 4}} \tau_k(d) \le R \sum_{\substack{d\le R\\ p|d\Rightarrow p\equiv 3 \pmod 4}} \frac{\tau_k(d)}{d} \ll R(\log R)^{k/2}.$$

(ii) Rewrite $S_2^{(m)}$ in the form

$$S_2^{(m)} = \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N\le n<2N\\ n\equiv v_0 \pmod W\\ n\equiv 1 \pmod 4\\ n\equiv -h_i \pmod{[d_i,e_i]}\ \forall i}} \rho(n+h_m).$$

By definition of $\rho(n+h_m)$ this is equal to

$$\frac{1}{\log v}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{a\le v\\ p\mid a\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)}{g_2(a)}\log\frac{v}{a} \sum_{\substack{N\le n<2N\\ n\equiv v_0 \pmod W\\ n\equiv 1 \pmod 4\\ n\equiv -h_i \pmod{[d_i,e_i]}\ \forall i\\ n\equiv -h_m \pmod a}} r(n+h_m).$$

From considering the support of $\lambda_{d_1,\dots,d_k}$ we see that for non-zero contribution we may assume $W, [d_1,e_1],\dots,[d_k,e_k]$ and a are pairwise coprime. In this case the inner sum can be evaluated according to Lemma 2.5.3, taking $q = W\prod_{i\neq m}[d_i,e_i]$ and $d = a[d_m,e_m]$. As $q \ll WR^2 \ll_\epsilon N^{\theta_2+\epsilon}$ and $d \ll vR^2 \ll N^{\theta_1+\theta_2}$ we see that the inner sum evaluates to

$$\frac{g_1(q)g_2(d)}{2qd}\pi N + O_\epsilon(N^{\frac{1}{3}+\frac{1}{2}(\theta_1+\theta_2)+\epsilon}).$$

Bounding the sum over a trivially by $v\log v$ and using (2.6.12), we see the error term contributes $O_\epsilon(N^{\frac{1}{3}+\frac{3}{2}(\theta_1+\theta_2)+\epsilon})$ which is negligible. We obtain a main term

$$\frac{X_{N,W}g_1(W)\pi N}{2W\log v} \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime}}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\prod_{i\neq m}\frac{g_1([d_i,e_i])}{[d_i,e_i]}\frac{1}{[d_m,e_m]^2},$$

where we have defined

$$X_{N,W} = \sum_{\substack{a\le v\\ (a,W)=1\\ p\mid a\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)}{a}\log\frac{v}{a}$$

as in (2.5.2). The sieve sum above is of the form S_J with $|J|=1$. We can evaluate this by Lemma 2.6.6 to obtain

$$S_2^{(m)} = (1+o(1))\frac{X_{N,W}g_1(W)\pi B^{k+1}N}{2W\log v}L_{k;m}^{(1)}(F).$$

Recalling the definition of B in (2.6.8), evaluating $X_{N,W}$ according to Lemma 2.5.6, and using the fact

$$\frac{g_1(W_3)\varphi(W_3)}{W_3} = \prod_{p\mid W_3}\left(1-\frac{1}{p^2}\right) = \frac{1}{2A^2}+O(D_0^{-1}),$$

we obtain

$$S_2^{(m)} = (1+o(1))\frac{4\sqrt{\frac{\log R}{\log v}}B^k N}{\pi W}L_{k;m}^{(1)}(F).$$

(iii) Rewrite $S_3^{(m,l)}$ in the form

$$S_3^{(m,l)} = \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N\le n<2N\\ n\equiv v_0 \pmod W\\ n\equiv 1 \pmod 4\\ n\equiv -h_i \pmod{[d_i,e_i]}\ \forall i}} \rho(n+h_m)\rho(n+h_l).$$

Expanding out the definition of ρ this is

$$\frac{1}{\log^2 v}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{a,b\le v\\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)}{g_2(a)g_2(b)}\log\frac{v}{a}\log\frac{v}{b}$$
$$\cdot \sum_{\substack{N\le n<2N\\ n\equiv v_0 \pmod W\\ n\equiv 1 \pmod 4\\ n\equiv -h_i \pmod{[d_i,e_i]}\ \forall i\\ n\equiv -h_m \pmod a\\ n\equiv -h_l \pmod b}} r(n+h_m)r(n+h_l).$$

Similarly to the above, for non-zero contribution we may restrict to the case $W, [d_1,e_1],\dots,[d_k,e_k], a, b$ are pairwise coprime (note that the last two congruences are solvable if and only if $(a,b)|h_l-h_m$, and in the case $(a,2W)=(b,2W)=1$ this is true if and only if $(a,b)=1$). We evaluate the inner sum according to Lemma 2.5.4. Using the same notation as in the statement of the lemma, we take $q = W\prod_{i\neq m,l}[d_i,e_i]$, $d_1 = a[d_m,e_m]$ and $d_2 = b[d_l,e_l]$. We note that $q \ll_\epsilon N^{\theta_2+\epsilon}$ and $d_1, d_2 \ll N^{\theta_1+\theta_2}$. Using the fact $\theta_1+\theta_2 < 1/18$, we see the second error term in the definition of $R_2(N;d_1,d_2,q)$ dominates, and so the inner sum evaluates to

$$\frac{g_1(q)^2\Gamma(d_1,d_2,q)}{q}\pi^2 N + O_\epsilon(N^{\frac{5}{6}+\theta_1+\theta_2+\epsilon}).$$

Bounding the rest of the sum trivially, we obtain a total error of size $O_\epsilon(N^{\frac{5}{6}+3\theta_1+2\theta_2+\epsilon})$ which, again, is negligible in the range $\theta_1+\theta_2<1/18$. We obtain a main term

$$\frac{g_1(W)^2\pi^2 N}{W\log^2 v}\sum_{\substack{a,b\le v\\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)}{g_2(a)g_2(b)}\log\frac{v}{a}\log\frac{v}{b}$$
$$\cdot \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime}}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\prod_{i\neq m,l}\frac{g_1([d_i,e_i])^2}{[d_i,e_i]}\Gamma([d_m,e_m]a,[d_l,e_l]b,W\prod_{i\neq m,l}[d_i,e_i]).$$

For arbitrary (square-free) moduli d_1, d_1 and q, we can write $\Gamma(d_1, d_2, q)$ as a product over primes (cf. the definition of $\Gamma(d_1, d_2, q)$ given in Lemma 2.5.4 and note that we are summing a multiplicative function). By considering the Euler-product and the various support restrictions on the variables d_i, e_i, a, b, one can write $\Gamma([d_m, e_m]a, [d_l, e_l]b, W\prod_{i\neq m,l}[d_i, e_i])$ in the form

$$\prod_{p\nmid 2W}\left(1-\frac{1}{p^2}\right)^{-1}\frac{g_2(a)g_2(b)}{g_7(a)g_7(b)}\prod_{i\neq m,l}\frac{[d_i,e_i]}{g_1([d_i,e_i]\varphi([d_i,e_i])}\prod_{j=m,l}\frac{1}{[d_j,e_j]\varphi([d_j,e_j])},$$

leaving us with a main term

$$\prod_{p\nmid 2W}\left(1-\frac{1}{p^2}\right)^{-1}\frac{g_1(W)^2Y_{N,W}\pi^2N}{W\log^2 v}$$
$$\cdot\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ W,[d_1,e_1],\dots,[d_k,e_k]\text{ coprime}}}\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\prod_{i\neq m,l}\frac{g_1([d_i,e_i])}{\varphi([d_i,e_i])}\prod_{j=m,l}\frac{1}{[d_j,e_j]\varphi([d_j,e_j])}.$$

Here we have defined

$$Y_{N,W}=\sum_{\substack{a,b\leq v\\ (a,W)=(b,W)=1\\ (a,b)=1\\ p|a,b\Rightarrow p\equiv 1\pmod 4}}\frac{\mu(a)\mu(b)}{g_7(a)g_7(b)}\log\frac{v}{a}\log\frac{v}{b}$$

as in (2.5.3). The main term is of the form S_J for $|J|=2$. By Lemma 2.6.6 it can be evaluated as

$$S_3^{(l,m)}=(1+o(1))\frac{Y_{N,W}g_1(W)^2\pi^2B^{k+2}N}{W\log^2 v}L^{(2)}_{k;m,l}(F),$$

where we have written

$$\prod_{p\nmid 2W}\left(1-\frac{1}{p^2}\right)^{-1}=1+O(D_0^{-1}).$$

Evaluating $Y_{N,W}$ as in Lemma 2.5.6, this simplifies to

$$S_3^{(l,m)}=(1+o(1))\frac{64(\frac{\log R}{\log v})B^kN}{\pi^2W}L^{(2)}_{k;m,l}(F).$$

(iv) Rewrite $S_4^{(m)}$ in the form

$$\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\sum_{\substack{N\leq n<2N\\ n\equiv v_0\pmod W\\ n\equiv 1\pmod 4\\ n\equiv -h_i\pmod{[d_i,e_i]}\ \forall i}}\rho^2(n+h_m).$$

Expanding out the definition of $\rho^2(n)$ we see this is equal to

$$\frac{1}{\log^2 v}\sum_{\substack{d_1,\dots,d_k\\e_1,\dots,e_k}}\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\sum_{a,b\le v}\frac{\mu(a)\mu(b)}{g_2(a)g_2(b)}\log\frac{v}{a}\log\frac{v}{b}\sum_{\substack{N\le n<2N\\ n\equiv v_0 \pmod W\\ n\equiv 1 \pmod 4\\ n\equiv -h_i \pmod{[d_i,e_i]}\ \forall i\\ n\equiv -h_m \pmod{[a,b]}}} r^2(n+h_m).$$

Again, we may restrict to the case $W, [d_1,e_1],\dots,[d_k,e_k],[a,b]$ are pairwise coprime. In this case the inner sum can be evaluated according to Lemma 2.5.5, taking $q = W\prod_{i\neq m}[d_i,e_i]$ and $d=[a,b][d_m,e_m]$. We note that $q\ll_\epsilon N^{\theta_2+\epsilon}$ and $d\ll N^{2\theta_1+\theta_2}$, and so the inner sum becomes

$$\frac{g_3(q)g_4(d)}{qd}\bigg(\log N + A_2 + 2\sum_{p\mid q}g_5(p) - 2\sum_{p\mid d}g_6(p)\bigg)N + O_\epsilon(N^{\frac34+\theta_2+\epsilon}).$$

Bounding the rest of the sum trivially, we see the error term contributes $O_\epsilon(N^{\frac34+2(\theta_1+\theta_2)+\epsilon})$ which is small. For the main term, let

$$Z^{(1)}_{N,W} = \sum_{a,b\le v}\frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]}\log\frac{v}{a}\log\frac{v}{b},$$
$$Z^{(2)}_{N,W} = \sum_{a,b\le v}\frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]}\log\frac{v}{a}\log\frac{v}{b}\sum_{p\mid[a,b]}g_6(p)$$

be as in (2.5.4) and (2.5.5). We can express $S_4^{(m)} = \Lambda_1+\Lambda_2+\Lambda_3+\Lambda_4$ where

$$\Lambda_1 = \frac{g_3(W)Z^{(1)}_{N,W}N}{W\log^2 v}\bigg(\log N + A_2 + 2\sum_{p\mid W}g_5(p)\bigg)T,$$
$$\Lambda_2 = \frac{2g_3(W)Z^{(1)}_{N,W}N}{W\log^2 v}\sum_{i\neq m}\sum_{\substack{D_0<p\le v\\ p\equiv 3 \pmod 4}}g_5(p)T^{(p,i)},$$
$$\Lambda_3 = -\frac{2g_3(W)Z^{(1)}_{N,W}N}{W\log^2 v}\sum_{\substack{D_0<p\le v\\ p\equiv 3 \pmod 4}}g_6(p)T^{(p,m)},$$
$$\Lambda_4 = -\frac{2g_3(W)Z^{(2)}_{N,W}N}{W\log^2 v}T$$

and

$$T = \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime}}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\neq m} \frac{g_1([d_i,e_i])}{[d_i,e_i]} \frac{1}{[d_m,e_m]^2},$$

$$T^{(p,i)} = \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ p|[d_i,e_i]\\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime}}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\neq m} \frac{g_1([d_i,e_i])}{[d_i,e_i]} \frac{1}{[d_m,e_m]^2}.$$

T is of the form S_J for $|J| = 1$, and so by Lemma 2.6.6 it can be evaluated as

$$T = (1 + o(1))B^{k+1}L^{(1)}_{k;m}(F).$$

To evaluate $T^{(p,i)}$, note by inclusion-exclusion we can write it as

$$\left(\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ p|d_i}}' + \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ p|e_i}}' - \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ p|d_i,e_i}}'\right)\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\neq m} \frac{g_1([d_i,e_i])}{[d_i,e_i]} \frac{1}{[d_m,e_m]^2},$$

where $\sum'$ denotes the condition $W, [d_1,e_1],\dots,[d_k,e_k]$ are pairwise coprime. Thus we see it is of the form $S_{J,p,1,i} + S_{J,1,p,i} - S_{J,p,p,i}$ for $|J| = 1$. By Lemma 2.6.6 we conclude

$$T^{(p,i)} \ll \begin{cases} \frac{F_{\max}^2 B^{k+1}(\log\log R)^2}{p}, & \text{if } i \neq m \\ \frac{F_{\max}^2 B^{k+1}(\log\log R)^2}{p^2}, & \text{if } i = m \end{cases}$$

Now we note that

$$\sum_{\substack{D_0<p\le v\\ p\equiv 3 \pmod 4}} \frac{g_5(p)}{p} \ll \sum_{p>D_0} \frac{\log p}{p^2} \ll \frac{\log D_0}{D_0},$$

$$\sum_{\substack{D_0<p\le v\\ p\equiv 3 \pmod 4}} \frac{g_6(p)}{p^2} \ll \sum_{p>D_0} \frac{\log p}{p^2} \ll \frac{\log D_0}{D_0},$$

and so, with our choice $D_0 = (\log\log N)^3$, the contributions from Λ_2 and Λ_3 are negligible. Because

$$\sum_{p|W} g_5(p) \ll \sum_{p<D_0} \frac{\log p}{p} \ll \log D_0,$$

we see that the only contribution to the main term comes from the Λ_1 term corresponding to $\log N$, and Λ_4, leaving us with

$$S_4^{(m)} = (1 + o(1))\frac{g_3(W)B^{k+1}N}{W\log^2 v}\left[Z^{(1)}_{N,W}\log N - 2Z^{(2)}_{N,W}\right]L^{(1)}_{k;m}(F).$$

Evaluating these according to Lemma 2.5.6, and using the fact

$$\frac{g_3(W_1)}{g_1(W_1)^3} = \prod_{\substack{p<D_0 \\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p^2}\right)^{-1} = \frac{3\zeta(2)}{8A^2} + O(D_0^{-1}) = \frac{\pi^2}{16A^2} + O(D_0^{-1}),$$

we obtain

$$S_4^{(m)} = (1+o(1))\frac{2\sqrt{\frac{\log R}{\log v}}(\frac{\log N}{\log v}+1)B^k N}{\pi W} L_{k;m}^{(1)}(F).$$

This finishes the proof of Proposition 2.6.2. □

Thus it remains to establish Lemma 2.6.6. First we require a few technical sieve lemmas. We list these in the following section.

2.7 Technical sieve sums lemmas

In the various sieve calculations that appear in the proof of Lemma 2.6.6, we will frequently encounter sums of the form

$$\sum_{\substack{n\le X \\ p|n\Rightarrow p\equiv 3 \pmod 4}} \mu^2(n) f(n),$$

where f is a multiplicative function satisfying $f(p) = O(1/p)$. We can evaluate sums of this type with the following lemmas.

Lemma 2.7.1 (Technical sieve sum lemma)**.** *Let $A_1, A_2, L > 0$. Let γ be a multiplicative function satisfying the sieve axioms*

$$0 \le \frac{\gamma(p)}{p} \le 1 - A_1,$$

and

$$-L \le \sum_{w\le p\le z} \frac{\gamma(p)\log p}{p} - \frac{1}{2}\log\frac{z}{w} < A_2$$

for any $2 \le w \le z$. Let g be the totally multiplicative function defined on primes by $g(p) = \frac{\gamma(p)}{p-\gamma(p)}$. Finally, let $G : [0,1] \to \mathbb{R}$ be a piecewise differentiable function, and let $G_{max} = \sup_{t\in[0,1]}(|G(t)| + |G'(t)|)$. Then

$$\sum_{d<z} \mu^2(d)g(d)G\left(\frac{\log d}{\log z}\right) = c_\gamma \frac{(\log z)^{\frac{1}{2}}}{\Gamma(1/2)} \int_0^1 G(x)\frac{\mathrm{d}x}{\sqrt{x}} + O_{A_1,A_2}(c_\gamma L G_{max}(\log z)^{-\frac{1}{2}}),$$

where

$$c_\gamma = \prod_p \left(1 - \frac{\gamma(p)}{p}\right)^{-1} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}}.$$

Here, the implied constant in the Landau notation is independent of G and L.

Proof. This is [10, Lemma 4] with slight changes to notation. □

To use this lemma in practice, we need to be able to evaluate the singular series c_γ which appears. In the next lemma we do this for a function $\gamma(p)$ which covers the cases of interest to us.

Lemma 2.7.2 (Evaluation of singular series)**.** *Let*

$$\gamma(p) = \begin{cases} 1 + O(1/p) & \text{if } p \nmid W, p \equiv 3 \ (\text{mod } 4), \\ 0 & \text{otherwise,} \end{cases}$$

With the notation of Lemma 2.7.1, we have

$$c_\gamma = \frac{A}{\sqrt{L(1,\chi)}} \cdot \frac{\varphi(W_3)}{W_3}(1 + O(D_0^{-1}))$$

where A is the Ramanujan-Landau constant defined in (2.4.1).

Proof. Let $\gamma(p) = 1 + \alpha(p)$ where $\alpha(p) = O(1/p)$. Define the auxiliary function

$$\delta(p) = \begin{cases} 1 & \text{if } p \equiv 3 \ (\text{mod } 4), \\ 0 & \text{otherwise.} \end{cases}$$

One can easily show $c_\delta = A/\sqrt{L(1,\chi)}$. The result follows because

$$c_\gamma = c_\delta \prod_{\substack{p \mid W \\ p \equiv 3 \ (\text{mod } 4)}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \nmid W \\ p \equiv 3 \ (\text{mod } 4)}} \left(1 - \frac{\alpha(p)}{p-1}\right)^{-1}.$$

The latter product is $1 + O(D_0^{-1})$ by our assumption $\alpha(p) = O(1/p)$. □

The next lemma collects both of these results together. First we recall the definition of the normalising factor from (2.6.8):

$$B = \frac{2A\varphi(W_3)(\log R)^{\frac{1}{2}}}{\pi W_3}. \tag{2.7.1}$$

Lemma 2.7.3 (Evaluation of sieve sums)**.** *Let f be a multiplicative function such that*

$$f(p) = \frac{1}{p} + O\Big(\frac{1}{p^2}\Big).$$

Then for any piece-wise smooth function G we have

$$\sum_{\substack{d\le R\\(d,W)=1\\p|d\Rightarrow p\equiv 3\ (mod\ 4)}} \mu^2(d)f(d)G\Big(\frac{\log d}{\log x}\Big) = B\int_0^1 G(x)\frac{\mathrm{d}x}{\sqrt{x}} + O\Big(\frac{G_{max}B}{D_0}\Big).$$

Proof. Let $f(p) = 1/p + g(p)$ where $g(p) = O(1/p^2)$, and consider the function γ defined on primes by

$$\gamma(p) = \begin{cases} 1 - \frac{1}{p+1+pg(p)} & \text{if } p\nmid W, p\equiv 3 \pmod 4,\\ 0, & \text{otherwise.}\end{cases}$$

With this choice of $\gamma(p)$ we have

$$\frac{\gamma(p)}{p-\gamma(p)} = f(p).$$

We wish to evaluate this sum by applying Lemma 2.7.1. We need to check the constraints on $\gamma(p)$ are satisfied. First, note that, for any $2 \le w \le z$, we have

$$\begin{aligned}\sum_{w\le p\le z}\frac{\gamma(p)\log p}{p} &= \sum_{\substack{w\le p\le z\\p\equiv 3\ (\mathrm{mod}\ 4)\\p\nmid W}}\frac{\log p}{p} + O\Big(\sum_{\substack{w\le p\le z\\p\equiv 3\ (\mathrm{mod}\ 4)\\p\nmid W}}\frac{\log p}{p^2}\Big)\\ &= \sum_{\substack{w\le p\le z\\p\equiv 3\ (\mathrm{mod}\ 4)}}\frac{\log p}{p} + O\Big(\sum_{\substack{w\le p\le z\\p\equiv 3\ (\mathrm{mod}\ 4)\\p\mid W}}\frac{\log p}{p}\Big) + O(1)\\ &= \frac{1}{2}\log\frac{z}{w} + O(\log D_0) + O(1).\end{aligned}$$

Therefore the lower bound in Lemma 2.7.1 holds with some L bounded by $L \ll 1 + \log D_0$. For the corresponding upper bound, simply note that

$$\begin{aligned}\sum_{w\le p\le z}\frac{\gamma(p)\log p}{p} &\le \sum_{\substack{w\le p\le z\\p\equiv 3\ (\mathrm{mod}\ 4)\\p\nmid W}}\frac{\log p}{p} + O(1)\\ &\le \sum_{\substack{w\le p\le z\\p\equiv 3\ (\mathrm{mod}\ 4)}}\frac{\log p}{p} + O(1)\\ &= \frac{1}{2}\log\frac{z}{w} + O(1),\end{aligned}$$

since we have $\gamma(p) \leq 1$ (whenever $p \equiv 3 \pmod 4$ and $p \nmid W$) for all but at most $O(1)$ values of p. Thus the upper bound in Lemma 2.7.1 holds with A_2 a suitably large constant. Hence we can apply Lemma 2.7.1. We obtain

$$\sum_{\substack{d\leq R\\(d,W)=1\\p|d\Rightarrow p\equiv 3 \pmod 4}} \mu^2(d)f(d)G\left(\frac{\log d}{\log x}\right) = \frac{c_\gamma(\log R)^{\frac{1}{2}}}{\Gamma(1/2)}\int_0^1 G(x)\frac{\mathrm{d}x}{\sqrt{x}} + O\left(\frac{G_{\max}c_\gamma(1+\log D_0)}{(\log R)^{\frac{1}{2}}}\right).$$

We can evaluate c_γ by Lemma 2.7.2 to find

$$c_\gamma = \frac{A}{\sqrt{L(1,\chi)}}\cdot\frac{\varphi(W_3)}{W_3}(1+O(D_0^{-1}))$$

When we substitute this back into our expression we see the error incurred here contributes $O(G_{\max}B/D_0)$ and dominates. The result follows as $\Gamma(1/2)\sqrt{L(1,\chi)} = \pi/2$. □

We highlight the following two results, the first of which follows immediately from Lemma 2.7.3, and the second of which is trivial.

1. For multiplicative functions f satisfying $f(p) = 1/p + O(1/p^2)$ we have the upper bound

$$\sum_{\substack{d\leq R\\(d,W)=1\\p|d\Rightarrow p\equiv 3 \pmod 4}} \mu^2(d)f(d) \ll B. \tag{2.7.2}$$

2. For multiplicative functions g satisfying $g(p) = O(1/p^2)$ we have the upper bound

$$\sum_{\substack{d\leq R\\(d,W)=1\\p|d\Rightarrow p\equiv 3 \pmod 4}} \mu^2(d)g(d) \ll 1. \tag{2.7.3}$$

These sums will appear frequently in our calculations, and we will use these bounds without comment in the arguments which follow.

2.8 Establishing Lemma 2.6.6

Our attention now turns to establishing Lemma 2.6.6. We follow the combinatorial arguments used by Maynard - the steps which follow mirror those found in [21].

2.8.1 Change of variables.

Our first step to evaluating the sums appearing in Lemma 2.6.6 is to make a change of variables. We do so in the following proposition.

Proposition 2.8.1 (Diagonalising the sieve sum)**.** *With notation as in Lemma 2.6.6, denote by f^*, g^* the convolutions*

$$f^* = \mu * \frac{1}{f}, \quad g^* = \mu * \frac{1}{g}.$$

Define the diagonalising vectors $y^{(J,p,m)}_{r_1,\dots,r_k} = y^{(J,p,m,f,g)}_{r_1,\dots,r_k}$ by

$$y^{(J,p,m)}_{r_1,\dots,r_k} = \Big(\prod_{i\in I}\mu(r_i)f^*(r_i)\Big)\Big(\prod_{j\in J}\mu(r_j)g^*(r_j)\Big)\sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\ \forall i\\ p|d_m}}\lambda_{d_1,\dots,d_k}\prod_{i\in I}f(d_i)\prod_{j\in J}g(d_j).$$

Let $y^{(J,p,m)}_{max} = \sup_{r_1,\dots,r_k}|y^{(J,p,m)}_{r_1,\dots,r_k}|$ and $\tilde{y}^{(J,p,m)}_{max} = \sup_{\substack{r_1,\dots,r_k\\(r_m,p)=1}}|y^{(J,p,m)}_{r_1,\dots,r_k}|$. (Note that these coincide if $p = 1$.) Then we have

$$S_{J,p_1,p_2,m} = \sum_{\substack{u_1,\dots,u_k\\(u_m,p_1p_2)=1\\u_j=1\ \forall j\in J}}\frac{(y^{(J,p_1,m)}_{u_1,\dots,u_k})(y^{(J,p_2,m)}_{u_1,\dots,u_k})}{\prod_{i\in I}f^*(u_i)\prod_{j\in J}g^*(u_j)} + E.$$

If $m \in J$ then the (error) term E satisfies

$$E \ll B^{|I|}\Bigg[\frac{(\tilde{y}^{(J,p_1,m)}_{max})(\tilde{y}^{(J,p_2,m)}_{max})}{D_0} + \frac{(y^{(J,p_1,m)}_{max})(y^{(J,p_2,m)}_{max})}{(p_1p_2/(p_1,p_2))^2} + \frac{(y^{(J,p_1,m)}_{max})(\tilde{y}^{(J,p_2,m)}_{max})}{p_1^2} + \frac{(\tilde{y}^{(J,p_1,m)}_{max})(y^{(J,p_2,m)}_{max})}{p_2^2}\Bigg].$$

If $m \notin J$ then E satisfies a similar estimate, namely that which is obtained upon replacing all occurrences of p_i^2 with p_i in the above expression, for $i \in \{1,2\}$. Moreover, in both of these cases, we adopt the convention that if $p_i = 1$ then any term in our expression for E involving p_i in the denominator may be omitted.

Proof. Recall the definition of $S_{J,p_1,p_2,m}$ given in Lemma 2.6.6:

$$S_{J,p_1,p_2,m} = \sum_{\substack{d_1,\dots,d_k\\e_1,\dots,e_k\\W,[d_1,e_1],\dots,[d_k,e_k]\text{ coprime}\\p_1|d_m,p_2|e_m}}\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}\prod_{i\in I}f([d_i,e_i])\prod_{j\in J}g([d_j,e_j]). \quad (2.8.1)$$

We can write this in the form

$$S_{J,p_1,p_2,m} = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime} \\ p_1|d_m, p_2|e_m}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\in I} \frac{f(d_i)f(e_i)}{f((d_i,e_i))} \prod_{j\in J} \frac{g(d_j)g(e_j)}{g((d_j,e_j))}, \quad (2.8.2)$$

using multiplicativity of the functions f and g, together with the fact $[d_i, e_i]$ is square-free for each i. We remark that because f, g are non-zero, the functions $1/f, 1/g$ are well-defined. We note the convolution identities

$$\frac{1}{f((d_i,e_i))} = \sum_{u_i|d_i,e_i} f^*(u_i), \qquad \frac{1}{g((d_j,e_j))} = \sum_{u_j|d_j,e_j} g^*(u_j)$$

for f^* and g^*. Substituting these into (2.8.2) and swapping the order of summation, we obtain

$$\sum_{u_1,\dots,u_k} \Big(\prod_{i\in I} f^*(u_i)\Big)\Big(\prod_{j\in J} g^*(u_j)\Big) \cdot \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ W,[d_1,e_1],\dots,[d_k,e_k] \text{ coprime} \\ u_i|d_i,e_i \ \forall i\in I \\ u_j|d_j,e_j \ \forall j\in J \\ p_1|d_m,p_2|e_m}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\in I} f(d_i)f(e_i) \prod_{j\in J} g(d_j)g(e_j).$$

From the support of the $\lambda_{d_1,\dots,d_k}$, we see the only restriction coming from the pairwise coprimality of $W, [d_1, e_1], \dots, [d_k, e_k]$ is from the possibility $(d_i, e_j) \neq 1$ for $i \neq j$. We can take care of this constraint by Möbius inversion: multiplying by $\sum_{s_{i,j}|d_i,e_j} \mu(s_{i,j})$ for all $i \neq j$, we obtain

$$\sum_{u_1,\dots,u_k} \Big(\prod_{i\in I} f^*(u_i)\Big)\Big(\prod_{j\in J} g^*(u_j)\Big) \sum_{s_{1,2},\dots,s_{k-1,k}} \Big(\prod_{\substack{1\le i,j\le k \\ i\neq j}} \mu(s_{i,j})\Big) \cdot \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ u_i|d_i,e_i \ \forall i\in I \\ u_j|d_j,e_j \ \forall j\in J \\ s_{i,j}|d_i,e_j \ \forall i\neq j \\ p_1|d_m,p_2|e_m}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \prod_{i\in I} f(d_i)f(e_i) \prod_{j\in J} g(d_j)g(e_j). \quad (2.8.3)$$

We may restrict to the case where $s_{i,j}$ is coprime to $s_{i,a}, s_{b,j}$ and u_i, u_j, for $a \neq j$ and $b \neq i$, because the vectors $\lambda_{d_1,\dots,d_k}$ are supported on square-free integers $d = \prod_{i=1}^k d_i$. Denote the sum over $s_{i,j}$ with these conditions by $\sum'$. Define the diagonalising

vectors

$$y_{r_1,\dots,r_k}^{(J,p,m)} = \Big(\prod_{i\in I}\mu(r_i)f^*(r_i)\Big)\Big(\prod_{j\in J}\mu(r_j)g^*(r_j)\Big)\sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\ \forall i\\ p|d_m}}\lambda_{d_1,\dots,d_k}\prod_{i\in I}f(d_i)\prod_{j\in J}g(d_j). \tag{2.8.4}$$

From the support of $\lambda_{d_1,\dots,d_k}$ we see that $y_{r_1,\dots,r_k}^{(J,p,m)}$ is also supported on $r_1,\dots,r_k$ with $r=\prod_{i=1}^k r_i$ square-free, $(r,W)=1$ and $p|r\Rightarrow p\equiv 3 \pmod 4$. We claim this change of variables is invertible. Indeed, from the definition (2.8.4), for $d_1,\dots,d_k$ with $\prod_{i=1}^k d_i$ square-free, we have

$$\begin{aligned}\sum_{\substack{r_1,\dots,r_k\\ d_i|r_i\ \forall i}}\frac{y_{r_1,\dots,r_k}^{(J,p,m)}}{\prod_{i\in I}f^*(r_i)\prod_{j\in J}g^*(r_j)} &= \sum_{\substack{r_1,\dots,r_k\\ d_i|r_i\ \forall i}}\prod_{i=1}^k\mu(r_i)\sum_{\substack{e_1,\dots,e_k\\ r_i|e_i\ \forall i\\ p|e_m}}\lambda_{e_1,\dots,e_k}\prod_{i\in I}f(e_i)\prod_{j\in J}g(e_j)\\ &= \sum_{e_1,\dots,e_k}1_{p|e_m}\lambda_{e_1,\dots,e_k}\prod_{i\in I}f(e_i)\prod_{j\in J}g(e_j)\sum_{\substack{r_1,\dots,r_k\\ r_i|e_i\ \forall i\\ d_i|r_i\ \forall i}}\prod_{i=1}^k\mu(r_i)\\ &= 1_{p|d_m}\lambda_{d_1,\dots,d_k}\prod_{i\in I}\mu(d_i)f(d_i)\prod_{j\in J}\mu(d_j)g(d_j). \end{aligned}\tag{2.8.5}$$

With this transformation our sum (2.8.3) becomes

$$\begin{aligned}&\sum_{u_1,\dots,u_k}\Big(\prod_{i\in I}f^*(u_i)\Big)\Big(\prod_{j\in J}g^*(u_j)\Big)\\ &\cdot\sum_{s_{1,2},\dots,s_{k-1,k}}{}'\Big(\prod_{\substack{1\le i,j\le k\\ i\ne j}}\mu(s_{i,j})\Big)\Big(\prod_{i\in I}\frac{\mu(a_i)\mu(b_i)}{f^*(a_i)f^*(b_i)}\Big)\Big(\prod_{j\in J}\frac{\mu(a_j)\mu(b_j)}{g^*(a_j)g^*(b_j)}\Big)y_{a_1,\dots,a_k}^{(J,p_1,m)}y_{b_1,\dots,b_k}^{(J,p_2,m)},\end{aligned}$$

where we have defined $a_i=u_i\prod_{j\ne i}s_{i,j}$ and $b_j=u_j\prod_{i\ne j}s_{i,j}$. Because of our constraints on the $s_{i,j}$ variables, we can use multiplicativity to write this as

$$\begin{aligned}&\sum_{u_1,\dots,u_k}\Big(\prod_{i\in I}\frac{\mu^2(u_i)}{f^*(u_i)}\Big)\Big(\prod_{j\in J}\frac{\mu^2(u_j)}{g^*(u_j)}\Big)\\ &\sum_{s_{1,2},\dots,s_{k-1,k}}{}'\Big(\prod_{\substack{i,j\in I\\ i\ne j}}\frac{\mu(s_{i,j})}{f^*(s_{i,j})^2}\Big)\Big(\prod_{\substack{i,j\in J\\ i\ne j}}\frac{\mu(s_{i,j})}{g^*(s_{i,j})^2}\Big)\\ &\Big(\prod_{i\in I,j\in J}\frac{\mu(s_{i,j})\mu(s_{j,i})}{f^*(s_{i,j})f^*(s_{j,i})g^*(s_{i,j})g^*(s_{j,i})}\Big)y_{a_1,\dots,a_k}^{(J,p_1,m)}y_{b_1,\dots,b_k}^{(J,p_2,m)}.\end{aligned}\tag{2.8.6}$$

We now wish to reduce to the case when $(a_m,p_1)=(b_m,p_2)=1$. Indeed, we will show the contribution from the alternative cases is negligible. Of course, depending

on whether of not $p_1 = 1$ and/or $p_2 = 1$, some (or all) of the analysis which follows is not necessary, and this accounts for the convention we assert in the statement of the proposition. First let us note the estimate

$$\frac{1}{f^*(p)} = \frac{f(p)}{1-f(p)} = \frac{\frac{1}{p} + O(\frac{1}{p^2})}{1 - \frac{1}{p} + O(\frac{1}{p^2})} = \frac{1}{p} + O\bigg(\frac{1}{p^2}\bigg), \tag{2.8.7}$$

and similarly

$$\frac{1}{g^*(p)} = \frac{1}{p^2} + O\bigg(\frac{1}{p^3}\bigg). \tag{2.8.8}$$

Now, there are three cases to consider.

1. Suppose that $p_1|a_m$ and $p_2|b_m$. This occurs if and only if $p_1|u_m$ or $p_1|s_{m,j}$ for some $j \neq m$, and $p_2|u_m$ or $p_2|s_{i,m}$ for some $i \neq m$. Suppose, for example, that $p_1|u_m$ and $p_2|u_m$. Moreover let us assume that $m \in J$. Then one can bound the contribution as follows:

$$\begin{aligned}
&\ll (y_{\max}^{(J,p_1,m)})(y_{\max}^{(J,p_2,m)})\bigg(\sum_{\substack{u\leq R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)}{f^*(u)}\bigg)^{|I|}\\
&\cdot\bigg(\sum_{\substack{u\leq R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)}{g^*(u)}\bigg)^{|J|-1}\bigg(\sum_{\substack{u_m\leq R\\(u_m,W)=1\\p_1,p_2|u_m\\p|u_m\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u_m)}{g^*(u_m)}\bigg)\\
&\bigg(\sum_{s\geq 1}\frac{\mu^2(s)}{f^*(s)^2}\bigg)^{|I|^2-|I|}\bigg(\sum_{s\geq 1}\frac{\mu^2(s)}{g^*(s)^2}\bigg)^{|J|^2-|J|}\bigg(\sum_{s\geq 1}\frac{\mu^2(s)}{f^*(s)g^*(s)}\bigg)^{2|I||J|}\\
&\ll \frac{(y_{\max}^{(J,p_1,m)})(y_{\max}^{(J,p_2,m)})B^{|I|}}{(p_1p_2/(p_1,p_2))^2}.
\end{aligned}$$

   It is easy to see that this bound also holds in any of the other possible cases in which $p_1|a_m$ and $p_2|b_m$ and $m \in J$. If instead $m \notin J$, then again it is easy to see the contribution is

$$\ll \frac{(y_{\max}^{(J,p_1,m)})(y_{\max}^{(J,p_2,m)})B^{|I|}}{p_1p_2/(p_1,p_2)},$$

   in all possible cases.

2. Suppose that $p_1|a_m$ and $p_2 \nmid b_m$. If $m \in J$, then similarly to the above, one can bound the contribution by

$$\ll \frac{(y_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})B^{|I|}}{p_1^2}.$$

If $m \notin J$ then likewise one obtains a contribution

$$\ll \frac{(y_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})B^{|I|}}{p_1}.$$

3. Finally, the case $p_1 \nmid a_m$ and $p_2 | b_m$ proceeds as above, interchanging the roles of p_1 and p_2.

Thus, we may now suppose that $(a_m, p_1) = (b_m, p_2) = 1$. From the support of the $y_{a_1,\dots,a_k}^{(J,p_1,m)}$ we see there is no contribution from $(s_{i,j}, W) \neq 1$ and so either $s_{i,j} = 1$ or $s_{i,j} > D_0$. The contribution from $s_{i,j} > D_0$ with $i, j \in I$ is

$$\ll (\tilde{y}_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})\Bigg(\sum_{\substack{u\leq R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)}{f^*(u)}\Bigg)^{|I|}\Bigg(\sum_{\substack{u\leq R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)}{g^*(u)}\Bigg)^{|J|}$$
$$\Bigg(\sum_{s_{i,j}\geq D_0} \frac{\mu^2(s_{i,j})}{f^*(s_{i,j})^2}\Bigg)\Bigg(\sum_{s\geq 1} \frac{\mu^2(s)}{f^*(s)^2}\Bigg)^{|I|^2-|I|-1}\Bigg(\sum_{s\geq 1} \frac{\mu^2(s)}{g^*(s)^2}\Bigg)^{|J|^2-|J|}\Bigg(\sum_{s\geq 1} \frac{\mu^2(s)}{f^*(s)g^*(s)}\Bigg)^{2|I||J|}$$
$$\ll \frac{(\tilde{y}_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})B^{|I|}}{D_0},$$

This contribution will be negligible. The cases $i, j \in J$ and $i \in I, j \in J$ can be treated the same way. This leaves us with a main term

$$\sum_{\substack{u_1,\dots,u_k\\(u_m,p_1p_2)=1}} \frac{(y_{u_1,\dots,u_k}^{(J,p_1,m)})(y_{u_1,\dots,u_k}^{(J,p_2,m)})}{\prod_{i\in I} f^*(u_i)\prod_{j\in J} g^*(u_i)}$$

To finish, we claim the contribution from $u_j > 1$ is small whenever $j \in J$. Indeed if $u_j > 1$ then it must be divisible by a prime $p > D_0$ (with $p \equiv 3 \pmod 4$). So suppose $|J| \geq 1$ and let $j \in J$. If $u_j > 1$ we get a contribution

$$\ll (\tilde{y}_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})\Bigg(\sum_{\substack{u\leq R\\(u,W)=1}} \frac{\mu^2(u)}{f^*(u)}\Bigg)^{|I|}\Bigg(\sum_{u\leq R} \frac{\mu^2(u)}{g^*(u)}\Bigg)^{|J|-1}\sum_{\substack{p>D_0\\p\equiv 3 \pmod 4}}\Bigg(\sum_{\substack{u_j<R\\p|u_j}} \frac{\mu^2(u_j)}{g^*(u_j)}\Bigg)$$
$$\ll (\tilde{y}_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})B^{|I|}\sum_{\substack{p>D_0\\p\equiv 3 \pmod 4}} \frac{1}{g^*(p)}\Bigg(\sum_{u_j} \frac{\mu^2(u_j)}{g^*(u_j)}\Bigg)$$
$$\ll \frac{(\tilde{y}_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})B^{|I|}}{D_0},$$

which is small. Putting all of these facts together establishes Proposition 2.8.1. □

2.8.2 Transformation for $y^{(J,p,m)}_{r_1,\dots,r_k}$ and proof of Lemma 2.6.6 parts (i) and (ii)

Define

$$y_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k}\mu(r_i)\varphi(r_i)\right)\sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\ \forall i}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}d_i},$$

and let $y_{\max} = \sup_{r_1,\dots,r_k}|y_{r_1,\dots,r_k}|$. By the inversion formula (2.8.5), our definition of $\lambda_{d_1,\dots,d_k}$ in Proposition 2.6.2 is equivalent to taking

$$y_{r_1,\dots,r_k} = F\left(\frac{\log r_1}{\log R},\dots,\frac{\log r_k}{\log R}\right). \tag{2.8.9}$$

We now wish to relate the more complicated diagonalisation vectors $y^{(J,p,m)}_{r_1,\dots,r_k}$ to these simpler vectors. We first deal with the case when $J=\emptyset$, which is straightforward. By inspecting the proof of Proposition 2.6.2, it is clear that we only need to understand this case when $f(p)=1/p$.

Lemma 2.8.2 (Relating $y^{(J,p_1,m)}_{r_1,\dots,r_k}$ to $y_{r_1,\dots,r_k}$ when $J=\emptyset$)**.** *Suppose $y^{(J,p_1,m)}_{r_1,\dots,r_k}\neq 0, J=\emptyset$ and $m\in\{1,\dots,k\}$. Moreover suppose $f(p)=1/p$ for all primes p. Then the following hold.*

1. *If $p_1|r_m$ then*
$$y^{(J,p_1,m)}_{r_1,\dots,r_k} = y_{r_1,\dots,r_k}.$$
2. *If $p_1\nmid r_m$ then*
$$y^{(J,p_1,m)}_{r_1,\dots,r_k} = \frac{y_{r_1,\dots,p_1r_m,\dots,r_k}}{\mu(p_1)\varphi(p_1)}.$$

Proof. If $f(p)=1/p$ then $f^*(p)=p-1=\varphi(p)$. Hence we are assuming

$$y^{(J,p,m)}_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k}\mu(r_i)\varphi(r_i)\right)\sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\ \forall i\\ p|d_m}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}d_i}.$$

The result then follows by comparing with the definition of $y_{r_1\dots,r_k}$ given above. □

Thus, proceeding, we may suppose that $|J|\geq 1$. We may further suppose that $f(p)\neq 1/p$ as this case is of no interest to us (again, this is clear by inspecting the proof of Proposition 2.6.2). The following proposition gives the result in full.

Proposition 2.8.3 (Relating $y^{(J,p_1,m)}_{r_1,\dots,r_k}$ to $y_{r_1,\dots,r_k}$ when $|J|\geq 1$)**.** *Suppose $y^{(J,p_1,m)}_{r_1,\dots,r_k}\neq 0, |J|\geq 1$ and $f(p)\neq 1/p$. Then the following hold:*

(i) If $m \in J$ and $(r_m, p) = 1$ we have

$$y^{(J,p_1,m)}_{r_1,\dots,r_k} = \frac{\mu(p_1)p_1 g(p_1)}{\varphi(p_1)}\Big(\prod_{j\in J}\frac{r_j g(r_j)g^*(r_j)}{g^{**}(r_j)}\Big) \cdot \sum_{\substack{e_1,\dots,e'_m,\dots,e_k \\ r_i|e_i\ \forall i\neq m \\ r_m|e'_m \\ e_i=r_i\ \forall i\in I}} y_{e_1,\dots,p_1e'_m,\dots,e_k}\Big(\prod_{\substack{j\in J \\ j\neq m}}\frac{g^{**}(e_j)}{\varphi(e_j)}\Big)\Big(\frac{g^{**}(e'_m)}{\varphi(e'_m)}\Big) + O\Big(\frac{y_{max}B^{|J|}\log\log R}{D_0p_1^2}\Big).$$

(ii) If $m \notin J$ and $(r_m, p) = 1$ we have

$$y^{(J,p_1,m)}_{r_1,\dots,r_k} = \frac{\mu(p_1)p_1 f(p_1)}{\varphi(p_1)}\Big(\prod_{j\in J}\frac{r_j g(r_j)g^*(r_j)}{g^{**}(r_j)}\Big) \cdot \sum_{\substack{e_1,\dots,e'_m,\dots,e_k \\ r_i|e_i\ \forall i\neq m \\ e_i=r_i\ \forall i\in I\setminus\{m\} \\ e'_m=r_m}} y_{e_1,\dots,p_1e'_m,\dots,e_k}\Big(\prod_{j\in J}\frac{g^{**}(e_j)}{\varphi(e_j)}\Big) + O\Big(\frac{y_{max}B^{|J|}\log\log R}{D_0p_1}\Big).$$

(iii) If $p_1|r_m$ we have

$$y^{(J,p_1,m)}_{r_1,\dots,r_k} = \Big(\prod_{j\in J}\frac{r_j g(r_j)g^*(r_j)}{g^{**}(r_j)}\Big) \cdot \sum_{\substack{e_1,\dots,e_k \\ r_i|e_i\ \forall i \\ e_i=r_i\ \forall i\in I}} y_{e_1,\dots,e_k}\Big(\prod_{j\in J}\frac{g^{**}(e_j)}{\varphi(e_j)}\Big) + O\Big(\frac{y_{max}B^{|J|}\log\log R}{D_0}\Big).$$

Here f^{**} and g^{**} are defined by the convolutions

$$f^{**} = \iota\mu f * 1, \quad g^{**} = \iota\mu g * 1,$$

where ι is the identity function, $\iota(p) = p$.

Proof. We prove (i), with the rest proved in exactly the same way. Directly from the definition (2.8.4) we have

$$\frac{y^{(J,p_1,m)}_{r_1,\dots,r_k}}{\prod_{i\in I}\mu(r_i)f^*(r_i)\prod_{j\in J}\mu(r_j)g^*(r_j)} = \sum_{\substack{d_1,\dots,d_k \\ r_i|d_i\ \forall i \\ p_1|d_m}} \lambda_{d_1,\dots,d_k}\prod_{i\in I}f(d_i)\prod_{j\in J}g(d_j). \tag{2.8.10}$$

From the inversion formula (2.8.5) and the definition of $y_{r_1,\dots,r_k}$, we see that the right hand side of (2.8.10) equals

$$\sum_{\substack{d_1,\dots,d_k \\ r_i|d_i\ \forall i \\ p_1|d_m}}\Big(\prod_{i\in I}\mu(d_i)d_i f(d_i)\Big)\Big(\prod_{j\in J}\mu(d_j)d_j g(d_j)\Big)\sum_{\substack{e_1,\dots,e_k \\ d_i|e_i\ \forall i}}\frac{y_{e_1,\dots,e_k}}{\prod_{i=1}^k\varphi(e_i)}.$$

Swapping sums we obtain

$$\sum_{\substack{e_1,\dots,e_k\\ r_i|e_i\ \forall i\\ p_1|e_m}} \frac{y_{e_1,\dots,e_k}}{\prod_{i=1}^k \varphi(e_i)} \sum_{\substack{d_1,\dots,d_k\\ r_i|d_i\ \forall i\\ d_i|e_i\ \forall i\\ p_1|d_m}} \Big(\prod_{i\in I} \mu(d_i)d_i f(d_i)\Big)\Big(\prod_{j\in J} \mu(d_j)d_j g(d_j)\Big). \tag{2.8.11}$$

We can evaluate the inner sums using the convolution identities

$$f^{**}(n) = \sum_{d|n} \mu(d)df(d), \quad g^{**}(n) = \sum_{d|n} \mu(d)dg(d).$$

We note that

$$f^{**}(p) = 1 - pf(p) = O\Big(\frac{1}{p}\Big), \tag{2.8.12}$$

and similarly

$$g^{**}(p) = 1 - pg(p) = 1 + O\Big(\frac{1}{p}\Big). \tag{2.8.13}$$

With our assumption $f(p) \neq 1/p$, we may suppose both of these functions are non-zero. Now, recall that we are assuming $m \in J$. Using these identities transforms (2.8.11) into

$$\frac{\mu(p_1)p_1 g(p_1)}{g^{**}(p_1)}\Big(\prod_{i\in I} \frac{\mu(r_i)r_i f(r_i)}{f^{**}(r_i)}\Big)\Big(\prod_{j\in J} \frac{\mu(r_j)r_j g(r_j)}{g^{**}(r_j)}\Big)$$
$$\cdot \sum_{\substack{e_1,\dots,e_k\\ r_i|e_i\ \forall i\\ p_1|e_m}} y_{e_1,\dots,e_k}\Big(\prod_{i\in I} \frac{f^{**}(e_i)}{\varphi(e_i)}\Big)\Big(\prod_{j\in J} \frac{g^{**}(e_j)}{\varphi(e_j)}\Big).$$

Here we are using the fact $y_{e_1,\dots,e_k}$ is supported on square-free integers $e = \prod_{i=1}^k e_i$. Hence, from (2.8.10), it follows that

$$y^{(J,p_1,m)}_{r_1,\dots,r_k} = \frac{\mu(p_1)p_1 g(p_1)}{\varphi(p_1)}\Big(\prod_{i\in I} \frac{r_i f(r_i) f^*(r_i)}{f^{**}(r_i)}\Big)\Big(\prod_{j\in J} \frac{r_j g(r_j) g^*(r_j)}{g^{**}(r_j)}\Big)$$
$$\cdot \sum_{\substack{e_1,\dots,e'_m,\dots e_k\\ r_i|e_i\ \forall i\neq m\\ r_m|e'_m}} y_{e_1,\dots,p_1e'_m,\dots e_k}\Big(\prod_{i\in I} \frac{f^{**}(e_i)}{\varphi(e_i)}\Big)\Big(\prod_{\substack{j\in J\\ j\neq m}} \frac{g^{**}(e_j)}{\varphi(e_j)}\Big)\frac{g^{**}(e'_m)}{\varphi(e'_m)}.$$

Here we have substituted $e_m = p_1 e'_m$ and used the fact $(r_m, p) = 1$. Now, since

$$\frac{pf(p)f^*(p)}{\varphi(p)} = \frac{p}{p-1}(1 - f(p)) = \frac{p}{p-1}\Big[1 - \frac{1}{p} + O\Big(\frac{1}{p^2}\Big)\Big] = 1 + O\Big(\frac{1}{p^2}\Big),$$

it follows that

$$\sup_{r_1,\dots,r_k} \prod_{j\in J} \frac{r_j f(r_j) f^*(r_j)}{\varphi(r_j)} \ll 1. \tag{2.8.14}$$

Similarly, since

$$\frac{pg(p)g^*(p)}{\varphi(p)} = \frac{p}{p-1}(1-g(p)) = \frac{p}{p-1}\Big[1+O\Big(\frac{1}{p^2}\Big)\Big],$$

we have the bound

$$\sup_{r_1,\dots,r_k}\prod_{j\in J}\frac{r_j g(r_j)g^*(r_j)}{\varphi(r_j)} \ll \sup_{r_1,\dots,r_k}\prod_{j\in J}\frac{r_j}{\varphi(r_j)} \ll \log\log R. \tag{2.8.15}$$

Here we have used the fact $r=\prod_{i=1}^k r_i \le R$ and the standard estimate

$$\frac{n}{\varphi(n)} \ll \log\log n.$$

Now, if $i\neq m$ then either $e_i = r_i$ or $e_i > D_0 r_i$. Suppose $e_{i_0} > D_0 r_{i_0}$ for some $i_0\in I$. By first using multiplicativity of the sum over the e_i variables, and then using estimates (2.8.14) and (2.8.15), we see that that this gives a contribution

$$\begin{aligned}
&\ll \frac{y_{\max}\log\log R}{p_1^2}\Big(\sum_{\substack{e_{i_0}>D_0\\(e_{i_0},W)=1}}\frac{\mu^2(e_{i_0})f^{**}(e_{i_0})}{\varphi(e_{i_0})}\Big)\\
&\cdot\Big(\sum_{\substack{u\le R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}}\frac{\mu^2(u)f^{**}(u)}{\varphi(u)}\Big)^{|I|-1}\Big(\sum_{\substack{u\le R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}}\frac{\mu^2(u)g^{**}(u)}{\varphi(u)}\Big)^{|J|}\\
&\ll \frac{y_{\max}B^{|J|}\log\log R}{D_0 p_1^2},
\end{aligned}$$

where we have used the fact $f^{**}(p)/\varphi(p)=O(1/p^2)$ and $g^{**}(p)/\varphi(p)=1/p+O(1/p^2)$, which follows from (2.8.12) and (2.8.13) respectively. This is small. Thus

$$\begin{aligned}
y^{(J,p_1,m)}_{r_1,\dots,r_k} &= \frac{\mu(p_1)p_1 g(p_1)}{\varphi(p_1)}\Big(\prod_{i\in I}\frac{r_i f(r_i)f^*(r_i)}{\varphi(r_i)}\Big)\Big(\prod_{j\in J}\frac{r_j g(r_j)g^*(r_j)}{g^{**}(r_j)}\Big)\\
&\cdot\sum_{\substack{e_1,\dots,e'_m,\dots,e_k\\ r_i|e_i\ \forall i\neq m\\ r_m|e'_m\\ e_i=r_i\ \forall i\in I}} y_{e_1,\dots,p_1e'_m,\dots e_k}\Big(\prod_{\substack{j\in J\\ j\neq m}}\frac{g^{**}(e_j)}{\varphi(e_j)}\Big)\Big(\frac{g^{**}(e'_m)}{\varphi(e'_m)}\Big) + O\Big(\frac{y_{\max}B^{|J|}\log\log R}{D_0p_1^2}\Big).
\end{aligned}$$

From the support restrictions on $y^{(J,p_1,m)}_{r_1,\dots,r_k}$ we necessarily have $(r_i,W)=1$. From the above, we see the first product may be replaced by $1+O(D_0^{-1})$. This incurs an acceptable error

$$\ll \frac{y_{\max}\log\log R}{D_0p_1^2}\Big(\sum_{\substack{u\le R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}}\frac{\mu^2(u)g^{**}(u)}{\varphi(u)}\Big)^{|J|} \ll \frac{y_{\max}B^{|J|}\log\log R}{D_0p_1^2},$$

which gives the result stated. □

We record the following useful corollary.

Corollary 2.8.4. *With notation as in the statement of Proposition 2.8.1, the following estimates hold.*

1. *If $m \in J$ then*
$$\tilde{y}_{max}^{(J,p_1,m)} \ll \frac{y_{max} B^{|J|} \log\log R}{p_1^2}.$$
2. *If $m \notin J$ then*
$$\tilde{y}_{max}^{(J,p_1,m)} \ll \frac{y_{max} B^{|J|} \log\log R}{p_1}.$$
3. *We have*
$$y_{max}^{(J,p,m)} \ll y_{max} B^{|J|} \log\log R.$$

Proof. This follows easily from Lemma 2.8.2 and Proposition 2.8.3. (We note that in the special case $J = \emptyset$, in items (2) and (3) we could drop the extra $\log\log R$ factor if required.) □

We are now in a position to prove the first two parts of Lemma 2.6.6.

Proof of Lemma 2.6.6 parts (i) and (ii). We prove part (i), in the case $m \in J$. The rest of the argument proceeds along the same lines. From Proposition 2.8.3 we have
$$S_{J,p_1,p_2,m} = \sum_{\substack{u_1,\dots,u_k \\ (u_m,p_1p_2)=1 \\ u_j=1 \ \forall j\in J}} \frac{(y_{u_1,\dots,u_k}^{(J,p_1,m)})(y_{u_1,\dots,u_k}^{(J,p_2,m)})}{\prod_{i\in I} f^*(u_i) \prod_{j\in J} g^*(u_j)} + O\Big(\frac{y_{\max}^2 B^{k+|J|}(\log\log R)^2}{(p_1p_2/(p_1,p_2))^2}\Big).$$
Here we have used Corollary 2.8.4 to control the various error terms in the statement of the proposition. We have also used the fact $|I| + |J| = k$. It follows that
$$\begin{aligned} S_{J,p_1,p_2,m} &\ll (\tilde{y}_{\max}^{(J,p_1,m)})(\tilde{y}_{\max}^{(J,p_2,m)})\Big(\sum_{\substack{u\le R \\ (u,W)=1 \\ p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)}{f^*(u)}\Big)^{|I|} + \frac{y_{\max}^2 B^{k+|J|}(\log\log R)^2}{(p_1p_2/(p_1,p_2))^2} \\ &\ll \frac{y_{\max}^2 B^{k+|J|}(\log\log R)^2}{(p_1p_2/(p_1,p_2))^2}, \end{aligned}$$
again using Corollary 2.8.4. This gives the result, as required. □

From now on we are only interested in the sums $S_J = S_{J,1,1,m}$, and in particular the cases $|J| \in \{0,1,2\}$. For ease of notation we let $y_{r_1,\dots,r_k}^{(J)} = y_{r_1,\dots,r_k}^{(J,1,m)}$ and $y_{\max}^{(J)} = \sup_{r_1,\dots,r_k} |y_{r_1,\dots,r_k}^{(J)}|$. For future reference we note the bound
$$y_{\max}^{(J)} \ll y_{\max} B^{|J|} \log\log R, \tag{2.8.16}$$
proved above.

2.8.3 Relating vectors to functionals and proof of Lemma 2.6.6 part (iii)

We first prove the following corollary that follows from Proposition 2.8.3.

Corollary 2.8.5 (Relating $y^{(J)}_{r_1,\dots,r_k}$ to integral operators)**.** *Let $y_{r_1,\dots,r_k}$ be defined in terms of a fixed, smooth function F, supported on $R_k = \{\vec{x} \in [0,1]^k : \sum_{i=1}^k x_i \le 1\}$, by*

$$y_{r_1,\dots,r_k} = F\Big(\frac{\log r_1}{\log R}, \dots, \frac{\log r_k}{\log R}\Big).$$

Let

$$F_{max} = \sup_{(t_1,\dots,t_k)\in[0,1]^k} |F(t_1,\dots,t_k)| + \sum_{i=1}^k |\frac{\partial F}{\partial t_i}(t_1,\dots,t_k)|.$$

Define the integral operators

$$I_{r_1,\dots,r_k;m}(F) = \int_0^1 F\Big(\frac{\log r_1}{\log R}, \dots, x_m, \dots, \frac{\log r_k}{\log R}\Big)\frac{\mathrm{d}x_m}{\sqrt{x_m}},$$
$$I_{r_1,\dots,r_k;m,l}(F) = \int_0^1 \Big(\int_0^1 F\Big(\frac{\log r_1}{\log R}, \dots, x_l, \dots, x_m, \dots, \frac{\log r_k}{\log R}\Big)\frac{\mathrm{d}x_m}{\sqrt{x_m}}\Big)\frac{\mathrm{d}x_l}{\sqrt{x_l}}.$$

Then

(i) if $J = \{m\}$ we have

$$y^{(J)}_{r_1,\dots,r_k}\Big|_{r_j=1\ \forall j\in J} = B\Big(\prod_{i\in I}\frac{\varphi(r_i)}{r_i}\Big)I_{r_1,\dots,r_k;m}(F) + O\Big(\frac{F_{max}B}{D_0}\Big).$$

(ii) if $J = \{m,l\}$ we have

$$y^{(J)}_{r_1,\dots,r_k}\Big|_{r_j=1\ \forall j\in J} = B^2\Big(\prod_{i\in I}\frac{\varphi(r_i)}{r_i}\Big)^2 I_{r_1,\dots,r_k;m,l}(F) + O\Big(\frac{F_{max}B^2}{D_0}\Big).$$

Proof. First suppose $J = \{m\}$. From Proposition 2.8.3 we have

$$y^{(J)}_{r_1,\dots,r_k}\big|_{r_j=1\ \forall j\in J} = \sum_{e_m}\frac{g^{**}(e_m)}{\varphi(e_m)}F\Big(\frac{\log r_1}{\log R}, \dots, \frac{\log e_m}{\log R}, \cdots \frac{\log r_k}{\log R}\Big) + O\Big(\frac{F_{\max}B}{D_0}\Big) \tag{2.8.17}$$

Consider the function

$$\gamma_1(p) = \begin{cases} \frac{p}{1+\frac{\varphi(p)}{g^{**}(p)}} & \text{if } p \nmid W\prod_{i\in I} r_i \text{ and } p \equiv 3 \pmod 4, \\ 0 & \text{otherwise.} \end{cases}$$

With this choice of $\gamma_1(p)$ we have

$$\frac{\gamma_1(p)}{p-\gamma_1(p)} = \frac{g^{**}(p)}{\varphi(p)}$$

and one can easily check $\gamma_1(p) = 1 + O(1/p)$. By an argument identical to the proof of Lemma 2.7.3, we can evaluate the sum in (2.8.17) as

$$y^{(J)}_{r_1,\dots,r_k}\big|_{r_j=1\ \forall j\in J} = B\bigg(\prod_{i\in I}\frac{\varphi(r_i)}{r_i}\bigg)\int_0^1 F\bigg(\frac{\log r_1}{\log R},\dots,t_m,\dots,\frac{\log r_k}{\log R}\bigg)\frac{\mathrm{d}t_m}{\sqrt{t_m}} + O\bigg(\frac{F_{\max}B}{D_0}\bigg),$$

which proves (i). If $J=\{m,l\}$ then, again using Proposition 2.8.3, we find

$$\begin{aligned} y^{(J)}_{r_1,\dots,r_k}\big|_{r_j=1\ \forall j\in J} &= \sum_{e_m,e_l}\bigg(\prod_{j=m,l}\frac{g^{**}(e_j)}{\varphi(e_j)}\bigg)F\bigg(\frac{\log r_1}{\log R},\dots,\frac{\log e_m}{\log R},\dots,\frac{\log e_l}{\log R},\dots,\frac{\log r_k}{\log R}\bigg) \\ &\quad + O\bigg(\frac{F_{\max}B^2}{D_0}\bigg). \end{aligned} \tag{2.8.18}$$

Take the sum over e_l first. Consider the function

$$\gamma_2(p) = \begin{cases} \frac{p}{1+\frac{\varphi(p)}{g^{**}(p)}} & \text{if } p\nmid W\prod_{i\in I}r_ie_m \text{ and } p\equiv 3 \pmod 4, \\ 0 & \text{otherwise.}\end{cases}$$

Reasoning as above, the sum on the right hand side of (2.8.18) becomes

$$\begin{aligned} B\bigg(\prod_{i\in I}\frac{\varphi(r_i)}{r_i}\bigg)\sum_{e_m}\frac{g^{**}(e_m)}{e_m}\int_0^1 F\bigg(\frac{\log r_1}{\log R},\dots,\frac{\log e_m}{\log R},\dots,t_l,\dots,\frac{\log r_k}{\log R}\bigg)\frac{\mathrm{d}t_l}{\sqrt{t_l}} \\ + O\bigg(\frac{F_{\max}B^2}{D_0}\bigg). \end{aligned}$$

We can evaluate this sum in much the same way, this time using the function

$$\gamma_3(p) = \begin{cases} \frac{p}{1+\frac{p}{g^{**}(p)}} & \text{if } p\nmid W\prod_{i\in I}r_i \text{ and } p\equiv 3 \pmod 4, \\ 0 & \text{otherwise,}\end{cases}$$

to get the stated result. □

If we define the (identity) operator

$$I_{r_1,\dots,r_k}(F) = F\bigg(\frac{\log r_1}{\log R},\dots,\frac{\log r_k}{\log R}\bigg),$$

then the results of Corollary 2.8.5 can be concisely written as

$$y^{(J)}_{r_1,\dots,r_k}\bigg|_{r_j=1\ \forall j\in J} = B^{|J|}\bigg(\prod_{i\in I}\frac{\varphi(r_i)}{r_i}\bigg)^{|J|}I_{r_1,\dots,r_k;J}(F) + O\bigg(\frac{F_{\max}B^{|J|}}{D_0}\bigg)$$

for $|J|\in\{0,1,2\}$. Here we have used $I_{r_1,\dots,r_k;J}(F)$ to denote $I_{r_1,\dots,r_k;j:j\in J}(F)$. We are now in a position to prove the remaining part of Lemma 2.6.6.

Proof of Lemma 2.6.6 part (iii). We can write the operators in the statement of Lemma 2.6.6 as follows:

$$L(F) = \int_0^1 \dots \int_0^1 \Big[I(F)\Big]^2 \prod_{i=1}^{k} \frac{\mathrm{d}x_i}{\sqrt{x_i}},$$
$$L_m(F) = \int_0^1 \dots \int_0^1 \Big[I_m(F)\Big]^2 \prod_{\substack{i=1\\ i\neq m}}^{k} \frac{\mathrm{d}x_i}{\sqrt{x_i}},$$
$$L_{m,l}(F) = \int_0^1 \dots \int_0^1 \Big[I_{m,l}(F)\Big]^2 \prod_{\substack{i=1\\ i\neq m,l}}^{k} \frac{\mathrm{d}x_i}{\sqrt{x_i}},$$

where we have defined

$$I(F) = F(x_1, \dots, x_k),$$
$$I_m(F) = \int_0^1 F(x_1, \dots, x_k) \frac{\mathrm{d}x_m}{\sqrt{x_m}},$$
$$I_{m,l}(F) = \int_0^1 \bigg(\int_0^1 F(x_1, \dots, x_k) \frac{\mathrm{d}x_m}{\sqrt{x_m}} \bigg) \frac{\mathrm{d}x_l}{\sqrt{x_l}}.$$

From Proposition 2.8.1 we see that

$$S_J = \sum_{\substack{u_1,\dots,u_k\\ u_j=1\ \forall j\in J}} \frac{(y^{(J)}_{u_1,\dots,u_k})^2}{\prod_{i\in I} f^*(u_i)} + O\bigg(\frac{(y^{(J)}_{\max})^2 B^{|I|}}{D_0}\bigg). \tag{2.8.19}$$

From Corollary 2.8.5, for $|J| \in \{0,1,2\}$, we have

$$(y^{(J)}_{r_1,\dots,r_k})^2\Big|_{r_j=1\ \forall j\in J} = B^{2|J|}\bigg(\prod_{i\in I}\frac{\varphi(r_i)}{r_i}\bigg)^{2|J|}\Big[I_{r_1,\dots,r_k;J}(F)\Big]^2 + O\bigg(\frac{F_{\max}^2 B^{2|J|}}{D_0}\bigg).$$

Substituting this into (2.8.19), and using (2.8.16), yields

$$S_J = B^{2|J|} \sum_{\substack{u_1,\dots,u_k\\ u_j=1\ \forall j\in J\\ (u_i,u_j)=1\ \forall i\neq j\\ (u_i,W)=1\ \forall i\\ p|u_i\Rightarrow p\equiv 3 \pmod 4}} \prod_{i\in I} \frac{\mu^2(u_i)\varphi(u_i)^{2|J|}}{f^*(u_i)u_i^{2|J|}} \Big[I_{u_1,\dots,u_k;J}(F)\Big]^2$$
$$+ O\bigg(\frac{F_{\max}^2 B^{2|J|}}{D_0} \sum_{\substack{u_1,\dots,u_k\\ u_j=1\ \forall j\in J\\ (u_i,W)=1\ \forall i\\ p|u_i\Rightarrow p\equiv 3 \pmod 4}} \prod_{i\in I}\frac{\mu^2(u_i)}{f^*(u_i)}\bigg) + O\bigg(\frac{F_{\max}^2 B^{k+|J|}(\log\log R)^2}{D_0}\bigg).$$

The first error contributes

$$\ll \frac{F_{\max}^2 B^{2|J|}}{D_0}\Bigg(\sum_{\substack{u\leq R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u_i)}{f^*(u_i)}\Bigg)^{|I|} \ll \frac{F_{\max}^2 B^{k+|J|}}{D_0}.$$

For the main term, if $(u_i, u_j) \neq 1$ then they must be divisible by a prime $q > D_0$ with $q \equiv 3 \pmod 4$. In this case we get a contribution

$$\ll F_{\max}^2 B^{2|J|} \sum_{\substack{q>D_0\\q\equiv 3 \pmod 4}} \sum_{\substack{u_1,\dots,u_k\\u_j=1\ \forall j\in J\\(u_i,W)=1\ \forall i\\p|u_i\Rightarrow p\equiv 3 \pmod 4\\q|u_i,u_j}} \prod_{i\in I} \frac{\mu^2(u_i)\varphi(u_i)^{2|J|}}{f^*(u_i)u_i^{2|J|}}$$

$$\ll F_{\max}^2 B^{2|J|}\Bigg(\sum_{\substack{u\leq R\\(u,W)=1\\p|u\Rightarrow p\equiv 3 \pmod 4}} \frac{\mu^2(u)\varphi(u)^{2|J|}}{f^*(u)u^{2|J|}}\Bigg)^{|I|} \sum_{q>D_0} \frac{\varphi(q)^{4|J|}}{f^*(q)^2 q^{4|J|}} \ll \frac{F_{\max}^2 B^{k+|J|}}{D_0}.$$

Thus this constraint can be removed at the cost of a negligible error and we are left with

$$S_J = B^{2|J|} \sum_{\substack{u_1,\dots,u_k\\u_j=1\ \forall j\in J\\(u_i,W)=1\ \forall i\\p|u_i\Rightarrow p\equiv 3 \pmod 4}} \prod_{i\in I} \frac{\mu^2(u_i)\varphi(u_i)^{2|J|}}{f^*(u_i)u_i^{2|J|}} \Big[I_{u_1,\dots,u_k;J}(F)\Big]^2 + O\Bigg(\frac{F_{\max}^2 B^{k+|J|}(\log\log R)^2}{D_0}\Bigg).$$

Now, since

$$\frac{\varphi(p)^{2|J|}}{f^*(p)p^{2|J|}} = \frac{1}{p} + O\Big(\frac{1}{p^2}\Big),$$

we can evaluate this multidimensional sum by applying Lemma 2.7.3 $|I| = k - |J|$ times. We obtain

$$S_J = B^{k+|J|}L_J(F) + O\Bigg(\frac{F_{\max}^2 B^{k+|J|}(\log\log R)^2}{D_0}\Bigg).$$

This completes the proof of Lemma 2.6.6. □

Chapter 3

On the asymmetric additive energy of polynomials

We prove a general result concerning the paucity of integer points on a certain family of 4-dimensional affine hypersurfaces. As a consequence, we deduce that integer-valued polynomials have small asymmetric additive energy.

3.1 Introduction

Given a non-zero polynomial $f \in \mathbb{Z}[x]$ of degree $d \geq 3$, an integer $k \in \mathbb{Z}$, and a parameter $B \geq 1$, we let $E_f(B;k)$ denote the number of integer solutions to the equation

$$f(x_1) + f(x_2) = f(x_3) + f(x_4) + k \tag{3.1.1}$$

inside the multi-dimensional box

$$S(B) = \{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4_{>0} : \max_i x_i \leq B\}. \tag{3.1.2}$$

Following Baker, Munsch and Shparlinski [1], when k is a fixed, non-zero integer, we call $E_f(B;k)$ the *asymmetric* additive energy of the polynomial f inside the box $S(B)$ with respect to k. If $k = 0$ we simply call $E_f(B;0)$ the *symmetric* additive energy of the polynomial f inside the box $S(B)$.

The latter case has been particularly well-studied in the literature, and here we have results available for any polynomial f. In this case, we immediately see there are $2B^2$ diagonal solutions to equation (3.1.1) of the form (a, b, a, b) and (a, b, b, a). Based on standard probabilistic heuristics, one would expect there to be very few other solutions. Indeed, it is now known that one has an asymptotic of the form

$$E_f(B;0) = 2B^2 + O_f(B^{2-\delta}) \tag{3.1.3}$$

for some explicit constant $\delta > 0$. This was first established in the special case $f(x) = x^d$ by Hooley [16, 18], with results for more general polynomials f being established later by various authors. We refer the reader to Browning's excellent paper [4] for a brief history of this interesting problem.

The case where k is a fixed, non-zero integer has received less attention. However, recently, it is has been realised that estimates in this alternate setting would have interesting applications. This is the regime we study. In this case, in the absence of any diagonal solutions, one would simply expect there to be very few solutions to equation (3.1.1). The estimate $E_f(B;k) \ll_{f,\epsilon} B^{2+\epsilon}$ is essentially trivial and follows from an application of the divisor bound. Hence in this situation one expects a bound of the form

$$E_f(B;k) \ll_f B^{2-\delta} \tag{3.1.4}$$

to hold. We remark that this estimate is uniform in k, and this is important in the interest of applications. Currently, a bound like (3.1.6) is only known in the special case when $f(x) = x^d$ and either $d = 3$ or $d \geq 5$. This is essentially due to Hooley [16] in the former case and Marmon [20] in the latter.

In this chapter, we prove a bound of type (3.1.4) holds for an arbitrary polynomial f. In other words, we establish that polynomials have small asymmetric additive energy.

Theorem 3.1.1. *Fix a polynomial $f \in \mathbb{Z}[x]$ of degree $d \geq 3$. For any non-zero integer k we have*

$$E_f(B;k) \ll_f B^{2-1/(50d)}. \tag{3.1.5}$$

The zero-set of equation (3.1.1) defines a 4-dimensional affine hypersurface over $\mathbb{Q}$. It is natural to consider this geometric object abstractly. In doing so, we are led to consider a family of 4-dimensional affine hypersurfaces which generalise equation (3.1.1). We are then able to prove the following result concerning the family, from which Theorem 3.1.1 will follow as a corollary. This general result may have independent interest.

Theorem 3.1.2. *Fix a polynomial $f \in \mathbb{Z}[x,y]$ of degree d with zero constant term, a polynomial $g \in \mathbb{Z}[x,y]$ of degree $(d-1)$, and non-zero integers $abk \neq 0$. Write f_d (resp. g_{d-1}) for the top-degree homogenous parts of f (resp. g), and let $M_{f,g}(B;k)$ denote the number of integer solutions to the equation*

$$f(x_1,x_2) = (ax_3 - bx_4)g(x_3,x_4) + k \tag{3.1.6}$$

inside the multi-dimensional box $S(B)$ defined in equation (3.1.2). Suppose, in addition, the following constraints hold:

1. *The affine curve $\{f(x,y)=k\} \subset \mathbb{A}^2_{\mathbb{Q}}$ does not contain a line.*
2. *The projective variety $\{f_d(x,y)=0\} \subset \mathbb{P}^1_{\mathbb{Q}}$ is smooth and does not contain any non-constant repeated components.*
3. *The projective variety $\{(ax-by)g_{d-1}(x,y)=0\} \subset \mathbb{P}^1_{\mathbb{Q}}$ does not contain any non-constant repeated components.*

If $d=4$ we additionally suppose:

(4) The projective variety

$$\left\{\frac{1}{a}\frac{\partial g_{d-1}}{\partial x}\left(\frac{x}{a},\frac{y}{b}\right)+\frac{1}{b}\frac{\partial g_{d-1}}{\partial y}\left(\frac{x}{a},\frac{y}{b}\right)=0\right\} \subset \mathbb{P}^1_{\mathbb{Q}}$$

does not contain any non-constant repeated components.

Then,

$$M_{f,g}(B;k) \ll_{f,g,a,b} B^{2-1/(50d)}. \tag{3.1.7}$$

We remark here that one can show the estimate $M_{f,g}(B;k) \ll_{f,g,a,b,\epsilon} B^{2+\epsilon}$ via a divisor-bound argument, and without constraints on f and g this is essentially optimal. Thus, one may wonder which of the assumptions of Theorem 3.1.2 are necessary in order for there to be significantly fewer solutions. We clearly require (1), as otherwise we would be able to generate $O(B^2)$ "trivial solutions" lying on lines contained in the hypersurface. Interestingly, (1) is *not* sufficient; one also requires (3). This is illustrated by the following example: there are $O(B^2)$ solutions to the equation

$$x_1^4 - x_2^4 = (x_3 - x_4)(x_3^3 - x_4^3 - 3x_4^2 - 3x_4) + 1$$

of the form $(a, a, b+1, b)$. In this example (1) is satisfied (see Lemma 3.1.5 below) but (3) is not, as the top-degree homogenous part of the RHS contains the square-factor $(x_3 - x_4)^2$. On the other hand, (2) and (4) are present purely to facilitate our proof method. Presumably, both of these assumptions could be removed if one had a different approach. We discuss this in more detail in Section 3.2.

We have written the conclusion (3.1.7) of Theorem 3.1.2 in the form stated for simplicity; in view of applications, the most important aspect is that we obtain

a power saving over the trivial bound. However, our proof actually yields the better bounds:

$$M_{f,g}(B;k) \ll_{f,g,a,b,\epsilon} \begin{cases} B^{2-1/(3d)+\epsilon} & \text{if } d \in \{3,4\}, \\ B^{1+\epsilon}(B^{1/2} + B^{2/\sqrt{d}+1/(d-1)-1/((d-2)\sqrt{d})}) & \text{if } d \geq 5. \end{cases}$$

The bounds present in Theorem 3.1.1 can be improved accordingly. We will deduce Theorem 3.1.1 from Theorem 3.1.2 in Section 3.1.2 below. As mentioned above, Theorem 3.1.1 has various applications in the literature. We discuss these now.

3.1.1 Applications

In [7] Chen, Kerr, Maynard, and Shparlinski were interested in showing that Weyl sums typically exhibit square-root cancellation. A key input to their method was an estimate of the form

$$\sum_{0<|k|\leq 4B^d} \frac{E_f(B;k)}{k} \ll_f B^{2-\kappa_d}$$

for the monomial $f(x) = x^d$, where $\kappa_d > 0$ is a constant depending only on d (cf. proof of [7, Lemma 4.3]). In the paper they establish such an estimate when $d = 3$ and $d \geq 5$, using work of Hooley [16] and Marmon [20]. This just left the case $d = 4$. It is clear that, with Theorem 3.1.1 applied to the polynomial $f(x) = x^4$, we can now extend [7, Theorem 2.1] to cover the case $d = 4$ and hence complete this aspect of the classification of Weyl sums.

Corollary 3.1.3 (Square-root cancellation in Weyl sums almost always)**.** *There exist positive constants c and C such that, for any $d \geq 3$ and any sequence of complex weights $(a_n)_{n=1}^{\infty}$ with $|a_n| = 1$, the set*

$$\left\{x \in [0,1) : cN^{1/2} \leq \left|\sum_{n=1}^{N} a_n e^{2\pi i x n^d}\right| \leq CN^{1/2} \text{ for infinitely many } N \in \mathbb{N}\right\}$$

has full Lebesgue measure.

As a further application of Theorem 3.1.1, in recent work Baker, Munsch and Shparlinski [1] proved a general result which enables one to establish large sieve inequalities for a general class of sparse sequences, provided that one has good estimates available for the symmetric and asymmetric additive energy of the sequence. Using the work [7] described above, the authors were able to establish large sieve inequalities for the monomial sequences $f(x) = x^d$ when $d = 3$ or $d \geq 5$. The authors also proved a weaker result about general polynomial sequences by

alternative methods [1, Theorem 1.5].

By using the new estimates contained in Theorem 3.1.1, we are able to establish their first result for the monomial $f(x) = x^4$ (albeit with a slightly weaker exponent), and also improve their result concerning polynomial sequences. A direct application of [1, Theorem 1.1] to the appropriate sequence yields the following.

Corollary 3.1.4 (Large sieve inequality for polynomial sequence)**.** *Fix $\epsilon > 0$. For any sequence of complex weights $(a_n)_{n=1}^{\infty}$ and $f \in \mathbb{Z}[x]$ of degree $d \geq 3$ and $Q^d \leq N \leq Q^{2d}$ we have*

$$\sum_{q=1}^{Q} \sum_{\substack{a=1 \\ (a,f(q))=1}}^{f(q)} \left| \sum_{n=M+1}^{M+N} a_n e\left(\frac{2\pi i a n}{f(q)}\right) \right|^2 \ll_{f,\epsilon} (NQ^{1/2} + N^{3/4}Q^{d/2+2-1/(50d)})Q^{\epsilon} \sum_{n=M+1}^{M+N} |a_n|^2.$$

It is likely that further applications of Theorem 3.1.1 will appear in the literature. We now show how Theorem 3.1.2 implies Theorem 3.1.1.

3.1.2 Deducing Theorem 3.1.1 from Theorem 3.1.2

Fix a polynomial $p \in \mathbb{Z}[x]$ of degree d and a non-zero integer k. Let us write $p(x) = \sum_{i=0}^{d} a_i x^i$. We would like to apply Theorem 3.1.2, taking

$$f(x, y) = (x - y)g(x, y) = p(x) - p(y). \tag{3.1.8}$$

First let us check the constraints on f are satisfied. The homogenous polynomial $f_d(x, y)$ is clearly smooth, and moreover over $\overline{\mathbb{Q}}$ we have the factorisation

$$f_d(x, y) = a_d(x^d - y^d) = a_d \prod_{\xi^d=1} (x - \xi y), \tag{3.1.9}$$

which shows that f_d has no repeated factors. Thus we just need to check that the curve $f(x, y) = k$ contains no rational lines. For this we have the following lemma. Note that in this special case we can prove the stronger assertion that $f(x, y) = k$ contains no lines over $\overline{\mathbb{Q}}$.

Lemma 3.1.5. *For any $p \in \mathbb{Z}[x]$ and non-zero integer k, the affine curve*

$$\{p(x) - p(y) = k\} \subset \mathbb{A}^2_{\overline{\mathbb{Q}}}$$

contains no lines.

Proof. Suppose for a contradiction that this affine curve contains a line. It is clear that in this case there must exist a parametrisation of this line of the form $(x, y) = (t, \alpha t + \beta)$ with $\alpha, \beta \in \overline{\mathbb{Q}}$. This leads us to the polynomial identity

$$p(t) = p(\alpha t + \beta) + k \tag{3.1.10}$$

in $\overline{\mathbb{Q}}[t]$. Comparing leading-term coefficients, we see that $\alpha^d = 1$. Then comparing the coefficients of t^{d-1}, we may solve for β and find that $\beta = a_{d-1}(\alpha - 1)/(da_d)$. If $\alpha = 1$ then we must have $\beta = 0$, and then setting $t = 0$ in (3.1.10) yields $k = 0$, a contradiction. Otherwise, setting $t = -\beta/(\alpha - 1)$ yields the same contradiction. □

It just remains to check our constraints on g. It follows from the above that $(x - y)g_{d-1}(x, y)$ is square-free. Finally, when $d = 4$, we must additionally check that the gradient of g_{d-1} is square-free. In this case, $g_3(x, y) = a_4(x^3 + x^2y + xy^2 + y^3)$ and we have

$$\frac{\partial g_3}{\partial x}(x, y) + \frac{\partial g_3}{\partial y}(x, y) = 4a_4(x^2 + xy + y^2) = 4a_4(x - \omega y)(x - \overline{\omega} y) \tag{3.1.11}$$

where $\omega = (-1 + \sqrt{3}i)/2$. Hence the gradient is square-free. This completes the check of all the constraints. Since $E_p(B; k) = M_{f,g}(B; k)$, it is now clear that Theorem 3.1.1 follows from Theorem 3.1.2.

3.2 Proof outline of Theorem 3.1.2

The proof of Theorem 3.1.2 will split into two cases, depending on whether $d \in \{3, 4\}$ or $d \geq 5$. In the former case we will apply a sieve method, and in the latter we will apply the determinant method.

The following notation will be useful in this section and throughout the chapter: whenever $F \in \mathbb{Z}[x_1, \ldots, x_n]$ is a polynomial in n variables, we let $M_F(B)$ denote the number of solutions to the equation $F(x_1, \ldots, x_n) = 0$ inside the multi-dimensional box $S(B)$ defined in equation (3.1.2). (Although this overloads the notation $M_{f,g}(B; k)$ used in Theorem 3.1.2, it will always be clear from the context which quantity we are referring to.)

3.2.1 The case $d \in \{3, 4\}$ and the polynomial sieve method

When $d \in \{3, 4\}$, we will establish Theorem 3.1.2 via a sieve method. The sieve can be viewed as a "local" method, where one attempts to rule out the existence of lots of "global" solutions by ruling out the possibility of lots of "local" solutions modulo p for "many" primes p. Hooley [15, 16, 18] was the first to appreciate how sieves could be applied in this context. We will find it convenient to use a particularly flexible sieve method called the *polynomial sieve* due to Browning [4]. We defer the statement of the main sieve proposition to Section 3.5.

Let us recall equation (3.1.6) where for simplicitly we assume $a = b = 1$:

$$f(x_1, x_2) = (x_3 - x_4)g(x_3, x_4) + k. \tag{3.2.1}$$

A key property of the above equation which enables the sieve method to work is the presence of a linear factor on the RHS. If we let $h = (x_3 - x_4)$ and eliminate x_4 (say) in the above equation, we may equivalently examine

$$f(x_1, x_2) = hg(x_3, x_3 - h) + k. \tag{3.2.2}$$

The argument then proceeds by first fixing the value of h, and then counting solutions to the simpler equation in (x_1, x_2, x_3) which remains. We can then apply the polynomial sieve to detect solutions to this equation where the variables (x_1, x_2) are constrained to satisfy the congruence $f(x_1, x_2) \equiv k \pmod{h}$. By applying the sieve to a congruenced set in this manner, we are able to retain the trivial bound at this step of the argument. This is crucial, as it allows one to obtain a power saving for $M_{f,g}(B; k)$ provided one gains only a small power of B from the sieve estimates.

This means we would like to sieve by primes p of size $O(B^{\delta})$ (say), which in turn requires one to understand our variables in arithmetic progressions with modulus of size $O(B^{1+2\delta})$. The modulus is slightly larger than the length of summation, but this difficulty can be overcome by a completion of sums argument. This leaves one with certain exponential sums over algebraic varieties to estimate. Hence, to execute the sieve method effectively, one has recourse to the deep work of Weil [28] and Deligne [9] concerning the Riemann Hypothesis for curves and higher dimensional varieties over finite fields. This argument works for a generic value of h, but in practice there might exist some exceptional values of h for which certain auxiliary varieties (depending on h) fail to be smooth. However, using elimination theory, it

is possible to show that there can't be too many of these exceptional values. One can then estimate the contribution from these cases via other methods, such as the Bombieri-Pila method (see below).

3.2.2 The case $d \geq 5$ and the determinant method

For the complementary case, when $d \geq 5$, we will use the determinant method. The determinant method can be viewed as a "global" method. The general philosophy is that any "large" contribution to the count $M_{f,g}(B)$ must come from rational points lying on lower dimensional varieties contained inside the hypersurface. This method has its origins in the pioneering work of Bombieri-Pila [3]. It was then greatly developed at a later date by Heath-Brown [13], and has enjoyed various refinements since due to a variety of authors.

Again, recalling equation (3.1.6) with $a = b = 1$, we wish to count points on the 3-dimensional surfaces

$$f(x_1, x_2) = (x_3 - n)g(x_3, n) + k \subset \mathbb{A}^3_{\mathbb{Q}} \tag{3.2.3}$$

for each fixed integer n. Thus, as in the sieve method, we begin by considering a simpler object of smaller dimension. However, in the former case it was crucial we had the linear factor on the RHS and our change of variables incorporated this information. This is less important here (however we will still make use of the linear factor later).

We will apply the determinant method to equation (3.2.3) in the form of the following result, which is implicit in the proof of [5, Theorem 3].

Proposition 3.2.1 (Browning and Heath-Brown)**.** *Let $F \in \mathbb{Z}[x, y, z]$ be a non-singular polynomial of degree $d \geq 4$. Then*

$$M_F(B) \ll_{d,\epsilon} M_F^{lines}(B) + B^{1/2+\epsilon} + B^{2/\sqrt{d}+1/(d-1)-1/(\sqrt{d}(d-2))+\epsilon},$$

where $M_F^{lines}(B)$ counts the number of integer points lying on lines contained in the hypersurface $\{F = 0\} \subset \mathbb{A}^3_{\mathbb{Q}}$ inside the box $S(B)$ defined by equation (3.1.2).

We note that the last error term exceeds B when $d < 5$. This is the reason we cannot apply the determinant method when $d \in \{3, 4\}$.

Therefore, to obtain a power saving for $M_{f,g}(B;k)$ via the determinant method, it is sufficient to have control over the possible lines which can appear in the surfaces (3.2.3). Here it is important we are averaging over n; for certain values of n lines may exist and hence contribute a larger amount to $M_{f,g}(B;k)$, however, one can show via elementary means that there cannot be too many values of n for which this can occur. We note that our argument will also make use of the linear factor on the RHS of (3.2.3).

We remark that Proposition 3.2.1 only applies when the surface (3.2.3) is smooth. This will be true for a generic choice of n. Thus we arrive at a similar situation to that described above with the sieve argument, where we must handle exceptional cases via different methods. For these values we will use the Bombieri-Pila method. We state the main result we will use here. The following appears as [3, Theorem 5].

Proposition 3.2.2 (Bombieri-Pila)**.** *Let $F \in \mathbb{Z}[x,y]$ be an absolutely irreducible curve of degree $d \geq 2$. Then*

$$M_F(B) \ll_{d,\epsilon} B^{1/d+\epsilon}.$$

3.2.3 Some basic facts about discriminant polynomials

Throughout the proof of Theorem 3.1.2 we will encounter various auxiliary curves and surfaces which depend on an integer parameter h (say). For both the determinant method and the polynomial sieve method to work, we require these varieties to be smooth for"most" choices of h. This in turn amounts to showing that certain discriminant polynomials, which by definition will be polynomials in the parameter h, are not the zero polynomial.

Our method of proving this is to extract the leading coefficient using limiting arguments. This leading coefficient will generically be non-zero, and only vanish if our polynomials are degenerate in some way. Our additional assumptions (2) and (4) in the statement of Theorem 3.1.2 ensure that we avoid these cases. It is possible that these additional assumptions could be removed if one had a different way of proving these discriminant polynomials didn't vanish.

With this in mind, we collect here a few basic facts about discriminant polynomials which we will use without comment throughout this chapter. Given a polynomial $f \in \mathbb{Q}[x]$ of degree d, leading coefficient a_d, and roots $\lambda_1, \dots, \lambda_d \in \overline{\mathbb{Q}}$, we

form its discriminant polynomial with respect to x, which we write as $\mathrm{Disc}_x[f(x)]$ by the formula

$$\mathrm{Disc}_x[f(x)] = (-1)^{d(d-1)/2} a_d^{d(d-1)} \prod_{i \neq j} (\lambda_i - \lambda_j). \tag{3.2.4}$$

The discriminant polynomial satisfies the following properties:

(i) $\mathrm{Disc}_x[f(x)]$ is a polynomial in the coefficients of f.

(ii) $\mathrm{Disc}_x[f(x)]$ vanishes if and only if f and f' possess a common factor over $\mathbb{Q}$. In particular, if f has no non-constant repeated factors over $\mathbb{Q}$ then $\mathrm{Disc}_x[f(x)] \neq 0$.

(iii) For any real numbers a, b and c we have the transformation formula

$$\mathrm{Disc}_x[af(bx+c)] = a^{2d-2} b^{d(d-1)} \mathrm{Disc}_x[f(x)]. \tag{3.2.5}$$

3.3 Notation

We will use both Landau and Vinogradov asymptotic notation throughout this chapter. B will denote a large integer, and all asymptotic notation is to be understood as referring to the limit as $B \to \infty$. We allow any implied constants to depend implicitly on the variables f, g, a and b, without specifying so. By this, we mean dependencies on the coefficients of f and g and also on the degree d. Any dependencies of the implied constants on other parameters A will be denoted by a subscript, for example $X \ll_A Y$ or $X = O_A(Y)$, unless stated otherwise. We let ϵ denote a small positive constant, and we adopt the convention it is allowed to change at each occurrence, and even within a line.

If k is a field, we let $\mathbb{A}^n_k$ (resp. $\mathbb{P}^n_k$) denote n-dimensional affine (resp. projective) space over k. If $F \in \mathbb{Z}[x_1, \ldots, x_n]$ we let $\{F = 0\} \subset \mathbb{A}^n_{\mathbb{Q}}$ denote the n-dimensional affine hypersurface generated by F over $\mathbb{Q}$. By slight abuse of notation, we may write this as $F = 0 \subset \mathbb{A}^n_{\mathbb{Q}}$, or even simply $F \subset \mathbb{A}^n_{\mathbb{Q}}$. We adopt similar conventions whenever F is homogenous and generates a projective hypersurface. The hypersurface defined by F is said to be *smooth* over $\mathbb{Q}$ if the system of equations

$$F(y_1, \ldots, y_n) = \frac{\partial F}{\partial x_1}(y_1, \ldots, y_n) = \ldots = \frac{\partial F}{\partial x_d}(y_1, \ldots, y_n) = 0$$

has no solutions with $(y_1, \ldots, y_n) \in \mathbb{A}^n_{\mathbb{Q}}$ in the affine case or $[y_1 : \ldots : y_n] \in \mathbb{P}^n_{\mathbb{Q}}$ in the projective case.

We let f_i (resp. g_i) denote the homogenous part of f (resp. g) of degree i. Thus, we may write

$$f(x,y) = \sum_{i=0}^{d} f_i(x,y), \quad g(x,y) = \sum_{i=0}^{d-1} g_i(x,y).$$

We will frequently use assumption (1) in Theorem 3.1.2 which says that the curve $\{f(x,y) = k\} \subset \mathbb{A}^2_{\mathbb{Q}}$ contains no lines. We note that the curve may well contain lines over the larger field $\overline{\mathbb{Q}}$, but these lines cannot simply be reparametrisations of lines over $\mathbb{Q}$ (e.g. $\sqrt{2}x + \sqrt{2}y = \sqrt{2}$). To this end, the following definition is useful: we say a line $\{\alpha x + \beta y + \gamma = 0\} \subset \mathbb{A}^2_{\overline{\mathbb{Q}}}$ is *definable over* $\mathbb{Q}$ if there exists $\lambda \in \overline{\mathbb{Q}}$ and $a, b, c \in \mathbb{Q}$ such that $\alpha x + \beta y + \gamma = \lambda(ax + by + c)$. With this definition, our assumption is precisely that the curve $f(x,y) = k$ doesn't contain any lines definable over $\mathbb{Q}$.

3.4 Proof of Theorem 3.1.2 in the case $d \geq 5$.

Fix $f, g \in \mathbb{Z}[x,y]$ as in the statement of Theorem 3.1.2, with $d \geq 5$. In this section we prove the Theorem 3.1.2 in this regime. Recalling equation (3.1.6), we wish to count integer points on the affine hypersurface

$$f(x_1, x_2) = (ax_3 - bx_4)g(x_3, x_4) + k \subset \mathbb{A}^4_{\mathbb{Q}}. \tag{3.4.1}$$

The method proceeds by fixing the value of x_4, which we now call n, and considering the resulting 3-dimensional affine surface

$$f(x_1, x_2) = (ax_3 - bn)g(x_3, n) + k \subset \mathbb{A}^3_{\mathbb{Q}}, \tag{3.4.2}$$

which we call Γ_n. For later purposes, we let $\Gamma_n^{\mathrm{proj}}(x_1, x_2, x_3, w) \subset \mathbb{P}^3_{\mathbb{Q}}$ denote the projectivisation of this surface. Recalling our notation so far, we can write

$$M_{f,g}(B; k) = \sum_{1 \leq n \leq B} M_{\Gamma_n}(B). \tag{3.4.3}$$

First let us deal with a degenerate situation, where n is such that $g(x_3, n)$ vanishes identically (as a polynomial in x_3).

Lemma 3.4.1. *Suppose n is such that $g(x_3, n)$ vanishes identically. Then*

$$M_{\Gamma_n}(B) \ll_\epsilon B^{3/2+\epsilon}.$$

Proof. Clearly

$$M_{\Gamma_n}(B) \ll B \cdot \#\{x_1, x_2 \in [1, B] \cap \mathbb{Z} : f(x_1, x_2) = k\}. \tag{3.4.4}$$

To evaluate this count, we can decompose our curve into $O(1)$ absolutely irreducible components and majorise by summing over each component. We can then apply Proposition 3.2.2 to each component. Components of degree ≥ 2 contribute $O_\epsilon(B^{1/2+\epsilon})$. By assumption, any components of degree 1 (i.e. lines) are not definable over $\mathbb{Q}$ and therefore contain at most 1 integer point, and so these contribute in total $O(1)$. Thus, this count is $O_\epsilon(B^{1/2+\epsilon})$, which yields the lemma. □

There can be at most $O(1)$ such values of n for which $g(x_3, n)$ vanishes identically, and so (3.4.3) becomes

$$M_{f,g}(B; k) = \sum_{\substack{1 \leq n \leq B \\ g(\cdot, n) \neq 0}} M_{\Gamma_n}(B) + O_\epsilon(B^{3/2+\epsilon}). \tag{3.4.5}$$

For these remaining values of n we would like to use Proposition 3.2.1 to estimate the corresponding $M_{\Gamma_n}(B)$. To do this we require the surface Γ_n to be smooth. Generically this will be the case, as the following lemma demonstrates.

Lemma 3.4.2. *Γ_n^{proj} is singular for at most $O(1)$ values of n.*

Proof. Write $g(x_3, x_4) = \sum_{i+j \leq d-1} e_{i,j} x_3^i x_4^j$. We first deal with possible singular points with $w = 0$. We can write Γ_n^{proj} as

$$\begin{aligned} f_d(x_1, x_2) + w f_{d-1}(x_1, x_2) = a e_{d-1,0} x_3^d + (a e_{d-2,1} n - b n e_{d-1,0} + a e_{d-2,0}) x_3^{d-1} w \\ + \text{ (terms involving } w^2). \end{aligned}$$

If $[r : s : t : 0]$ is a singular point, by considering the x_1 and x_2 derivatives, we see that necessarily

$$\frac{\partial f_d}{\partial x_1}(r, s) = \frac{\partial f_d}{\partial x_2}(r, s) = 0.$$

By Euler's identity, we see that $f_d(r, s) = 0$ also. As we are assuming f_d is smooth we must have $r = s = 0$. If $e_{d-1,0} \neq 0$ then the equation above yields $t = 0$, which is a contradiction. If $e_{d-1,0} = 0$ then necessarily $e_{d-2,1} \neq 0$ as otherwise $g_{d-1}(x_3, x_4)$ would contain a square factor of x_4^2. In this case the w derivative evaluated at $[0 : 0 : t : 0]$ yields

$$a(e_{d-2,1} n + e_{d-2,0}) t^{d-1} = 0.$$

Unless $n = -e_{d-2,0}/e_{d-2,1}$ we conclude again that $t = 0$. Thus there is at most 1 value of n for which Γ_n^{proj} contains a singular point with $w = 0$.

This leaves us to examine possible singular points with $w = 1$. For ease, let us write $G_n(x_3) = (ax_3 - bn)g(x_3, n)$ and denote by $G_n'(x_3)$ the derivative with respect to x_3. Again, by examining derivatives, it is clear that any singular point $[r : s : t : 1]$ must satisfy, in particular,

$$\frac{\partial f}{\partial x_1}(r, s) = \frac{\partial f}{\partial x_2}(r, s) = 0 \text{ and } G_n'(t) = 0.$$

Now, our assumption that f_d is square-free implies that the partial derivatives $\partial f/\partial x_1$ and $\partial f/\partial x_2$ are coprime and hence, by Bézout's theorem, they have at most $O(1)$ common zeros.[1] Thus, this system constrains r and s to at most $O(1)$ possible values. For each pair we must then solve the system

$$\begin{aligned} G_n(t) &= f(r, s), \\ G_n'(t) &= 0. \end{aligned}$$

We would like to show that this system is only solvable in t for at most $O(1)$ choices of n. If this were the case, it would follow that there are at most $O(1)$ values of n for which Γ_n^{proj} contains a singular point with $w = 1$. This, together with the above, would yield the conclusion of the lemma.

We will prove this via the following strategy, which will be used numerous times throughout the chapter: if the system is solvable then the discriminant

$$\text{Disc}_t[G_n(t) - f(r, s)]$$

will vanish identically. However, by definition, this will be a polynomial in n which generically will be non-zero and so only vanish for $O(1)$ values of n. Hence it is sufficient to prove that this discriminant is not identically zero. We prove this by extracting the leading coefficient. Our assumptions on f and g will then imply this leading coefficient doesn't vanish.

[1] If $\partial f/\partial x_1$ and $\partial f/\partial x_2$ have a common factor p then f must be of the form $f = p^2q + c$ for some constant c. By comparing homogenous parts of top-degree we see f_d will be divisible by a square in this case.

Now we have

$$\begin{aligned}\frac{G_n(nt)}{n^d} &= \frac{(at-b)g(nt,n)}{n^{d-1}} \\ &= \frac{(at-b)}{n^{d-1}}\sum_{i=0}^{d-1} g_i(nt,n) \\ &= (at-b)g_{d-1}(t,1) + O(n^{-1}).\end{aligned}$$

Thus, taking limits, we see that

$$\lim_{n\to\infty} \frac{G_n(nt)}{n^d} = (at-b)g_{d-1}(t,1). \tag{3.4.6}$$

By standard properties of discriminant polynomials, as detailed in Section 3.2.3, whenever $n \neq 0$ we can write

$$\mathrm{Disc}_t\left[\frac{G_n(nt)-f(r,s)}{n^d}\right] = \frac{\mathrm{Disc}_t[G_n(t)-f(r,s)]}{n^{(D-1)(2d-D)}},$$

where $1 \leq D \leq d$ is the degree of $G_n(t)$ as a polynomial in t. This is valid for any $n \neq 0$, and moreover both sides of equation (3.4.6) have the same degree D in t. Thus we may take the limit as $n \to \infty$ inside the discriminant, and it follows that

$$\lim_{n\to\infty} \frac{\mathrm{Disc}_t[G_n(t)-f(r,s)]}{n^{(D-1)(2d-D)}} = \mathrm{Disc}_t[(at-b)g_{d-1}(t,1)]$$

The RHS is non-zero by our assumption that $\{(ax-by)g_{d-1}(x,y)\} \subset \mathbb{P}^2_{\mathbb{Q}}$ is square-free. Thus, the discriminant polynomial has a non-zero leading coefficient. This completes the proof of the lemma. □

Before we can dispense with those values of n for which Γ_n is singular, we require some information about the possible lines which can be contained in level sets of the curve $\{f(x,y)=0\} \subset \mathbb{A}^2_{\overline{\mathbb{Q}}}$.

Lemma 3.4.3 (Lines contained in level sets of f)**.** *Let $f \in \mathbb{Z}[x_1,x_2]$ be such that f_d is not divisible by a square and let $l \in \overline{\mathbb{Q}}$. Then, if the variety*

$$\{f(x_1,x_2)=l\} \subset \mathbb{A}^2_{\overline{\mathbb{Q}}}$$

contains a line, this line must be equal to one of the possible lines listed below:

1. *The line parametrised by $(x_1,x_2) = (t, \alpha t+\beta)$ where $f_d(1,\alpha)=0$ and $\beta = -f_{d-1}(1,\alpha)/(\partial f_d/\partial y)(1,\alpha)$.*

2. *The line parametrised by* $(x_1, x_2) = (\gamma, t)$ *where* $\gamma = -f_{d-1}(0,1)/(\partial f_d/\partial x)(0,1)$. *(This case requires* $f_d(0,1) = 0$.*)*

Proof. Let us suppose that the level set $f(x_1, x_2) = l$ contains a line. This line can be parametrised by $(x_1, x_2) = (\lambda_1 t + \mu_1, \lambda_2 t + \mu_2)$, where all coefficients lie in $\overline{\mathbb{Q}}$ and λ_1, λ_2 are not both zero. We have the Taylor expansion

$$f(\lambda_1 t + \mu_1, \lambda_2 t + \mu_2) = \sum_{i=0}^{d} \sum_{j=0}^{i} \Bigg[\sum_{m+k=j} \frac{1}{k!}\frac{1}{m!}\frac{\partial^j f_i}{\partial x^k y^m}(\lambda_1, \lambda_2)\mu_1^k \mu_2^m \Bigg] t^{i-j}. \tag{3.4.7}$$

We consider two cases, depending on whether or not λ_1 is zero.

1. If $\lambda_1 \neq 0$ then our line may be parametrised by $(x_1, x_2) = (t, \alpha t + \beta)$ for some α and β. Now since we are assuming $f(t, \alpha t + \beta) = l$, we arrive at the following polynomial identity in $\overline{\mathbb{Q}}[t]$:

$$f_d(1,\alpha)t^d + \left[f_{d-1}(1,\alpha) + \beta \frac{\partial f_d}{\partial y}(1,\alpha) \right] t^{d-1} + \ldots = l.$$

   Since f_d is smooth, $f_d(1, \alpha)$ is a non-zero polynomial in α of degree at most d. Therefore, there are at most $O_d(1)$ choices of α for which the leading coefficient vanishes. For every such α, we must have $(\partial f_d/\partial y)(1, \alpha) \neq 0$ as otherwise the discriminant $\mathrm{Disc}_y[f_d(1, y)]$ would vanish, contradicting the fact f_d is square-free. The result follows by looking at the vanishing of the coefficient of t^{d-1}.

2. If $\lambda_1 = 0$ then necessarily $\lambda_2 \neq 0$. In this case our line may be parametrised by $(x_1, x_2) = (\gamma, t)$. Now

$$f(\gamma, t) = f_d(0,1)t^d + \left[f_{d-1}(0,1) + \gamma \frac{\partial f_d}{\partial x}(0,1) \right] t^{d-1} + \ldots.$$

   For the coefficient of t^d to vanish we must have $f_d(0, 1) = 0$. It follows that $(\partial f_d/\partial x)(0, 1) \neq 0$ as otherwise $f_d(x_1, x_2)$ would be divisible by the square x_1^2. The coefficient of t^{d-1} vanishing then implies $\gamma = -f_{d-1}(0,1)/(\partial f_d/\partial x)(0,1)$, as required.

□

From now on we let $\Lambda \subset \overline{\mathbb{Q}}$ consist of the set of α, β, γ defined in Lemma 3.4.3 above, whenever they exist. These numbers depend only on f_d and f_{d-1}, and it is clear that $|\Lambda| = O(1)$. In case (1) we must have $l = f(0, \beta)$ and in case (2) we must have $l = f(\gamma, 0)$.

We are now finally in a position to deal with the contribution from those n for which Γ_n^{proj} is singular.

Lemma 3.4.4. *We have*

$$\sum_{\substack{1\leq n\leq B\\ \Gamma_n^{proj}\ singular\\ g(\cdot,n)\neq 0}} M_{\Gamma_n}(B) \ll_\epsilon B^{3/2+\epsilon}.$$

Proof. There are $O(1)$ choices of x_3 for which $(ax_3-bn)g(x_3,n)=(l-k)$ and $l\in\{f(0,\beta),f(\gamma,0)\}_{\beta,\gamma\in\Lambda}$. For these values of x_3 we use the trivial bound $O(B)$ for the number of possible values of $x_1,x_2\in[1,B]\cap\mathbb{Z}$ for which $f(x_1,x_2)=l$. For the other $O(B)$ values of x_3, we claim that

$$\#\{x_1,x_2\in[1,B]\cap\mathbb{Z}: f(x_1,x_2)=(ax_3-bn)g(x_3,n)+k\}\ll_\epsilon B^{1/2+\epsilon}.$$

Indeed, this follows from Proposition 3.2.2 in much the same way as Lemma 3.4.1. We split our curve into absolutely irreducible components and sum over each component. By Lemma 3.4.3 we are avoiding any level set which could potentially contain a line over $\overline{\mathbb{Q}}$, and hence every absolutely irreducible component of our curve must have degree ≥ 2. By Proposition 3.2.2 we can therefore bound this count by $O_\epsilon(B^{1/2+\epsilon})$, as required. We are done as there are only $O(1)$ choices for n by Lemma 3.4.2 and only $O(1)$ choices for β,γ by Lemma 3.4.3. □

Lemma 3.4.4 together with equation (3.4.5) yields

$$M_{f,g}(B;k)=\sum_{\substack{1\leq n\leq B\\ \Gamma_n^{\mathrm{proj}}\ \mathrm{smooth}\\ g(\cdot,n)\neq 0}} M_{\Gamma_n}(B)+O_\epsilon(B^{3/2+\epsilon}). \tag{3.4.8}$$

We are now in a position to apply Proposition 3.2.1 to estimate each term in the sum. Let us analogously define $M_{\Gamma_n}^{\mathrm{lines}}(B)$ to count the number of integer points lying on a line contained in the surface $\{\Gamma_n=0\}\subset\mathbb{A}^3_{\mathbb{Q}}$. From Proposition 3.2.1, we conclude that

$$M_{f,g}(B;k)=\sum_{\substack{1\leq n\leq B\\ \Gamma_n^{\mathrm{proj}}\ \mathrm{smooth}\\ g(\cdot,n)\neq 0}} M_{\Gamma_n}^{\mathrm{lines}}(B)+O_\epsilon(B^{1+\epsilon}(B^{1/2}+B^{2/\sqrt{d}+1/(d-1)-1/((d-2)\sqrt{d})})). \tag{3.4.9}$$

We turn to understanding the lines which can appear in Γ_n. The reason we work projectively is so that we can apply the following lemma due to Colliot-Thélène, which can be found in [13, Appendix].

Lemma 3.4.5 (Colliot-Thélène)**.** *Suppose that $X \subset \mathbb{P}^3_{\mathbb{Q}}$ is a smooth projective surface of degree $d \geq 3$. Then there are $O_d(1)$ lines contained in X.*

The following proposition, reminiscent of Lemma 3.4.3 above, summarises our information about possible lines contained in the affine surfaces Γ_n.

Proposition 3.4.6 (Analysis of lines contained in Γ_n)**.** *Suppose f and g satisfy the hypotheses of Theorem 3.1.2 and let Λ be defined as in the remarks following Lemma 3.4.3. Fix a positive integer n for which $g(x_3, n)$ is not identically zero as a polynomial in x_3. Then, if the variety*

$$\{\Gamma_n = 0\} \subset \mathbb{A}^3_{\overline{\mathbb{Q}}}$$

contains a line, this line must be equal to one of the possible lines listed below:

1. *The line $x_2 = \alpha x_1 + \beta$, where $\alpha, \beta \in \Lambda$ and x_3 and n satisfy the equation $(ax_3 - bn)g(x_3, n) + k = f(0, \beta)$ with $f(0, \beta) \neq k$.*

2. *The line $x_1 = \gamma$, where $\gamma \in \Lambda$ and x_3 and n satisfy $(ax_3 - bn)g(x_3, n) + k = f(\gamma, 0)$ where $f(\gamma, 0) \neq k$. (This case requires $f_d(0, 1) = 0$.)*

3. *Lines which contain at most 1 integer point (x_1, x_2, x_3).*

Proof. Any line in the surface can be parametrised by $x_i = \lambda_i t + \mu_i$ for $i \in \{1, 2, 3\}$, where $\lambda_i, \mu_i \in \overline{\mathbb{Q}}$ and the λ_i are not all zero. This then leads to an equality of polynomials in $\overline{\mathbb{Q}}[t]$:

$$f(\lambda_1 t + \mu_1, \lambda_2 t + \mu_2) = [a(\lambda_3 t + \mu_3) - bn]g(\lambda_3 t + \mu_3, n) + k.$$

Our proof proceeds by a careful case analysis.

1. Suppose that $\lambda_3 = 0$ and $\lambda_1 \neq 0$. Then, by Lemma 3.4.3, our line must be equal to the line with parametrisation

   $$x_1 = t, \;\; x_2 = \alpha t + \beta, \;\; x_3 = \mu_3$$

   where $\alpha, \beta \in \Lambda$ and $x_3 = \mu_3$ must satisfy $(ax_3 - bn)g(x_3, n) + k = f(0, \beta)$. If $f(0, \beta) = k$ then, because we are assuming the curve $f(x, y) = k$ doesn't contain a line definable over $\mathbb{Q}$, we must have at least one of $\alpha, \beta \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$. But now the line $x_2 = \alpha x_1 + \beta$ contains at most one integer point (x_1, x_2).

2. Suppose that $\lambda_3 = 0$ and $\lambda_1 = 0$. Then, by Lemma 3.4.3, our line must equal the line with parametrisation

$$x_1 = \gamma, \;\; x_2 = t, \;\; x_3 = \mu_3$$

where $\gamma \in \Lambda$ and we see $x_3 = \mu_3$ must satisfy

$$f(\gamma, 0) = (ax_3 - bn)g(x_3, n) + k.$$

This case requires $f_d(0, 1) = 0$. From the definition of γ in Lemma 3.4.3, we see that $\gamma \in \mathbb{Q}$. We are assuming that $f(x, y) = k$ doesn't contain any lines definable over $\mathbb{Q}$, and so it follows that in this situation we must have $f(\gamma, 0) \neq k$.[2]

3. Suppose that $\lambda_3 \neq 0$. We may parametrise our line as follows:

$$x_1 = \tilde{\lambda}_1 t + \tilde{\mu}_1, \;\; x_2 = \tilde{\lambda}_2 t + \tilde{\mu}_2, \;\; x_3 = t,$$

where $\tilde{\lambda}_1, \tilde{\mu}_1, \tilde{\lambda}_2, \tilde{\mu}_2 \in \overline{\mathbb{Q}}$. Then we must examine

$$f(\tilde{\lambda}_1 t + \tilde{\mu}_1, \tilde{\lambda}_2 t + \tilde{\mu}_2) = (at - bn)g(t, n) + k.$$

Recall we are supposing that $g(t, n)$ is not the zero polynomial. In particular, as polynomials in t, we must have the factorisation

$$at - bn | f(\tilde{\lambda}_1 t + \tilde{\mu}_1, \tilde{\lambda}_2 t + \tilde{\mu}_2) - k$$

over $\overline{\mathbb{Q}}[t]$. Now, because we are assuming that the curve $f(x, y) = k$ doesn't contain a line definable over $\mathbb{Q}$, it follows that at least one of the variables $\tilde{\lambda}_1, \tilde{\mu}_1, \tilde{\lambda}_2, \tilde{\mu}_2 \in \overline{\mathbb{Q}} \backslash \mathbb{Q}$. But then, since $x_i = \tilde{\lambda}_i x_3 + \tilde{\mu}_i$ for $i \in \{1, 2\}$, it is clear that any line which arises in this way contains at most 1 integer point.

□

Our last technical estimate is the following lemma. We note that our assumption $(ax - by)g(x, y)$ is square-free means that, in particular, we have $g_{d-1}(1, a/b) \neq 0$.

Lemma 3.4.7. *Suppose $g \in \mathbb{Z}[x, y]$ is such that $g_{d-1}(1, a/b) \neq 0$. Then for any $l \neq 0$ we have*

$$\#\{x, y \in [1, B] \cap \mathbb{Z} : (ax - by)g(x, y) = l\} \ll_\epsilon B^{1/2+\epsilon}.$$

[2]For otherwise we would have $f(\gamma, t) = k$ identically in t, and then $f(x, y) = k$ would contain the rational line $(x - \gamma)$.

Proof. This is proved along the same lines of Lemma 3.4.1. We will be done by Proposition 3.2.2 provided that we can show this curve doesn't contain any lines defined over $\overline{\mathbb{Q}}$. As $l \neq 0$, any line contained in this variety must have a parametrisation of the form $(x, y) = (t, \lambda t + \mu)$. In this case we must have the following polynomial identity in $\overline{\mathbb{Q}}[t]$:

$$[(a - b\lambda)t - b\mu]g(t, \lambda t + \mu) = l.$$

Since $l \neq 0$, for this to be true clearly the first factor must be constant, i.e. $\lambda = a/b$. Now, by Taylor expansion, we have

$$g(t, \lambda t + \mu) = g_{d-1}(1, \lambda)t^{d-1} + \dots.$$

For the leading term to vanish we must have $g_{d-1}(1, \lambda) = g_{d-1}(1, a/b) = 0$. This is a contradiction. □

The following lemma, together with equation (3.4.9), completes the proof of Theorem 3.1.2, in the case $d \geq 5$.

Lemma 3.4.8. *We have*

$$\sum_{\substack{1 \leq n \leq B \\ \Gamma_n^{proj} \text{ smooth} \\ g(\cdot, n) \neq 0}} M_{\Gamma_n}^{lines}(B) \ll_\epsilon B^{3/2+\epsilon}$$

Proof. This follows by assembling the information gathered thus far. Consider again Proposition 3.4.6. It is easy to see that the contribution from lines in cases (1) or (2) is $O_\epsilon(B^{3/2+\epsilon})$ by Lemma 3.4.7 together with the fact $|\Lambda| = O(1)$, and the contribution from lines in case (3) is $O(B)$ by Lemma 3.4.5. □

We conclude that

$$M_{f,g}(B; k) \ll_\epsilon B^{1+\epsilon}(B^{1/2} + B^{2/\sqrt{d}+1/(d-1)-1/((d-2)\sqrt{d})}). \tag{3.4.10}$$

One can check the exponents appearing here are strictly less than $(2 - 1/(50d))$ whenever $d \geq 5$, and so the bound stated in Theorem 3.1.2 follows.

3.5 Proof of Theorem 3.1.2 in the case $d \in \{3, 4\}$.

We now proceed to prove Theorem 3.1.2 in the remaining cases when $d \in \{3, 4\}$. As discussed in Section 3.2, we will use the polynomial sieve developed by Browning in this regime. We state the main sieve proposition here. By slightly adjusting the set-up, we are able to make the implied constant absolute and transfer any dependencies

into our choice of $\mathcal{P}$, the set of sieving primes. This is a technical convenience which will prove useful to us, as for our applications to asymmetric additive energy of polynomials we wish to explicitly keep track of any dependencies on the constant term.

It is clear that the following result follows from the proof of [4, Theorem 1.1].

Proposition 3.5.1 (Browning)**.** *Let $\mathcal{A} \subset \mathbb{Z}^2$, and let $F \in \mathbb{Z}[x, X_1, X_2]$ be a polynomial of the form*

$$F(x; X_1, X_2) = c_d x^d + c_{d-1}(X_1, X_2)x^{d-1} + \ldots + c_0(X_1, X_2),$$

where c_d is a non-zero integer and $c_i \in \mathbb{Z}[X_1, X_2]$ for every $i \in \{0, \ldots, d-1\}$. Let $\mathcal{P}$ be a set of primes such that $(c_d, p) = 1$ for every $p \in \mathcal{P}$ and $\sqrt{X_1^2 + X_2^2} \leq \exp(\#\mathcal{P})$ whenever $(X_1, X_2) \in \mathcal{A}$. Then, for any integer $\alpha \geq 1$, we have

$$\#\{(X_1, X_2) \in \mathcal{A} : F(x; X_1, X_2) = 0 \text{ for some } x \in \mathbb{Z}\} \ll \frac{1}{\#\mathcal{P}^2} \sum_{p,q \in \mathcal{P}} \left| \sum_{i,j \in \{0,1,2\}} c_{i,j}(\alpha) S_{i,j}(p, q) \right|,$$

where

$$S_{i,j}(p, q) = \sum_{(X_1, X_2) \in \mathcal{A}} v_p(X_1, X_2)^i v_q(X_1, X_2)^j,$$

the $v_p(X_1, X_2)$ denote the "local counts" of solutions

$$v_p(X_1, X_2) = \#\{x \ (mod\ p) : F(x; X_1, X_2) \equiv 0 \ (mod\ p)\},$$

and the coefficients $c_{i,j}(\alpha)$ are given by

$$c_{i,j}(\alpha) = \begin{cases} (\alpha - d)^2 & \text{if } (i,j) = (0,0), \\ \alpha + (\alpha - 1)d - d^2 & \text{if } (i,j) = (1,0) \text{ or } (0,1), \\ (1+d)^2 & \text{if } (i,j) = (1,1), \\ -\alpha - d & \text{if } (i,j) = (2,0) \text{ or } (0,2), \\ -1 - d & \text{if } (i,j) = (2,1) \text{ or } (1,2), \\ 1 & \text{if } (i,j) = (2,2). \end{cases}$$

The implied constant is absolute.

The purpose of the α parameter will become clear later. We will choose it in such a way as to eliminate the "main term" contribution.

Before we begin, we first make an observation. If $|k| \gg B^{d+1}$ (say) then, by

size considerations, we must have $M_{f,g}(B;k) = 0$. Thus, continuing, we may assume that

$$0 < |k| \ll B^{d+1}. \tag{3.5.1}$$

The fact that we can restrict to the case when k is polynomially bounded in terms of B will be useful later on.

To apply the determinant method, we began by making a change of variables and proceeded to count points on the simpler 3-dimensional surface Γ_n. We will do a similar transformation now for the sieve method. Recall, we wish to count integer points on the affine hypersurface

$$f(x_1, x_2) = (ax_3 - bx_4)g(x_3, x_4) + k \subset \mathbb{A}^4_{\mathbb{Q}}. \tag{3.5.2}$$

Unlike the determinant method, the sieve method we will use makes crucial use of the factorisation properties of the above equation. Thus we make a different change of variables. In spite of this change, much of the preliminary work is the same. Let us write

$$\begin{aligned} X_1 &= x_1, \\ X_2 &= x_2, \\ X_3 &= ax_3 + bx_4, \\ h &= ax_3 - bx_4. \end{aligned} \tag{3.5.3}$$

We view h as fixed and consider counting integer points on the affine surface

$$(2ab)^{d-1} f(X_1, X_2) = (2ab)^{d-1} hg\left(\frac{X_3 + h}{2a}, \frac{X_3 - h}{2b}\right) + (2ab)^{d-1} k \subset \mathbb{A}^3_{\mathbb{Q}}. \tag{3.5.4}$$

Here we multiply through by suitable powers of $2, a$ and b to ensure that our polynomials have integer coefficients. Let us denote by $K_h(x, y, z, w)$ the projectivisation of this surface in $\mathbb{P}^3_{\mathbb{Q}}$. We can write

$$M_{f,g}(B;k) \leq \sum_{0 \leq |h| \ll B} \sum_{\substack{1 \leq X_1, X_2 \leq B \\ 1 \leq X_3 \ll B \\ K_h(X_1, X_2, X_3, 1) = 0}} 1. \tag{3.5.5}$$

Exactly as above, we first deal with the degenerate case when h is such that

$$hg\left(\frac{X_3 + h}{2a}, \frac{X_3 - h}{2b}\right) = 0 \tag{3.5.6}$$

identically (as a polynomial in X_3). There are $O(1)$ values of h for which this is the case. For these values of h we conclude the contribution to (3.5.5) is $O_\epsilon(B^{3/2+\epsilon})$, by Lemma 3.4.1. Our aim is to estimate the remaining terms using the polynomial sieve. The sieve method works most effectively when K_h is smooth. Generically this will be true, as the following lemma demonstrates.

Lemma 3.5.2. *The varieties $K_h \subset \mathbb{P}^3_{\mathbb{Q}}$ are smooth for all but at most $O(1)$ values of h.*

Proof. This is proved in the same way as Lemma 3.4.2 with minor differences. □

It will also be important to have control over various auxiliary curves which arise in the argument. In particular, we will need to have control over the the curves

$$(2ab)^{d-1}h\left[g\left(\frac{x+h}{2a},\frac{x-h}{2b}\right)-g\left(\frac{y+h}{2a},\frac{y-h}{2b}\right)\right]\Big/(x-y)\subset\mathbb{A}^2_{\mathbb{Q}}. \tag{3.5.7}$$

We let $P_h(x,y,w)$ denote the projectivisation of this curve in $\mathbb{P}^2_{\mathbb{Q}}$. For future convenience, we note that

$$\begin{aligned}P_h(x,y,w) = g_{d-1}(b,a)h(x^{d-2}+x^{d-3}y+\ldots+xy^{d-3}+y^{d-2})\\ +(\text{terms involving } w)\end{aligned} \tag{3.5.8}$$

and

$$P_h(x,x,1)=(2ab)^{d-1}hg'\left(\frac{x+h}{2a},\frac{x-h}{2b}\right). \tag{3.5.9}$$

Here, by the dash notation on the RHS we mean the derivative of the function $g(\frac{x+h}{2a},\frac{x-h}{2b})$ with respect to x. We would also like to restrict to the generic case when P_h is smooth. For this we require the following lemma.

Proposition 3.5.3. *The varieties $P_h \subset \mathbb{P}^2_{\mathbb{Q}}$ are smooth for all but at most $O(1)$ values of h.*

Proof. We split into two cases, depending on the degree d. In this proof $c_1(h), c_2(h)$ and $c_3(h)$ will denote polynomials in h whose coefficients will depend on those of g, a and b. We note that our assumption the variety $(ax-by)g_{d-1}(x,y)\subset\mathbb{P}^1_{\mathbb{Q}}$ does not contain any non-constant repeated components implies that, in particular, we have $g_{d-1}(b,a)\neq 0$.

The case $d=3$ is simple, as here we have

$$P_h(x,y,w)=g_{d-1}(b,a)h(x+y)+c_1(h)w$$

for some polynomial $c_1(h)$, and it clear that we do not have any singular points whenever $h \neq 0$.

Let us now examine the case $d = 4$. Here we are going to use the additional assumption (4) we make in the statement of Theorem 3.1.2. We have

$$P_h(x, y, w) = g_{d-1}(b, a)h(x^2 + xy + y^2) + c_2(h)(x + y)w + c_3(h)w^2$$

for some polynomials $c_2(h)$ and $c_3(h)$. From this it is clear that there are no singular points when $w = 0$ and $h \neq 0$.

Thus we consider possible singular points with $w = 1$. It is easy to check that for the partial derivatives to vanish we must have $x = y$, and so any singular point is necessarily of the form $[x : x : 1]$ where x satisfies, in particular, the system

$$P_h(x, x, 1) = P_h'(x, x, 1) = 0.$$

Here the latter quantity denotes the derivative of $P_h(x, x, 1)$ with respect to x.[3] Now, if this is the case, the discriminant $\mathrm{Disc}_x[P_h(x, x, 1)]$ must vanish identically. However this is a polynomial in h which generically will be non-zero. Arguing as above, we prove this is non-zero by extracting the leading coefficient and showing this doesn't vanish. From (3.5.9) we obtain

$$\begin{aligned}\frac{P_h(hx, hx, 1)}{h^{d-1}} &= \frac{(2ab)^{d-1}}{h^{d-2}} \sum_{i=0}^{d-1} g_i'\left(\frac{hx + h}{2a}, \frac{hx - h}{2b}\right) \\ &= (2ab)^{d-1} g_{d-1}'\left(\frac{x + 1}{2a}, \frac{x - 1}{2b}\right) + O(h^{-1})\end{aligned}$$

Hence, by a similar limiting argument to the proof of Lemma 3.4.2, we have

$$\lim_{h\to\infty} \frac{\mathrm{Disc}_x[P_h(x, x, 1)])}{h^{d(d-3)}} = \mathrm{Disc}_x\left[(2ab)^{d-1} g_{d-1}'\left(\frac{x + 1}{2a}, \frac{x - 1}{2b}\right)\right].$$

Note that

$$g_{d-1}'\left(\frac{x + 1}{2a}, \frac{x - 1}{2b}\right) = \left[\frac{1}{2a}\frac{\partial g_{d-1}}{\partial x} + \frac{1}{2b}\frac{\partial g_{d-1}}{\partial y}\right]\left(\frac{x + 1}{2a}, \frac{x - 1}{2b}\right).$$

Hence it is clear that this discriminant doesn't vanish from our assumption that the projective variety

$$\left[\frac{1}{2a}\frac{\partial g_{d-1}}{\partial x} + \frac{1}{2b}\frac{\partial g_{d-1}}{\partial y}\right]\left(\frac{x}{a}, \frac{y}{b}\right) \subset \mathbb{P}^2_{\mathbb{Q}}$$

is square-free. □

[3] Note $P_h'(t, t, 1) = \frac{P_h}{\partial x}(t, t, 1) + \frac{P_h}{\partial y}(t, t, 1)$.

We now deal with the contribution from those values of h for which either K_h or P_h is singular.

Lemma 3.5.4. *Suppose that h is constrained to lie in a set of size $O(1)$ and moreover h is such that*

$$hg\left(\frac{X_3+h}{2a}, \frac{X_3-h}{2b}\right)$$

doesn't vanish identically as a polynomial in X_3. Then the contribution from these values of h to (3.5.5) is at most $O_\epsilon(B^{3/2+\epsilon})$.

Proof. This follows in much the same way as the proof of Lemma 3.4.4. □

With this lemma, we can rewrite (3.5.5) as

$$M_{f,g}(B;k) \leq \sum_{\substack{0<|h|\ll B \\ K_h,P_h \text{ smooth}}} \sum_{\substack{1\leq X_1,X_2\leq B \\ 1\leq X_3\ll B \\ K_h(X_1,X_2,X_3,1)=0}} 1 + O_\epsilon(B^{3/2+\epsilon}). \tag{3.5.10}$$

For each fixed h we will apply the polynomial sieve to count the inner sum, by detecting solubility of the equation in the X_3 variable. In the notation of Proposition 3.5.1, we will take

$$\mathcal{A} := \{(X_1,X_2) \in ([1,B]\cap\mathbb{Z})^2 : (2ab)^{d-1}f(X_1,X_2) \equiv (2ab)^{d-1}k \pmod{|h|}\} \tag{3.5.11}$$

and

$$F(x;X_1,X_2) := K_h(X_1,X_2,x,1). \tag{3.5.12}$$

After unravelling the definition of K_h we find that

$$F(x;X_1,X_2) = hg_{d-1}(b,a)x^{d-1} + (\text{lower order terms in } x). \tag{3.5.13}$$

We are assuming that $hg_{d-1}(b,a) \neq 0$.[4] In particular, F is of the correct form to apply Proposition 3.5.1. We define

$$\mathcal{P} = \{p \leq Q : p \nmid 6abg_{d-1}(b,a)\text{cont}(f_d)\text{Disc}[f_d]\text{Disc}[K_h]\text{Disc}[P_h]h\} \tag{3.5.14}$$

for some large value of Q. By $\text{cont}(f_d)$ we mean the content of the polynomial f_d (i.e. the gcd of all the coefficients). Here, whenever F is a homogenous polynomial we denote by $\text{Disc}[F]$ its discriminant. This choice is important, as it will ensure our varieties remain smooth when viewed over $\overline{\mathbb{F}}_p$ (for any $p \in \mathcal{P}$).

[4]Recall that our assumption that the projective variety $\{(ax-by)g_{d-1}(x,y)\} \subset \mathbb{P}^1_{\mathbb{Q}}$ is square-free implies, in particular, that $g_{d-1}(b,a) \neq 0$.

We need to be careful here, as this set clearly depends on h and will also depend (in some complicated manner) on k. Now, it is a standard fact that the discriminant of a homogenous polynomial of degree N is a homogenous polynomial of degree $(2N-2)$ in the coefficients. This, together with the size bounds $|h| \ll B$ and $|k| \ll B^{d+1}$ (recall (3.5.1)) imply that

$$\mathrm{Disc}[K_h]\mathrm{Disc}[P_h]h \ll B^{5d^2}$$

uniformly in h and k (say). We will eventually take $Q = B^\delta$ for some small $\delta > 0$. This means, by the prime number theorem, we will have the asymptotic

$$\#\mathcal{P} \sim Q/\log Q \tag{3.5.15}$$

uniformly in h and k, whenever $B \gg 1$.

Thus, applying Proposition 3.5.1 with our choices above to each term in the sum (3.5.10) yields

$$M_{f,g}(B;k) \ll_\epsilon \sum_{\substack{0<|h|\ll B \\ K_h, P_h \text{ smooth}}} \frac{1}{(\#\mathcal{P})^2} \sum_{p,q\in\mathcal{P}} \left| \sum_{i,j\in\{0,1,2\}} c_{i,j}(\alpha) S_{i,j}(p,q) \right| + B^{3/2+\epsilon}, \tag{3.5.16}$$

where

$$S_{i,j}(p,q) = \sum_{(X_1,X_2)\in\mathcal{A}} v_p(X_1,X_2)^i v_q(X_1,X_2)^j, \tag{3.5.17}$$

$$v_p(X_1,X_2) = \#\{x \pmod p : K_h(X_1,X_2,x,1) \equiv 0 \pmod p\}, \tag{3.5.18}$$

and the constants $c_{i,j}(\alpha)$ are defined as in the statement of Proposition 3.5.1.

We evaluate the sums $S_{i,j}(p,q)$ following the method of Browning [4], by first restricting to congruence classes modulo $pq|h|$ and then completing exponential sums. We have

$$\begin{aligned} S_{i,j}(p,q) &= \sum_{r,s \pmod{pq|h|}} \sum_{\substack{(X_1,X_2)\in\mathcal{A} \\ X_1\equiv r \pmod{pq|h|} \\ X_2\equiv s \pmod{pq|h|}}} v_p(X_1,X_2)^i v_q(X_1,X_2)^j \\ &= \sum_{\substack{r,s \pmod{pq|h|} \\ (2ab)^{d-1}f(r,s)\equiv(2ab)^{d-1}k \pmod{|h|}}} v_p(r,s)^i v_q(r,s)^j \sum_{\substack{1\le X_1,X_2\le B \\ X_1\equiv r \pmod{pq|h|} \\ X_2\equiv s \pmod{pq|h|}}} 1. \end{aligned} \tag{3.5.19}$$

We can detect the congruence condition in the inner sum using additive characters, as follows:

$$\begin{aligned}\sum_{\substack{1\le X_1\le B\\ X_1\equiv r \pmod{pq|h|}}} 1 &= \frac{1}{pq|h|}\sum_{1\le X_1\le B}\sum_{m \pmod{pq|h|}} e\Big(-\frac{m(X_1-r)}{pq|h|}\Big)\\ &= \frac{1}{pq|h|}\sum_{-pq|h|/2<m\le pq|h|/2} e\Big(\frac{mr}{pq|h|}\Big)\sum_{1\le X_1\le B} e\Big(-\frac{mX_1}{pq|h|}\Big)\\ &:= \frac{1}{pq|h|}\sum_{-pq|h|/2<m\le pq|h|/2} \Gamma(B,m)e\Big(\frac{mr}{pq|h|}\Big), \end{aligned} \tag{3.5.20}$$

where we have defined

$$\Gamma(B,m) := \sum_{1\le l\le B} e\Big(\frac{-ml}{pq|h|}\Big). \tag{3.5.21}$$

We note the well-known bound here

$$\Gamma(B,m) \ll \min\left\{B, \frac{pq|h|}{|m|}\right\}, \tag{3.5.22}$$

which will be used later. A similar identity holds for the sum over X_2. Putting these facts together, and then swapping sums, we obtain the expression

$$S_{i,j}(p,q) = \frac{1}{(pqh)^2}\sum_{-pq|h|/2<m,n\le pq|h|/2} \Gamma(B,m)\Gamma(B,n)\Psi_{i,j}(m,n), \tag{3.5.23}$$

where

$$\Psi_{i,j}(m,n) := \sum_{\substack{r,s \pmod{pq|h|}\\ (2ab)^{d-1}f(r,s)\equiv(2ab)^{d-1}k \pmod{|h|}}} v_p(r,s)^i v_q(r,s)^j e\Big(\frac{mr+ns}{pq|h|}\Big). \tag{3.5.24}$$

By our choice of $\mathcal{P}$ we have $(pq,h)=1$. This allows us to deduce the following multiplicativity property for the exponential sums $\Psi_{i,j}$.

Lemma 3.5.5. *The following factorisations hold.*

1. *Suppose $p\neq q$ and let $p',q',\overline{pq},\overline{h}\in\mathbb{Z}$ be defined by $pq\overline{pq}+|h|\overline{h}=1$ and $pp'+qq'=1$. Then*

$$\Psi_{i,j}(m,n) = \Sigma_i(p;\overline{h}q'm,\overline{h}q'n)\Sigma_j(q;\overline{h}p'm,\overline{h}p'n)\Phi(|h|;\overline{pq}m,\overline{pq}n).$$

2. *Suppose $p=q$ and let $\overline{p},\overline{h}\in\mathbb{Z}$ be defined by $p\overline{p}+|h|\overline{h}=1$. Then*

$$\Psi_{i,j}(m,n) = \begin{cases} p^2\Sigma_{i+j}(p;\overline{h}m',\overline{h}n')\Phi(|h|;\overline{p}m',\overline{p}n') & \text{if } (m,n)=p(m',n'),\\ 0 & \text{otherwise.}\end{cases}$$

Here

$$\Sigma_t(p; M, N) = \sum_{x,y \in \mathbb{F}_p} v_p(x,y)^t e\left(\frac{Mx+Ny}{p}\right) \tag{3.5.25}$$

and

$$\Phi(h; M, N) = \sum_{\substack{x,y \ (mod\ h) \\ (2ab)^{d-1} f(x,y) \equiv (2ab)^{d-1} k \ (mod\ h)}} e\left(\frac{Mx+Ny}{h}\right). \tag{3.5.26}$$

Proof. This is [4, Lemma 3.4] with slight changes to notation. □

Recall $i, j \in \{0, 1, 2\}$. Thus, to examine the exponential sums $\Psi_{i,j}$ we may restrict our analysis to the exponential sums Σ_t for $0 \leq t \leq 4$ and Φ.

For the former, it is important that we have restricted to the case where our varieties are smooth; the desired bounds will then follow relatively straightforwardly from the work of Weil and Deligne. We will make use of Hooley's method of moments, which allows us to estimate an exponential sum over an algebraic variety by counting points on the variety over finite fields. The following result originates in [17] and appears in the form stated here as [4, Lemma 3.5].

Lemma 3.5.6 (Hooley's method of moments)**.** *Let $F, G_1, \ldots, G_k$ be polynomials over $\mathbb{Z}$ of degree at most d, and let*

$$S = \sum_{\substack{\mathbf{x} \in \mathbb{F}_p^n \\ G_1(\mathbf{x}) = \ldots = G_k(\mathbf{x}) = 0}} e\left(\frac{F(\mathbf{x})}{p}\right)$$

for any prime p. For each $j \geq 1$ and $\tau \in \mathbb{F}_{p^j}$ we define the sets

$$N_j(\tau) = \#\{\mathbf{x} \in \mathbb{F}_{p^j}^n : G_1(\mathbf{x}) = \ldots = G_k(\mathbf{x}) = 0 \text{ and } F(\mathbf{x}) = \tau\}.$$

Suppose there exists $N_j \in \mathbb{R}$ such that

$$\sum_{\tau \in \mathbb{F}_{p^j}} |N_j(\tau) - N_j|^2 \ll_{d,k,n} p^{\kappa j}$$

where $\kappa \in \mathbb{Z}$ is independent of j. Then $S \ll_{d,k,n} p^{\kappa/2}$.

Once we have reduced to this point-counting problem over finite fields, we may employ the work of Weil [28] to count points on curves, and the work of Deligne [9] to count points on higher-dimensional varieties. The following two results will be sufficient for our purposes.

Lemma 3.5.7 (Deligne)**.** *Let $W \subset \mathbb{P}^n_{\mathbb{F}_q}$ be a non-singular complete intersection of dimension 2 and degree d. Then*

$$\#\{\mathbf{x} \in \mathbb{F}_q^n : [\mathbf{x}] \in W\} = q^3 + O_{d,n}(q^2).$$

Lemma 3.5.8 (Weil)**.** *Let $V \subset \mathbb{A}^n_{\mathbb{F}_q}$ be an absolutely irreducible curve of degree d. Then*

$$\#\{\mathbf{x} \in \mathbb{F}_q^n : \mathbf{x} \in V\} = q + O_{d,n}(q^{1/2}).$$

Recall that a projective variety $W \subset \mathbb{P}^n_{\mathbb{F}_p}$ is a *complete intersection* if it is generated by exactly $\mathrm{codim}(W)$ elements.

We will estimate the exponential sums $\Phi(h; M, N)$ by using multiplicativity to reduce to studying the sums $\Phi(p^l; M, N)$ for $p^l || h$. We will then obtain square-root cancellation when $l = 1$ (the generic case), and obtain a (weaker) power saving bound for higher powers. This is the part of the argument where we will use the fact the curve $f(x, y) = k$ doesn't contain any lines definable over $\mathbb{Q}$.

In both cases, care must be taken to ensure that our results have no dependence on the constant term k. We recall our convention, adopted in Section 3.3, which says all implied constants are allowed to depend on f, g, a and b without specifying so, and this includes dependencies on the coefficients of f and g as well as on the degree d.

Finally, the following two sections will require us to perform arithmetic in $\overline{\mathbb{F}}_p$. To this end, we adopt the convention that any rational number a/b whose denominator is coprime to p may be viewed as an element of $\overline{\mathbb{F}}_p$, namely $\overline{a}\overline{b}^{-1}$, where $\overline{x}$ denotes the reduction map modulo p and $\overline{x}\overline{x}^{-1} \equiv 1 \pmod{p}$. In particular, the rational number a/b vanishes when viewed as an element of $\overline{\mathbb{F}}_p$ if and only if $p|a$.

3.6 Estimation of exponential sums (I)

Recall the definition of Σ_t given by (3.5.25). In this section we are going to estimate the exponential sums

$$\Sigma_t(p; M, N) = \sum_{x,y \in \mathbb{F}_p} v_p(x, y)^t e\left(\frac{Mx + Ny}{p}\right) \tag{3.6.1}$$

for $0 \leq t \leq 4$ and integers M, N. We argue in much the same way as Browning [4] did for the analogous sums he encountered when investigating the symmetric additive

energy of quartic polynomials, with a few changes. Our main result is the following (cf. [4, Lemma 4.3]).

Proposition 3.6.1. *Let $p \in \mathcal{P}$. For $0 \leq t \leq 4$ we have*

$$\Sigma_t(p; M, N) \ll p(p, M, N)$$

and for $0 \leq t \leq 2$ we have

$$\Sigma_t(p; 0, 0) = \max\{1, t\}p^2 + O(p).$$

We will prove this result in stages. The case $t = 0$ follows immediately from orthogonality of additive characters. Thus we turn our attention to the case $t = 1$, where

$$\Sigma_1(p; M, N) = \sum_{\substack{x,y,z \pmod p \\ K_h(x,y,z,1)=0}} e\left(\frac{Mx + Ny}{p}\right). \tag{3.6.2}$$

We begin by proving the following lemma.

Lemma 3.6.2. *For any integers N and M we have*

$$\mathrm{Disc}_x[f_d(Nx, 1 - Mx)] = N^D \mathrm{Disc}_x[f_d(x, 1)] \tag{3.6.3}$$

for some integer D depending on f_d, M and N.

Proof. The result is true if $N = 0$ as then both sides equal zero. Thus we may suppose that $N \neq 0$. We have

$$\mathrm{Disc}_x[f_d(Nx, 1 - Mx)] = N^D \mathrm{Disc}_x[f_d(x, 1 - Mx/N)]$$

where $D := l(l-1)$ and l is the degree of $f_d(x, 1 - Mx/N)$ as a polynomial in x. To prove the lemma, it suffices to show that the discriminant $\mathrm{Disc}_x(f_d(x, 1 - tx))$, which by definition is a polynomial in t, is in fact constant in t. To do this, we require two further properties of discriminant polynomials which we state here. Namely, for any polynomial F we have

$$\mathrm{Disc}_x[xF(x)] = F(0)^2 \mathrm{Disc}_x[F(x)]$$

and, if in addition F has degree d and $F(0) \neq 0$, we have

$$\mathrm{Disc}_x[F(x)] = \mathrm{Disc}_x[x^d F(1/x)].$$

We split into two cases.

1. Suppose $f_d(0,1) \neq 0$. In this case, provided t is such that $f_d(1,-t) \neq 0$, we have

$$\begin{aligned}\mathrm{Disc}_x[f_d(x,1-tx)] &= \mathrm{Disc}_x[x^d f_d(1,1/x-t)] \\ &= \mathrm{Disc}_x[f_d(1,x-t)] \\ &= \mathrm{Disc}_x[f_d(1,x)].\end{aligned}$$

   As both sides are polynomials in t, we conclude this identity in fact holds for all t. The result follows.

2. Suppose $f_d(0,1) = 0$. Then we must have $(\partial f_d/\partial x)(0,1) \neq 0$ as otherwise $f_d(x,y)$ would be divisible by x^2. Again supposing t is such that $f_d(1,-t) \neq 0$, we have

$$\begin{aligned}\mathrm{Disc}_x[f_d(x,1-tx)] &= \mathrm{Disc}_x[x^d f_d(1,1/x-t)] \\ &= \left[\lim_{x\to 0}\frac{f_d(x,1-xt)}{x}\right]^2 \mathrm{Disc}_x[x^{d-1} f_d(1,1/x-t)] \\ &= \left[\frac{\partial f_d}{\partial x}(0,1)\right]^2 \mathrm{Disc}_x[f_d(1,x)]\end{aligned}$$

   The result follows, as above.

□

We isolate the $t = 1$ case of Proposition 3.6.1 in the following lemma.

Lemma 3.6.3. *Let $p \in \mathcal{P}$. Then*

$$\Sigma_1(p;M,N) = \begin{cases} p^2 + O(p) & \text{if } p|(M,N), \\ O(p) & \text{otherwise.}\end{cases}$$

Proof. First we consider the case $p|(M,N)$. We may write

$$\Sigma_1(p;0,0) = \frac{1}{p-1}\#\{x,y,z,w \in \mathbb{F}_p : K_h(x,y,z,w) = 0 \text{ and } w \neq 0\}.$$

Our set-up ensures that $K_h(x,y,z,w)$ is a non-singular projective surface over $\mathbb{F}_p$. The hypotheses of Lemma 3.5.7 are satisfied, and so we obtain

$$\#\{x,y,z,w \in \mathbb{F}_p : K_h(x,y,z,w) = 0\} = p^3 + O(p^2).$$

We have $K_h(x,y,z,0) = (2ab)^{d-1} f_d(x,y)$. Assuming $p \in \mathcal{P}$, it follows that

$$\#\{x,y,z \in \mathbb{F}_p : K_h(x,y,z,0) = 0\} \ll p^2.$$

Putting these facts together yields

$$\Sigma_1(p;0,0) = p^2 + O(p).$$

Now let us suppose $p \nmid (M,N)$. We will use Lemma 3.5.6 to show that (generically) we have square-root cancellation. To this end, fix an integer $j \geq 1$ and $\tau \in \mathbb{F}_{p^j}$, and define

$$N_j(\tau) := \#\{x,y,z \in \mathbb{F}_{p^j} : K_h(x,y,z,1) = 0 \text{ and } Mx + Ny = \tau\}.$$

We may suppose WLOG that $p \nmid N$, with the case $p \nmid M$ being treated similarly. We may rewrite the above as

$$N_j(\tau) = \#\{x,z \in \mathbb{F}_{p^j} : K_h(x,(\tau - Mx)N^{-1},z,1) = 0\}.$$

We claim the following.

Claim. $K_h(x,(\tau - Mx)N^{-1},z,1) = 0$ defines an absolutely irreducible curve for all but at most $O(1)$ values of τ.

Proof (of claim). To examine whether the curve $K_h(x,(\tau - Mx)N^{-1},z,1) = 0$ is absolutely irreducible, we investigate the smoothness properties of its projectivisation over $\overline{\mathbb{F}}_p$. By Taylor expansion (see e.g. (3.4.7)), and using the fact $p \nmid N$, we may write

$$\begin{aligned} f(x,(\tau - Mx)N^{-1}) = &\frac{f_d(N,-M)}{N^d}x^d \\ &+ \left[\frac{f_{d-1}(N,-M)}{N^{d-1}} - \tau\frac{(\partial f_d/\partial y)(N,-M)}{N^d}\right]x^{d-1} + \dots. \end{aligned}$$

We also have

$$(2ab)^{d-1}hg\left(\frac{z+h}{2a}, \frac{z-h}{2b}\right) = g_{d-1}(b,a)hz^{d-1} + \dots.$$

There are two cases to consider.

1. Suppose $f_d(N,-M) = 0$ in $\overline{\mathbb{F}}_p$. In this case, since f_d is smooth and $N \neq 0$ we have $(\partial f_d/\partial y)(N,-M) \neq 0$. We exclude the value $\tau = Nf_{d-1}(N,-M)/(\partial f_d/\partial y)(N,-M)$, as we may, and then we see the projectivisation of this curve can be written as

$$\left[\frac{f_{d-1}(N,-M)}{N^{d-1}} - \tau\frac{(\partial f_d/\partial y)(N,-M)}{N^d}\right]x^{d-1} = g_{d-1}(b,a)hz^{d-1} + (\text{terms involving } w).$$

It is then clear, by considering vanishing of partial derivatives, that there cannot be any singular points with $w = 0$. This leaves us to investigate singular points of the form $[r : s : 1]$. By considering the z-derivative, we see that s is constrained to at most $O(1)$ values. For each such value, there will be a solution in r if and only if the discriminant

$$\mathrm{Disc}_x\left[f(x,(\tau - Mx)N^{-1}) - (2ab)^{d-1}hg\left(\frac{s+h}{2a}, \frac{s-h}{2b}\right) - (2ab)^{d-1}k\right] \quad (3.6.4)$$

vanishes. This will be a polynomial in τ which generically is non-zero, and so will only vanish for $O(1)$ values of τ. As previously, we will prove this by extracting the leading coefficient and showing this is non-zero. We have

$$\frac{f(\tau x,(\tau - M\tau x)N^{-1}}{\tau^d} = f_d(x,(1 - Mx)N^{-1}) + O(\tau^{-1}).$$

By similar arguments to the proof of Lemma 3.4.2, it follows that the leading coefficient of the dscriminant (3.6.4), as a polynomial in τ, is

$$\mathrm{Disc}_x[f_d(x,(1 - Mx)N^{-1}].$$

By Lemma 3.6.2 and our assumptions on p, this doesn't vanish.

2. Suppose $f_d(N, -M) \neq 0$ in $\overline{\mathbb{F}}_p$. Then the projectivised curve can be written as

$$\frac{f_d(N,-M)}{N^d}x^d = g_{d-1}(b,a)hz^{d-1}w + (\text{terms involving } w).$$

In exactly the same way as above, we conclude that there are no singular points with $w = 0$ and for any singular point of the form $[r : s : 1]$, s is constrained to at most $O(1)$ values and for each such value there exists an r if and only if the discriminant defined by (3.6.4) vanishes. This can only occur for at most $O(1)$ values of τ.

This finishes the proof of the claim. □

Now, for the $O(1)$ values of τ for which the curve $K_h(x,(\tau - Mx)N^{-1}, z, 1) = 0$ is not absolutely irreducible, we will apply the trivial bound $N_j(\tau) \ll p^j$. In the complementary case, by Lemma 3.5.8, we obtain

$$N_j(\tau) = p^j + O(p^{j/2})$$

We may therefore take $N_j = p^j$ and $\kappa = 2$ in the statement of Lemma 3.5.6, and the result follows. □

For the case $t = 2$, we must examine the exponential sum

$$\Sigma_2(p; M, N) = \sum_{\substack{x,y,z_1,z_2 \pmod p \\ K_h(x,y,z_1,1)=0 \\ K_h(x,y,z_2,1)=0}} e\left(\frac{Mx+Ny}{p}\right). \tag{3.6.5}$$

Recalling the definition of P_h in (3.5.7), we see that

$$K_h(x, y, z_1, 1) = K_h(x, y, z_2, 1) \iff (z_1 - z_2)P_h(z_1, z_2, 1) = 0. \tag{3.6.6}$$

Thus we may equivalently write

$$\Sigma_2(p; M, N) = \sum_{\substack{x,y,z_1,z_2 \pmod p \\ K_h(x,y,z_1,1)=0 \\ (z_1-z_2)P_h(z_1,z_2,1)=0}} e\left(\frac{Mx+Ny}{p}\right). \tag{3.6.7}$$

We isolate the $t = 2$ case of Proposition 3.6.1 in the following lemma.

Lemma 3.6.4. *Let $p \in \mathcal{P}$. Then*

$$\Sigma_2(p; M, N) = \begin{cases} 2p^2 + O(p) & \text{if } p|(M, N), \\ O(p) & \text{otherwise.} \end{cases}$$

Proof. Separating out the contribution from $z_1 = z_2$, and recalling the definition of Σ_1 (see (3.6.2) above), we may write

$$\Sigma_2(p; M, N) = \Sigma_1(p; M, N) + \sum_{\substack{x,y,z_1,z_2 \pmod p \\ z_1 \neq z_2 \\ K_h(x,y,z_1,1)=0 \\ P_h(z_1,z_2,1)=0}} e\left(\frac{Mx+Ny}{p}\right). \tag{3.6.8}$$

In this last sum we may add back in the terms with $z_1 = z_2$, as these contribute

$$\leq \sum_{\substack{z \pmod p \\ P_h(z,z,1)=0}} \sum_{\substack{x,y \pmod p \\ K_h(x,y,z,1)=0}} 1 \ll p \sum_{\substack{z \pmod p \\ P_h(z,z,1)=0}} 1 \ll p. \tag{3.6.9}$$

Overall, we obtain

$$\Sigma_2 = \Sigma_1 + \sum_{\substack{x,y,z_1,z_2 \pmod p \\ K_h(x,y,z_1,1)=0 \\ P_h(z_1,z_2,1)=0}} e\left(\frac{Mx+Ny}{p}\right) + O(p).$$

Let us call this inner sum $T(p; M, N)$. The following claim is important.

Claim. For any $p \in \mathcal{P}$ the variety

$$\{K_h(x, y, z_1, w) = P_h(z_1, z_2, w) = 0\} \subset \mathbb{P}^4_{\overline{\mathbb{F}}_p} \tag{3.6.10}$$

is smooth.

Proof (of claim). Any singular point by definition must solve the system

$$K_h = P_h = 0,\ \lambda \nabla K_h = \mu \nabla P_h$$

for some $(\lambda, \mu) \neq (0,0)$. By the work above we know that both K_h and P_h are non-singular over $\mathbb{Q}$. It follows that we must have $\lambda\mu \neq 0$. Now, the gradient identity implies the following equations must be solved:

$$\begin{aligned}
\frac{\partial K_h}{\partial x} &= 0, \\
\frac{\partial K_h}{\partial y} &= 0, \\
\lambda \frac{\partial K_h}{\partial z_1} &= \mu \frac{\partial P_h}{\partial z_1}, \\
\frac{\partial P_h}{\partial z_2} &= 0, \\
\lambda \frac{\partial K_h}{\partial w} &= \mu \frac{\partial P_h}{\partial w}.
\end{aligned}$$

We first rule out the possibility of any singular points with $w = 0$. If $[r : s : t : u : 0]$ is a singular point, then the first two equations imply that

$$\frac{\partial f_d}{\partial x}(r,s) = \frac{\partial f_d}{\partial y}(r,s) = 0.$$

By Euler's identity we conclude that $f_d(r,s) = 0$. As we are assuming f_d is smooth over $\mathbb{F}_p$, we must therefore have $r = s = 0$. Now $\partial K_h/\partial z_1$ vanishes when $w = 0$. Recalling the definition of P_h (see (3.5.9)), we have

$$P_h(x,y,w) = g_{d-1}(b,a)h(x^{d-2} + x^{d-3}y + \ldots + xy^{d-3} + y^{d-2}) + \ldots.$$

If $d = 3$ then the third equation (say) cannot be satisfied, and so there are no singular points in this case. Thus we may suppose that $d = 4$. In this case the third and fourth equation imply that

$$\begin{aligned}
2t + u &= 0 \\
t + 2u &= 0,
\end{aligned}$$

whence we must have $t = u = 0$. This is a contradiction, and so there cannot be any singular points with $w = 0$. We now consider singular points of the form $[r : s : t : u : 1]$. The fourth equation implies that $(\partial P_h/\partial z_2)(t,u) = 0$. Likewise, on replacing $K(x,y,z_1,w)$ by $K(x,y,z_2,w)$ and using the symmetry of $P_h(z_1,z_2,w)$ in the first two variables, we see that $(\partial P_h/\partial z_1)(r,s) = 0$ also. Since we are assuming $P_h(r,s,1) = 0$, by Euler's identity we see that $(\partial P_h/\partial w)(r,s) = 0$. But now we have produced a singular point on the curve P_h, a contradiction. $\square$

With this claim proven, we move on to estimating the exponential sum $T(p; M, N)$ defined above. We begin by considering the case $p|(M, N)$. By definition,

$$T(p; 0, 0) = \#\{x, y, z_1, z_2 \in \mathbb{F}_p : K_h(x, y, z_1, 1) = P_h(z_1, z_2, 1) = 0\},$$

which we write as

$$T(p; 0, 0) = \frac{1}{p-1}\#\{x, y, z_1, z_2, w \in \mathbb{F}_p : K_h(x, y, z_1, w) = P_h(z_1, z_2, w) = 0 \text{ and } w \neq 0\}.$$

This set defines a non-singular, complete intersection, projective variety of dimension 2. Thus, we may apply Lemma 3.5.7 to conclude that

$$\#\{x, y, z_1, z_2, w \in \mathbb{F}_p : K_h(x, y, z_1, w) = P_h(z_1, z_2, w) = 0\} = p^3 + O(p^2).$$

The contribution from points with $w = 0$ is

$$\sum_{\substack{z_1, z_2 \in \mathbb{F}_p \\ P_h(z_1, z_2, 0) = 0}} \sum_{\substack{x, y \in \mathbb{F}_p \\ K_h(x, y, z_1, 0) = 0}} 1 \ll p \sum_{\substack{z_1, z_2 \in \mathbb{F}_p \\ P_h(z_1, z_2, 0) = 0}} 1 \ll p^2.$$

It follows that

$$T(p; 0, 0) = p^2 + O(p).$$

Now let us suppose $p \nmid (M, N)$. We will use Lemma 3.5.6 to show that (generically) we have square-root cancellation. Fix $j \geq 1$ and $\tau \in \mathbb{F}_{p^j}$. Then we must count

$$N_j(\tau) := \#\{x, y, z_1, z_2 \in \mathbb{F}_{p^j} : K_h(x, y, z_1, 1) = P_h(z_1, z_2, 1) = 0 \text{ and } Mx + Ny = \tau\}.$$

We may suppose WLOG that $p \nmid N$. Then we may write this as

$$N_j(\tau) = \#\{x, z_1, z_2 \in \mathbb{F}_{p^j} : K_h(x, (\tau - Mx)N^{-1}, z_1, 1) = P_h(z_1, z_2, 1) = 0\}.$$

We claim the following.

Claim. $K_h(x, (\tau - Mx)N^{-1}, z_1, 1) = P_h(z_1, z_2, 1) = 0$ defines an absolutely irreducible curve for all but at most $O(1)$ values of τ.

Proof (of claim). This proceeds much the same way as the analogous claim contained in Lemma 3.6.3. We examine the absolute irreducibility of this curve by investigating the smoothness properties of its projectivisation over $\overline{\mathbb{F}}_p$. There are two cases to consider.

1. If $f_d(N,-M) = 0$ in $\overline{\mathbb{F}}_p$, then we exclude the value $\tau = Nf_{d-1}(N,-M)/(\partial f_d/\partial y)(N,-M)$, as we may, and consider the equations

$$\left[\frac{f_{d-1}(N,-M)}{N^{d-1}} - \tau\frac{(\partial f_d/\partial y)(N,-M)}{N^d}\right]x^{d-1} = g_{d-1}(b,a)hz_1^{d-1} + (\text{terms involving } w)$$

and

$$P_h(z_1,z_2,w) = 0.$$

Call the first equation $\psi(x,z_1,w) = 0$. We must examine the system

$$\psi = P_h = 0 \text{ and } \lambda\nabla\psi = \mu\nabla P_h$$

for some $(\lambda,\mu) \neq (0,0)$. Clearly $\lambda \neq 0$ as P_h is smooth. Let us suppose that $\mu = 0$. We consider possible singular points of the form $[r:s:t:0]$. The equations $(\partial\psi/\partial x)(r,s) = (\partial\psi/\partial z_1)(r,s) = 0$ yield $r = s = 0$, and then the equation $P_h(0,t,0) = 0$ yields $t = 0$, a contradiction. Thus we may look for singular points of the form $[r:s:t:1]$. The equation $\partial\psi/\partial x = 0$ becomes $f'(x,(\tau - Mx)N^{-1}) = 0$ and, as above, the equation $\partial\psi/\partial z_1 = 0$ constrains s to at most $O(1)$ values. In this case, there exists a valid r if and only if the discriminant

$$\mathrm{Disc}_x\left[f(x,(\tau-Mx)N^{-1}) - (2ab)^{d-1}hg\left(\frac{s+h}{2a},\frac{s-h}{2b}\right) - (2ab)^{d-1}k\right]$$

vanishes. This is the same discriminant as defined in the proof of Lemma 3.6.3 (see (3.6.4)), and we showed there that this vanishes for at most $O(1)$ values of τ. Hence the claim holds in this case.

Thus we may suppose that $\lambda\mu \neq 0$. Our equations become

$$\begin{aligned}\frac{\partial\psi}{\partial x} &= 0,\\ \lambda\frac{\partial\psi}{\partial z_1} &= \mu\frac{\partial P_h}{\partial z_1},\\ \frac{\partial P_h}{\partial z_2} &= 0,\\ \lambda\frac{\partial\psi}{\partial w} &= \mu\frac{\partial P_h}{\partial w}.\end{aligned}$$

On replacing $\psi(x,z_1,w)$ with $\psi(x,z_2,w)$ and using the symmetry of $P_h(z_1,z_2,w)$ in the first two arguments, we may adjoin to this system the equation $\partial P_h/\partial z_1 =$

0. Now, if $[r : s : t : 1]$ is a singular point then the equations $(\partial P_h/\partial z_1)(r,s) = (\partial P_h/\partial z_2)(r,s) = 0$ together with Euler's identity and the equation $P_h(s,t,1) = 0$ yield $(\partial P_h/\partial w)(r,s) = 0$. This is a contradiction as P_h is smooth. Thus we may restrict ourselves to looking at singular points of the form $[r : s : t : 0]$. But now our first equation implies that $r = 0$, and similar to the proof of the claim above, the equations $(\partial P_h/\partial z_1)(r,s) = (\partial P_h/\partial z_2)(r,s) = 0$ either cannot be satisfied in the case $d = 3$, or imply that $s = t = 0$ in the case $d = 4$. In both cases we arrive at a contradiction.

2. If $f_d(N,-M) \neq 0$ in $\overline{\mathbb{F}}_p$, then we must instead consider the equations

$$\frac{f_d(N,-M)}{N^d}x^d = g_{d-1}(b,a)hz^{d-1}w + (\text{terms involving } w).$$

and

$$P_h(z_1,z_2,w) = 0.$$

One can proceed exactly as above and conclude there are at most $O(1)$ values of τ for which this system is singular.

This completes the proof of the claim. □

Now, for the $O(1)$ values of τ for which the curve $K_h(x,(\tau - Mx)N^{-1},z,1) = P_h(z_1,z_2,1) = 0$ is not absolutely irreducible, we will apply the trivial bound $N_j(\tau) \ll p^j$. In the complementary case, by Lemma 3.5.8, we obtain

$$N_j(\tau) = p^j + O(p^{j/2})$$

Thus we may take $N_j = p^j$ and $\kappa = 2$ in the statement of Lemma 3.5.6, and the result follows. □

We are left to proof Proposition 3.6.1 in the cases when $t \in \{3,4\}$. In this regime we only require an upper bound for $\Sigma_t(p;M,N)$ whenever $p \in \mathcal{P}$. To do this we follow the argument of Browning [4]. By definition, we have

$$\Sigma_t(p;M,N) = \sum_{\substack{x,y,z_1,\dots,z_t \pmod p \\ K_h(x,y,z_1,1)=0 \\ (z_i-z_j)P_h(z_i,z_j,1)=0 \text{ for } i\neq j}} e\left(\frac{Mx+Ny}{p}\right). \tag{3.6.11}$$

Let $\sigma(\mathbf{z})$ denote the number of distinct elements in the set $\{z_1,\dots,z_t\}$, so that $1 \leq \sigma(\mathbf{z}) \leq t$. We may split our sum according to the value of $\sigma(\mathbf{z})$. The contribution from

those $z_1, \dots, z_t$ for which $\sigma(\mathbf{z}) = 1$ is Σ_1, and this event arises in precisely one way. The contribution from those $z_1, \dots, z_t$ with $\sigma(\mathbf{z}) = 2$ is $\Sigma_2 - \Sigma_1$ by (3.6.8) and this event arises in c_t ways, for some appropriate constant c_t depending only on t. Let us now consider the contribution from those $\mathbf{z}$ with $\sigma(\mathbf{z}) = 3$. We claim the following. From the definition of P_h it is easy to see the following:

1. If $d = 3$ we have
$$P_h(x, y, 1) = P_h(x, z, 1) \iff y = z.$$
2. If $d = 4$ we have
$$P_h(x, y, 1) = P_h(x, z, 1) \iff y = z \text{ or } x + y + z = g_{d-1}(b, a)^{-1} h^{-1} c(h)$$
for some polynomial $c(h)$ whose coefficients depend on g, a and b.

With this, it is clear there is no contribution from the case $\sigma(\mathbf{x}) \geq 3$, whenever $d = 3$. Hence, we obtain
$$\Sigma_t(p; M, N) = (1 - c_t)\Sigma_1 + c_t\Sigma_2 \tag{3.6.12}$$
whenever $t \in \{3, 4\}$ and $d = 3$, and Proposition 3.6.1 follows. Thus we may suppose that $d = 4$. In this case it is clear that there is no contribution from $\sigma(\mathbf{x}) \geq 4$. This just leaves us to examine the case $\sigma(\mathbf{x}) = 3$. This event will arise in d_t ways, for some appropriate constant d_t depending only on t. We must examine the exponential sum
$$\sum_{\substack{x,y,z_1,z_2 \pmod p \\ (z_1-z_2)(2z_1+z_2-c(h))(z_1+2z_2-c(h))\neq 0 \\ K_h(x,y,z_1,1)=0 \\ P_h(z_1,z_2,1)=0}} e\left(\frac{Mx + Ny}{p}\right). \tag{3.6.13}$$

As $p \in \mathcal{P}$ and so, in particular, $p \nmid 6hg_{d-1}(b, a))$, the polynomials $P_h(z, z, 1), P_h(z, c(h) - 2z, 1)$ and $P_h(z, 2^{-1}(c(h) - z), 1)$ are non-zero quadratic polynomials in z. It follows that the terms omitted contribute $O(p)$ altogether. In other words, this equals
$$\sum_{\substack{x,y,z_1,z_2 \pmod p \\ K_h(x,y,z_1,1)=0 \\ P_h(z_1,z_2,1)=0}} e\left(\frac{Mx + Ny}{p}\right) + O(p). \tag{3.6.14}$$

This exponential sum is precisely $\Sigma_2 - \Sigma_1 + O(p)$ by (3.6.8) and (3.6.9). Thus, we obtain
$$\Sigma_t(p; M, N) = (1 - c_t - d_t)\Sigma_1(p; M, N) + (c_t + d_t)\Sigma_2(p; M, N) + O(p) \tag{3.6.15}$$
whenever $t \in \{3, 4\}$ and $d = 4$. This completes the proof of Proposition 3.6.1.

3.7 Estimation of exponential sums (II)

Recall the definition of Φ given by (3.5.26). In this section we will estimate the exponential sums

$$\Phi(h; M, N) = \sum_{\substack{x,y \pmod h \\ (2ab)^{d-1}f(x,y) \equiv (2ab)^{d-1}k \pmod h}} e\left(\frac{Mx+Ny}{h}\right) \tag{3.7.1}$$

where h is a fixed, positive integer and M and N are integers. We first note the following multiplicativity property of these sums: if $(j,l)=1$ and $j\overline{j}+l\overline{l}=1$ is it not difficult to show that

$$\Phi(jl; M, N) = \Phi(j; \overline{l}M, \overline{l}N)\Phi(l; \overline{j}M, \overline{j}N). \tag{3.7.2}$$

Thus is suffices to study $\Phi(p^l; M, N)$ for some prime p and integer $l \geq 1$. To tackle these exponential sums we will obtain square-root cancellation in the generic case for $l = 1$, and use elementary bounds for higher powers.

We now consider estimating $\Phi(p; M, N)$. This exponential sum will be sensitive to whether or not the curve $\{f(x_1, x_2) = k\} \subset \mathbb{A}^2_{\mathbb{F}_p}$ contains a line. In this case, if this line can be parametrised by $Mx + Ny = \tau$, for some constant $\tau \in \mathbb{F}_p$, we will get zero cancellation and hence the sum will be large. Because we are assuming the curve $f(x, y) = k$ contains no line definable over $\mathbb{Q}$, this should be a rare event. Our aim is to define a non-zero integer $\Delta_f(M, N, k)$ such that whenever this occurs, we must have that $p|\Delta_f$. This, together with size bounds on Δ_f, will be enough to control the cases where this exponential sum is large. This is the content of the following lemma.

Lemma 3.7.1. *Let f, k be as in the statement of Theorem 3.1.2. Fix integers $(M, N) \in \mathbb{Z}^2$, not both zero. Fix a prime p such that $p \nmid (M, N)$ and p is sufficiently large in terms of d. Let $\tau \in \overline{\mathbb{F}}_p$. Then there exists a non-zero integer $\Delta_f(M, N, k)$ such that whenever the curve $\{f(x, y) = k\} \subset \mathbb{A}^2_{\overline{\mathbb{F}}_p}$ contains the line $Mx + Ny = \tau$, we must have $p|\Delta_f(M, N, k)$. Moreover, $\Delta_f(M, N, k)$ satisfies the size bound*

$$|\Delta_f(M, N, k)| \ll_{f,d} |k| \max\{|M|, |N|\}^{d^2}. \tag{3.7.3}$$

Proof. We may suppose WLOG that $N \neq 0$. (If $M \neq 0$ then an identical case-analysis argument holds with minor adjustments.) With notation as above, let us suppose that

the curve $f(x,y) = k$ contains the line $Mx + Ny = \tau$ over $\overline{\mathbb{F}}_p$. In other words, we have the polynomial identity

$$f(x, (\tau - Mx)N^{-1}) = 0 \tag{3.7.4}$$

in $\overline{\mathbb{F}}_p[x]$. By Taylor expansion (see e.g. (3.4.7)), and using the fact $p \nmid N$, we see our assumption is that the identity

$$\frac{f_d(N,-M)}{N^d}x^d + \left[\frac{f_{d-1}(N,-M)}{N^{d-1}} - \tau\frac{(\partial f_d/\partial y)(N,-M)}{N^d}\right]x^{d-1} + \ldots = k \tag{3.7.5}$$

holds in $\overline{\mathbb{F}}_p[x]$. The proof now proceeds by careful case-analysis.

If $f_d(N,-M) \neq 0$ in $\mathbb{Q}$, then for the leading term to vanish we must have $p|f_d(N,-M)$. Thus in this case we define $\Delta_f(M,N,k) := f_d(N,-M)$ and the size bound is easily satisfied.

Thus, proceeding, we may suppose that $f_d(N,-M) = 0$ in $\mathbb{Q}$. In this case, by Euler's identity, and the fact f_d is assumed to be smooth and $N \neq 0$, we must have $(\partial f_d/\partial y)(N,-M) \neq 0$ in $\mathbb{Q}$.

If $p|(\partial f_d/\partial y)(N,-M)$ then we set $\Delta_f(M,N,k) := (\partial f_d/\partial y)(N,-M)$ and we are done; again the size bound is immediate.

Now let us suppose that $p \nmid (\partial f_d/\partial y)(N,-M)$. The vanishing of the coefficient of x^{d-1} implies that

$$\tau = \frac{N f_{d-1}(N,-M)}{(\partial f_d/\partial y)(N,-M)} \text{ in } \overline{\mathbb{F}}_p. \tag{3.7.6}$$

Substituting (3.7.6) back into (3.7.5), we obtain

$$\sum_{j=0}^{d} E_j(M,N)x^j = k \text{ in } \overline{\mathbb{F}}_p[x], \tag{3.7.7}$$

where, for each $j \in \{0,\ldots,d\}$, we have defined the rational numbers

$$\begin{aligned} E_j(M,N) &:= \frac{1}{N^j}\sum_{i=j}^{d}\frac{(-1)^{i-j}}{(i-j)!}\left(\frac{f_{d-1}(N,-M)}{(\partial f_d/\partial y)(N,-M)}\right)^{i-j}\frac{\partial^{i-j}f_i}{\partial y^{i-j}}(N,-M) \\ &= \frac{\sum_{i=j}^{d}\frac{(d-j)!}{(i-j)!}f_{d-1}(N,-M)^{i-j}(\partial f_d/\partial y)(N,-M)^{d-i}(\partial^{i-j}f_i/\partial y^{i-j})(N,-M)}{N^j(\partial f_d/\partial y)(N,-M)^{d-j}(d-j)!} \\ &:= \frac{A_j(M,N)}{B_j(M,N)}. \end{aligned} \tag{3.7.8}$$

Note that $A_j(M,N)$ and $B_j(M,N)$ are both integers, $B_j(M,N)$ is non-zero and our assumptions imply that $p \nmid B_j(M,N)$ (for every j).

Suppose that $E_j(M,N) \neq 0$ in $\mathbb{Q}$ for some $j \in \{1,\dots,d-1\}$. Let J be the maximal such integer. Then, in particular, we must have that p divides $A_J(M,N)$ and in this case we set $\Delta_f(M,N,k) := A_J(M,N)$. Note

$$|\Delta_f(M,N,k)| \ll \max_{J\leq i\leq d}\{|M|,|N|\}^{(d-1)(i-j)+(d-2)(d-i)+j} \ll \max\{|M|,|N|\}^{d^2},$$

and so the size bound is satisfied.

Otherwise, we arrive at the identity

$$E_0(M,N) = k \text{ in } \overline{\mathbb{F}}_p.$$

If $E_0(M,N) = k$ in $\mathbb{Q}$, then, together with all of our assumptions thus far, we arrive at a bonafide identity over $\mathbb{Q}$:

$$\sum_{j=0}^{d} E_j(M,N)x^j = k \text{ in } \mathbb{Q}[x].$$

Translating everything back, this says that $f(x,y)+k$ contains the line

$$Mx + Ny = \frac{Nf_{d-1}(N,-M)}{(\partial f_d/\partial y)(N,-M)}.$$

This is a rational line, which is a contradiction.

Thus, we must have that $E_0(M,N) \neq k$ in $\mathbb{Q}$. In this case we must have p divides the numerator of $E_0(M,N)-k$, and so we define $\Delta_f(M,N,k) := A_0(M,N)-kB_0(M,N)$. As above, we have $|A_0(M,N)| \ll \max\{|M|,|N|\}^{d^2}$. Note that

$$|B_0(M,N)| \ll \max\{|M|,|N|\}^{d(d-1)} \ll \max\{|M|,|N|\}^{d^2}.$$

As

$$|\Delta_f(M,N,k)| \leq |A_0(M,N)| + |k||B_0(M,N)|,$$

the stated bound follows. □

With Lemma 3.7.1, we can prove the following.

Lemma 3.7.2. *For any integers M and N we have*

$$\Phi(p;M,N) \ll p^{1/2}(p,\Delta_f(M,N,k))^{1/2}. \tag{3.7.9}$$

Proof. We may suppose that p is sufficiently large in terms of f, a and b as otherwise both sides are $O(1)$. We note that

$$\#\{x, y \in \mathbb{F}_p : (2ab)^{d-1} f(x, y) \equiv (2ab)^{d-1} k \pmod{p}\} \ll p.$$

Thus, by bounding trivially, we may apply the bound $\Phi(p; M, N) \ll p$ whenever $M = N = 0, p|(M, N)$ or $p|\Delta_f(M, N, k)$. By inspecting the proof of Lemma 3.7.1, it is clear that $\Delta_f(0, 0, k) = 0$ and $(M, N)|\Delta_f(M, N, k)$. Thus (3.7.9) holds in these cases. Proceeding, we may suppose M and N are not both zero and $p \nmid \Delta_f(M, N, k)$.

In this regime, we will obtain square-root cancellation in $\Phi(p; M, N)$ using Lemma 3.5.6. For any $j \geq 1$ and $\tau \in \mathbb{F}_{p^j}$, we define

$$N_j(\tau) = \#\{x, y \in \mathbb{F}_{p^j} : (2ab)^{d-1} f(x, y) = (2ab)^{d-1} k \text{ and } Mx + Ny = \tau\}.$$

We may suppose WLOG that $p \nmid N$. We can write

$$N_j(\tau) = \#\{x \in \mathbb{F}_{p^j} : (2ab)^{d-1} f(x, (\tau - Mx)N^{-1}) = (2ab)^{d-1} k\}.$$

Since we are assuming $p \nmid \Delta_f(M, N, k)$, it follows from Lemma 3.7.1 that the curve $f(x, y) = k$ contains no lines over $\mathbb{F}_{p^j}$. Hence $f(x, (\tau - Mx)N^{-1}) - k$ is never the zero polynomial in $\mathbb{F}_{p^j}[x]$, and we can bound $N_j(\tau) \ll 1$. Thus we may take $N_j = 0$ and $\kappa = 1$ in the statement of Lemma 3.5.6, and the result follows. □

We now turn our attention to bounding $\Phi(p^l; M, N)$ when $l \geq 2$. To do this we will bound trivially and forego any cancellation in our exponential sum. In other words, we bound

$$\Phi(p^l; M, N) \leq \#\{x, y \in \mathbb{Z}/p^l\mathbb{Z} : (2ab)^{d-1} f(x, y) \equiv (2ab)^{d-1} k \pmod{p^l}\} \tag{3.7.10}$$

and aim to estimate the count on the RHS. To do this we need some understanding of the number of solutions to polynomial congruences over the finite rings $\mathbb{Z}/p^l\mathbb{Z}$.

To this end, let $Q \in \mathbb{Z}[x]$ be a polynomial of degree d with leading coefficient a_d. We will make the dependencies on implied constants explicit for the following estimates involving Q. We are interested in general bounds for the count

$$\#\{x \in \mathbb{Z}/p^l\mathbb{Z} : Q(x) \equiv 0 \pmod{p^l}\}. \tag{3.7.11}$$

As a first estimate, whenever $p \nmid \mathrm{cont}(Q)$, we have

$$\#\{x \in \mathbb{Z}/p^l\mathbb{Z} : Q(x) \equiv 0 \pmod{p^l}\} \ll_d p^{l-1}. \tag{3.7.12}$$

This is easily proven by induction; there are $O_d(1)$ roots when $l = 1$ and, when $l \geq 2$, any element of $\mathbb{Z}/p^{l-1}\mathbb{Z}$ has exactly p lifts to an element of $\mathbb{Z}/p^l\mathbb{Z}$.

By using p-adic arithmetic, we can improve on this bound for large l.

Lemma 3.7.3. *With notation as above, for any prime p and integer $l \geq 1$, we have*

$$\#\{x \in \mathbb{Z}/p^l\mathbb{Z} : Q(x) \equiv 0 \ (mod\ p^l)\} \ll_d p^{l-l/d+v_p(a_d)/d}, \tag{3.7.13}$$

where $v_p(a_d)$ denotes the p-adic valuation of the non-zero integer a_d.

Proof. We will prove this by using the fact any root must be "p-adically close" to one of the d (not necessarily distinct) roots of Q in an algebraic closure of $\mathbb{Q}_p$, the p-adic numbers. To this end, we define the following (standard) notation. We let $|\cdot|_p$ denote the usual norm in $\overline{\mathbb{Q}}_p$ and μ denote the Haar measure. For any $\beta \in \overline{\mathbb{Q}}_p$ and $m \in \mathbb{Z}$ we define

$$B(\beta, p^m) := \{y \in \overline{\mathbb{Q}}_p : |y - \beta|_p \leq p^m\},$$

i.e. the (closed) ball of radius p^m centered at β, so that $\mu(B(\beta, p^m)) = p^m$. The estimate (3.7.13) is true for $l = 1$ since in this case we can use the bound $O_d(1)$.

Proceeding, we fix an integer $l \geq 2$ and roots $\beta_1, \ldots, \beta_d$ of Q in an algebraic closure $\overline{\mathbb{Q}}_p$. In $\overline{\mathbb{Q}}_p[t]$ we have the factorisation

$$Q(t) = a_d \prod_{i=1}^{d} (t - \beta_i).$$

We can partition the set we are interested in as follows:

$$\bigcup_{i=1}^{d} \#\{x \in \mathbb{Z}/p^l\mathbb{Z} : Q(x) \equiv 0 \ (\text{mod } p^l) \text{ and } |x - \beta_i|_p \text{ minimal}\}.$$

Suppose we are looking at the set corresponding to the root β. For an element $x \in \mathbb{Z}/p^l\mathbb{Z}$ to be counted we must have

$$|a_d|_p |x - \beta|_p^d \leq |a_d|_p \prod_{i=1}^{d} |x - \beta_i|_p = |Q(x)|_p \leq p^{-l}.$$

Suppose $m = v_p(a_d)$ so that $|a_d|_p = p^{-m}$. The line above equivalently says that $x \in B(\beta, p^{-(l-m)/d})$. By reduction, we see that x must take the form $x = \alpha + \lambda p$ for some root $\alpha \in \mathbb{Z}/p\mathbb{Z}$ and $\lambda \in \mathbb{Z}/p^{l-1}\mathbb{Z}$. There are $O_d(1)$ choices for α. Suppose that

$\alpha + \lambda p \in \overline{B}(\beta, p^{-(l-m)/d})$ for $\lambda \in \Lambda \subset \mathbb{Z}/p^{l-1}\mathbb{Z}$. Our aim is therefore to bound $|\Lambda|$. We claim the following:

Claim: If $\lambda \neq \lambda' \in \mathbb{Z}/p^{l-1}\mathbb{Z}$ then the balls $B_\lambda := B(\alpha + \lambda p, p^{-l})$ are disjoint.

Proof (of claim). For any distinct elements $\lambda \neq \lambda' \in \mathbb{Z}/p^{l-1}\mathbb{Z}$ we have

$$|\lambda - \lambda'|_p \geq p^{-(l-2)}.$$

Now, if $x \in \overline{B}_\lambda \cap \overline{B}_{\lambda'}$ we have

$$\begin{aligned} p^{-(l-1)} &\leq |(\alpha + \lambda p) - (\alpha + \lambda' p)|_p \\ &= |(\alpha + \lambda p) - x - (\alpha + \lambda' p - x)|_p \\ &\leq \max\{|\alpha + \lambda p - x|_p, |\alpha + \lambda' p - x|_p\} \\ &\leq p^{-l}, \end{aligned}$$

a contradiction. Here we have used the fact $|\cdot|_p$ is non-Archimedean. □

With this claim proven we can complete the proof. Fix α. As $|\cdot|_p$ is non-Archimedean, whenever $\alpha + \lambda p \in B(\beta, p^{-(l-m)/d})$ we must actually have

$$B(\alpha + \lambda p, p^{-(l-m)/d}) = B(\beta, p^{-(l-m)/d}).$$

Hence we are assuming that

$$\bigcup_{\lambda \in \Lambda} B(\alpha + \lambda p, p^{-l}) \subseteq \bigcup_{\lambda \in \Lambda} B(\alpha + \lambda p, p^{-(l-m)/d}) = B(\beta, p^{-(l-m)/d}).$$

From the claim, these sets on the LHS are disjoint. Using the fact μ is a measure, it follows that

$$\mu\bigg(\bigcup_{\lambda \in \Lambda} B(\alpha + \lambda p^l, p^{-l})\bigg) = \sum_{\lambda \in \Lambda} \mu(B(\alpha + \lambda p^l, p^{-l})) = |\Lambda| p^{-l}.$$

On the other hand

$$\mu(B(\beta, p^{-(l-m)/d})) = \mu(B(\beta, p^{-\lceil (l-m)/d \rceil})) = p^{-\lceil (l-m)/d \rceil}.$$

Putting these facts together, and using monotonicity of μ, we obtain

$$|\Lambda| \leq p^{l - \lceil (l-m)/d \rceil} \leq p^{l - l/d + m/d}.$$

We are done as there are only $O_d(1)$ possibilities for α and β. □

These results can easily be extended to the case $p^m||\text{cont}(Q)$.

Corollary 3.7.4. *Suppose $p^m||\text{cont}(Q)$. Then*

$$\#\{x \in \mathbb{Z}/p^l\mathbb{Z} : Q(x) \equiv 0 \ (mod\ p^l)\} \ll_{d,a_d} \begin{cases} p^l & \text{if } l \leq m, \\ p^{\min\{l-1, l-l/d\}}) & \text{if } l > m. \end{cases} \tag{3.7.14}$$

Proof. The statement is clear when $l \leq m$ and so we suppose that $l > m$. Write $Q(x) = p^m R(x)$ where $\text{cont}(R) = 1$. Then we have

$$\#\{x \in \mathbb{Z}/p^l\mathbb{Z} : Q(x) \equiv 0 \ (\text{mod } p^l)\} = p^N \cdot \#\{y \in \mathbb{Z}/p^{l-m}\mathbb{Z} : R(y) \equiv 0 \ (\text{mod } p^{l-m})\}.$$

Hence, using (3.7.12) and (3.7.13), we can bound this by

$$\ll_d p^m \cdot p^{\min\{l-m-1, l-m-(l-m)/d+v_p(a_d p^{-m})/d\}} = p^{\min\{l-1, l-l/d+v_p(a_d)/d\}}.$$

The result follows upon noting the $p^{v_p(a_d)/d}$ factor can be absorbed into the constant term, which we allow to depend on a_d. □

The following estimate will also be convenient for us: for any $A, B \in \mathbb{Z}$ such that $A \neq 0$ and $p \nmid A$, one has

$$\#\{x \in \mathbb{Z}/p^l\mathbb{Z} : p^m | Ax + B\} \leq \begin{cases} p^{l-m} & \text{if } m \leq l, \\ 1 & \text{if } m > l. \end{cases} \tag{3.7.15}$$

To proceed we require the following lemma.

Lemma 3.7.5. *Let $f \in \mathbb{Z}[x, y]$ be such that the projective variety $\{f_d(x, y) = 0\} \subset \mathbb{P}^1_{\mathbb{Q}}$ has no non-constant repeated factors. Then the polynomial*

$$\text{Disc}_t((2ab)^{d-1} f(x, t) - (2ab)^{d-1} k)$$

is not identically zero, and the leading coefficient is independent of k.

Proof. We wish to show a particular resultant polynomial is not identically zero. We will follow the strategy adopted in Lemma 3.4.2: once again, we will extract the leading coefficient and show this is non-zero. Since

$$f(x, xt) = \sum_{i=0}^{d} f_i(x, xt) = \sum_{i=0}^{d} x^i f_i(1, t),$$

it follows that

$$\lim_{x \to \infty} \frac{(2ab)^{d-1} f(x, xt) - (2ab)^{d-1} k}{x^d} = (2ab)^{d-1} f_d(1, t).$$

By a similar argument to the proof of Lemma 3.4.2, it follows that our discriminant polynomial has the leading coefficient

$$\mathrm{Disc}_t((2ab)^{d-1}f_d(1,t)).$$

Now this discriminant is non-zero by our assumption on $f_d(x,y)$, and it is clearly independent of k. □

Let us write $f(x,y) = \sum_{i+j\leq d} c_{i,j}x^iy^j$, so that

$$f_d(x,y) = c_{d,0}x^d + c_{d-1,1}x^{d-1}y + \ldots + c_{1,d-1}xy^{d-1} + c_{0,d}y^d. \tag{3.7.16}$$

If both $c_{d,0} = c_{d-1,1} = 0$ then $f_d(x,y)$ will contain a a square factor. Thus with our assumptions at least one of $c_{d-1,1}$ or $c_{d,0}$ is non-zero. (Similarly for $c_{0,d}$ and $c_{1,d-1}$.) We will make use of this fact in what follows. Our main result is the following. We recall our convention that implied constants may depend on f, g, a and b without specifying so, and this includes dependencies on the coefficients of f and g as well as dependencies on the degree d.

Lemma 3.7.6. *Fix $l \geq 2$. We have*

$$\Phi(p^l;0,0) \ll \begin{cases} p^{2l-2} & \text{if } 2 \leq l \leq d, \\ p^{2l-l/d-1} & \text{if } l \geq d. \end{cases}$$

Proof. For this proof it will also be helpful to define the polynomial

$$F(x,y) := (2ab)^{d-1}f(x,y) - (2ab)^{d-1}k. \tag{3.7.17}$$

We may assume that p is sufficiently large in terms of f, a and b as otherwise the result holds trivially. In particular, in view of Lemma 3.7.5, in this regime we may assume the polynomial $\mathrm{disc}_t(F(x,t))$ has content coprime to p. By Hensel's lemma, if $x \in \mathbb{Z}/p^l\mathbb{Z}$ is such that $\mathrm{disc}_t(F(x,t)) \not\equiv 0 \pmod{p}$, then any of the $\leq p^l$ choices for x will lead to at most $O(1)$ solutions in y. Hence we have

$$\Phi(p^l;0,0) = \sum_{\substack{x,y\in\mathbb{Z}/p^l\mathbb{Z} \\ F(x,y)\equiv 0 \pmod{p^l} \\ \mathrm{disc}_t(F(x,t))\equiv 0 \pmod{p}}} 1 + O(p^l). \tag{3.7.18}$$

Let us take the sum over x on the outside. The last constraint restricts x to $O(1)$ values modulo p and hence $O(p^{l-1})$ values modulo p^l. We would like to use the estimates proved above to tackle the inner sum over y. To do this, we need some understanding of how p divides the content of $F(x,y)$ as a polynomial in y. We write

this as $\mathrm{cont}_y(F(x,y))$.

If $f_d(0,1) = c_{0,d} \neq 0$ we have

$$F(x,y) = (2ab)^{d-1}c_{0,d}y^d + (\text{lower order terms in } y). \tag{3.7.19}$$

In the regime under consideration, $p \nmid c_{0,d}$, and so we get an overall bound

$$\Phi(p^l;0,0) \ll p^l + p^{l-1+\min\{l-1,l-l/d\}} \tag{3.7.20}$$

by Corollary 3.7.4. This agrees with the result stated.

Now let us suppose that $f_d(0,1) = c_{0,d} = 0$. From the remarks above, we must therefore have $c_{1,d-1} \neq 0$. In particular, we are assuming $p \nmid c_{1,d-1}$. It follows that

$$F(x,y) = (2ab)^{d-1}(c_{1,d-1}x + c_{0,d-1})y^{d-1} + (\text{lower order terms in } y) \tag{3.7.21}$$

for some $c_{0,d-1} \in \mathbb{Z}$. We now split the sum in (3.7.18) according to the power p^m which divides $\mathrm{cont}_y(F(x,y))$. Write this sum as

$$\sum_m \sum_{\substack{x \in \mathbb{Z}/p^l\mathbb{Z} \\ \mathrm{disc}_t(F(x,t)) \equiv 0 \pmod p \\ p^m || \mathrm{cont}_y(F(x,y))}} \sum_{\substack{y \in \mathbb{Z}/p^l\mathbb{Z} \\ F(x,y) \equiv 0 \pmod{p^l}}} 1. \tag{3.7.22}$$

The term with $m = 0$ contributes $\ll_d p^{l-1+\min\{l-1,l-l/d\}}$ by Corollary 3.7.4. To tackle the remaining sums we will majorise by replacing the condition $p^m || \mathrm{cont}_y(F(x,y))$ with the simpler condition $p^m | (2ab)^{d-1}(c_{1,d-1}x + c_{0,d-1})$. The terms with $m \geq l+1$ contribute

$$\leq p^l \sum_{\substack{x \in \mathbb{Z}/p^l\mathbb{Z} \\ \mathrm{disc}_t(F(x,t)) \equiv 0 \pmod p \\ p^{l+1} | \mathrm{cont}_y(F(x,y))}} 1 \leq p^l \sum_{\substack{x \in \mathbb{Z}/p^l\mathbb{Z} \\ p^{l+1} | (2ab)^{d-1}(c_{1,d-1}x + c_{0,d-1})}} 1 \leq p^l \tag{3.7.23}$$

by (3.7.15). To finish we need to estimate the contribution to (3.7.22) from when $m \in \{1, \ldots, l\}$. To do this, we split into two cases.

1. Suppose that $l \leq d$. Fix $1 \leq m \leq l$. By Corollary 3.7.4 we may bound the sum over y by $O(p^{l-1})$. We therefore get a contribution

$$\ll p^{l-1} \sum_{m=1}^{l} \sum_{\substack{x \in \mathbb{Z}/p^l\mathbb{Z} \\ p^m | (2ab)^{d-1}(c_{1,d-1}x + c_{0,d-1})}} 1$$

Using (3.7.15) we may bound this by

$$\ll p^{l-1}\sum_{m=1}^{l} p^{l-m} \ll p^{2l-2}.$$

Putting everything together, in this case we get

$$\Phi(p^l;0,0) \ll p^{2l-2} + p^{l-1+\min\{l-1,l-l/d\}} + p^l \ll p^{2l-2}. \tag{3.7.24}$$

This agrees with the stated result.

2. Now suppose that $l > d$. In this case we split our sum at $m = l - d$.

   (a) Fix $1 \leq m \leq l-d$. We can bound the sum over y by $O(p^{l-l/d})$ using Corollary 3.7.4. These terms therefore contribute

   $$\ll p^{l-l/d}\sum_{m=1}^{l-d} \sum_{\substack{x\in\mathbb{Z}/p^l\mathbb{Z} \\ p^m \mid c_{1,d-1}x+c_{0,d-1}}} 1.$$

   Using (3.7.15) we can bound this by

   $$\ll p^{l-l/d}\sum_{m=1}^{l-d} p^{l-m} \ll p^{2l-l/d-1}.$$

   (b) Fix $l-d < m \leq l$. We can bound the sum over y by $O(p^{l-1})$ using Corollary 3.7.4. These terms therefore contribute

   $$\ll p^{l-1}\sum_{m=l-d+1}^{l} \sum_{\substack{x\in\mathbb{Z}/p^l\mathbb{Z} \\ p^m \mid c_{1,d-1}x+c_{0,d-1}}} 1.$$

   Again, using equation (3.7.15) we see the overall contribution in this case is

   $$\ll p^{l-1}\sum_{m=l-d+1}^{l} p^{l-m} \ll p^{l+d-2}.$$

Now, since $l > d$ the first term dominates. Putting everything together, we conclude that

$$\Phi(p^l;0,0) \ll p^{2l-l/d-1} + p^{l-1+\min\{l-1,l-l/d\}} + p^l \ll p^{2l-l/d-1}. \tag{3.7.25}$$

This agrees with the result stated.

□

Finally, we have the following.

Proposition 3.7.7. *Fix $\epsilon > 0$. For any integers M, N we have*

$$\sum_{0<|h|\ll B} \frac{\Phi(h; M, N)}{|h|^{2-1/d+\epsilon}} \ll_\epsilon \Delta_f(M, N, k)^\epsilon B^\epsilon. \tag{3.7.26}$$

Proof. Fix $0 < \delta < 1/d$. By multiplicativity, and the fact $\Phi(-h; M, N) = \Phi(h; M, N)$, we can bound our sum by

$$\sum_{0<|h|\ll B} \frac{\Phi(h; M, N)}{|h|^{2-\delta}} \ll \prod_{p\ll B} \left(1 + \frac{\Phi(p; M, N)}{p^{2-\delta}} + \sum_{l=2}^{\infty} \frac{\Phi(p^l; 0, 0)}{p^{l(2-\delta)}}\right).$$

We first deal with the contribution from higher powers. Using the bounds established in Lemma 3.7.6, this contribution is bounded by

$$\ll \frac{1}{p^2} \sum_{l=2}^{d} p^{l\delta} + \frac{1}{p} \sum_{l=d+1}^{\infty} \frac{1}{p^{l/d-\delta l}} \ll_\delta \frac{1}{p^{2-d\delta}} + \frac{1}{p^{2+1/d-(d+1)\delta}} \ll_\delta \frac{1}{p},$$

using the fact $\delta < 1/d$. Now, fix positive constants $A_i > 0$ which may depend on f, a, b and δ. We recall Lemma 3.7.2, which says that

$$|\Phi(p; M, N)| \ll p^{1/2}(p, \Delta_f(M, N, k))^{1/2}.$$

We see the contribution from those primes dividing $\Delta_f(M, N, k)$ is bounded by

$$\prod_{p|\Delta_f(M,N,k)} \left(1 + \frac{A_1}{p^{1-\delta}} + \frac{A_2}{p}\right) \ll_\delta \tau(\Delta_f(M, N, k)) \ll_{\delta,\epsilon} \Delta_f(M, N, k)^\epsilon.$$

The contribution from the remaining terms is bounded by

$$\begin{aligned}\prod_{p\ll B} \left(1 + \frac{A_3}{p^{3/2-\delta}} + \frac{A_4}{p}\right) &\ll_\delta \prod_{p\ll B} \left(1 + \frac{A_5}{p}\right) \\ &\ll_\delta \prod_{p\ll B} \left(1 + \frac{1}{p}\right)^{A_5} \ll_{\delta,\epsilon} B^\epsilon\end{aligned}$$

by Mertens' estimate. The proof of the proposition is completed upon taking $\delta = 1/d - \epsilon$. □

3.8 Final estimates

Let us recall our work so far. Putting together equations (3.5.10) and (3.5.16) we arrive at the bound

$$M_{f,g}(B;k) \ll_\epsilon \sum_{\substack{0<|h|\ll_{a,b} B \\ K_h, P_h \text{ smooth}}} \frac{1}{(\#\mathcal{P})^2} \sum_{p,q\in\mathcal{P}} \left| \sum_{i,j\in\{0,1,2\}} c_{i,j}(\alpha) S_{i,j}(p,q) \right| + B^{3/2+\epsilon} \quad (3.8.1)$$

where

$$S_{i,j}(p,q) = \frac{1}{(pqh)^2} \sum_{-pq|h|/2<m,n\leq pq|h|/2} \Gamma(B,m)\Gamma(B,n)\Psi_{i,j}(m,n). \quad (3.8.2)$$

Using Lemma 3.5.5 we were able to decompose the exponential sums $\Psi_{i,j}$ into the simpler exponential sums Σ_t and Φ which we were able to estimate individually. In this section we aim to bring everything together.

Firstly, we isolate the main term contribution to the above sum. To this end, let $L_{i,j}(p,q)$ denote the the contribution from the term $(m,n) = (0,0)$. Note that $\Gamma(B,0) = \lfloor B \rfloor$, and so, with the estimate $\lfloor B \rfloor = B + O(1)$, we obtain

$$L_{i,j}(p,q) = \frac{B^2\Psi_{i,j}(0,0)}{(pqh)^2} + O\left(\frac{B\Psi_{i,j}(0,0)}{(pqh)^2}\right). \quad (3.8.3)$$

Let us concentrate our attention on this first term. If $p \neq q$, then for $i,j \in \{0,1,2\}$, we have

$$\begin{aligned} \Psi_{i,j}(0,0) &= \Sigma_i(p;0,0)\Sigma_j(q;0,0)\Phi(h;0,0) \\ &= \max\{1,i\}\max\{1,j\}[p^2+O(p)][q^2+O(q)]\Phi(h;0,0) \end{aligned} \quad (3.8.4)$$

using Lemma 3.5.5 for the decomposition of $\Psi_{i,j}$ and Lemma 3.6.1 for the asymptotics for Σ_t. Recalling the definition of the constants $c_{i,j}(\alpha)$ in Proposition 3.5.1, we obtain an expression

$$\sum_{i,j\in\{0,1,2\}} c_{i,j}(\alpha)L_{i,j}(p,q) = \frac{B^2\Phi(h;0,0)}{h^2}(\alpha-1)^2 + O\left(\frac{B^2\Phi(h;0,0)}{\min\{p,q\}h^2}\right). \quad (3.8.5)$$

Thus we may take $\alpha = 1$ to eliminate the main term. In this case, including the error present in equation (3.8.3) and using the bound $\Psi_{i,j}(0,0) \ll p^2q^2\Phi(h;0,0)$ which follows from our work so far, we obtain

$$\sum_{i,j\in\{0,1,2\}} c_{i,j}(1)L_{i,j}(p,q) \ll \frac{B^2\Phi(h;0,0)}{\min\{p,q\}h^2} + \frac{B\Phi(h;0,0)}{h^2} \quad (3.8.6)$$

for the total contribution to the main term from terms with $p \neq q$. We see the first term dominates in our range of p and q. If $p = q$ then we bound trivially, to obtain

$$\sum_{i,j\in\{0,1,2\}} c_{i,j}(1)L_{i,j}(p,p) \ll \frac{B^2\Phi(h;0,0)}{h^2}. \tag{3.8.7}$$

Now note that, from Lemma 3.7.2 and Lemma 3.7.6, it follows that we can bound $\Phi(h;0,0) \ll A^{\omega(h)}h^2/\mathrm{rad}(|h|)$, where $A > 0$ is a constant and $\mathrm{rad}(|h|)$ denotes the radical of the non-zero integer h. Thus

$$\begin{aligned}\sum_{0<|h|\ll B} \frac{\Phi(h;0,0)}{h^2} &\ll \sum_{0<|h|\ll B} \frac{A^{\omega(h)}}{\mathrm{rad}(|h|)} \\ &\ll_\epsilon B^\epsilon \sum_{0<|h|\ll B} \frac{A^{\omega(h)}}{h^\epsilon \mathrm{rad}(|h|)} \\ &\ll_\epsilon B^\epsilon \prod_{p\ll B} \left(1 + \frac{A}{p}\left[\frac{1}{p^\epsilon} + \frac{1}{p^{2\epsilon}} + \dots\right]\right) \\ &\ll_\epsilon B^\epsilon \prod_{p\ll B} \left(1 + \frac{A}{p^{1+\epsilon/2}}\right) \ll_\epsilon B^\epsilon. \end{aligned} \tag{3.8.8}$$

Thus, the total contribution from the main term, using the asymptotic $\#\mathcal{P} \sim Q/\log Q$, is

$$\begin{aligned}\frac{B^2\log^2 Q}{Q^2} \sum_{0<|h|\ll B} \frac{\Phi(h;0,0)}{h^2}\Bigg[\sum_{\substack{p,q\in\mathcal{P}\\ p\neq q}} \frac{1}{\min\{p,q\}} + \sum_{p\in\mathcal{P}} 1\Bigg] &\\ \ll \frac{B^2\log Q\log\log Q}{Q} \sum_{0<|h|\ll B} \frac{\Phi(h;0,0)}{h^2} &\\ \ll_\epsilon \frac{B^{2+\epsilon}}{Q}. \end{aligned} \tag{3.8.9}$$

We now focus on the contribution from the remaining terms. From now on we put $T_{i,j} = S_{i,j} - L_{i,j}$. It follows that

$$T_{i,j}(p,q) \ll \frac{1}{(pqh)^2} \sum_{\substack{-pq|h|/2<m,n\leq pq|h|/2\\ (m,n)\neq(0,0)}} \min\left\{B, \frac{pq|h|}{|m|}\right\} \min\left\{B, \frac{pq|h|}{|n|}\right\} |\Psi_{i,j}(m,n)|. \tag{3.8.10}$$

We would like to find a pointwise estimate for the exponential sums $\Psi_{i,j}$. There are two regimes to consider.

1. If $p \neq q$, then recalling Lemma 3.5.5 and Lemma 3.6.1 we obtain

$$|\Psi_{i,j}(m,n)| \ll pq(pq,m,n)|\Phi(h;\overline{pq}m,\overline{pq}n)|.$$

   Here $\overline{pq}$ is the multiplicative inverse of pq modulo $|h|$.

2. If $p = q$, then again recalling the results above we have

$$|\Psi_{i,j}(m,n)| \ll 1_{p|(m,n)}p^3(p,m/p,n/p)\Phi(h;\overline{p}m/p,\overline{p}n/p).$$

   Here $\overline{p}$ is the multiplicative inverse of p modulo $|h|$.

Now if $p = q$ then $1_{p|(m,n)}p^3(p,m/p,n/p) \leq pq(pq,m,n)$. We conclude that the first bound holds in all cases. Thus we may write

$$T_{i,j} \ll \frac{1}{pqh^2} \sum_{\substack{-pq|h|/2<m,n\leq pq|h|/2 \\ (m,n)\neq(0,0)}} \min\left\{B, \frac{pq|h|}{|m|}\right\} \min\left\{B, \frac{pq|h|}{|n|}\right\}(pq,m,n)|\Phi(h;\overline{pq}m,\overline{pq}n)|. \tag{3.8.11}$$

There are now 3 regimes to consider.

1. The contribution from when $m = 0$ is

$$\frac{B}{|h|} \sum_{\substack{-pq|h|/2<n\leq pq|h|/2 \\ n\neq 0}} \frac{(pq,n)|\Phi(h;0,\overline{pq}n)|}{|n|}. \tag{3.8.12}$$

2. The contribution from when $n = 0$ is

$$\frac{B}{|h|} \sum_{\substack{-pq|h|/2<m\leq pq|h|/2 \\ m\neq 0}} \frac{(pq,m)|\Phi(h;\overline{pq}m,0)|}{|m|}. \tag{3.8.13}$$

3. The contribution from when $mn \neq 0$ is

$$pq \sum_{\substack{-pq|h|/2<m,n\leq pq|h|/2 \\ mn\neq 0}} \frac{(pq,m,n)|\Phi(h;\overline{pq}m,\overline{pq}n)|}{|m||n|}. \tag{3.8.14}$$

To evaluate these sums we will now bring the sum over h on the inside. Recall Proposition 3.7.7, which states that for any $\epsilon > 0$ we have

$$\sum_{0<|h|\ll B} \frac{\Phi(h;M,N)}{|h|^{2-1/d+\epsilon}} \ll_\epsilon \Delta_f(M,N,k)^\epsilon B^\epsilon, \tag{3.8.15}$$

and the corresponding results which follow by partial summation. From Lemma 3.7.1 we have the size bound

$$|\Delta_f(M,N,k)| \leq |k| \max\{|M|,|N|\}^{d^2}. \tag{3.8.16}$$

We are also assuming $0 < |k| \ll_f B^{d+1}$ (see (3.5.1)). In our range of variables we thus have

$$\Delta_f(\overline{pq}m, \overline{pq}n, k)^\epsilon \ll_\epsilon B^\epsilon \tag{3.8.17}$$

It follows that the total contribution from the terms $T_{i,j}$ is bounded by

$$\frac{B^{2-1/d+\epsilon}\log^2 Q}{Q^2} \sum_{p,q\in\mathcal{P}} \Bigg[\sum_{\substack{-pq|h|/2<n\leq pq|h|/2 \\ n\neq 0}} \frac{(pq,n)}{|n|} + pq \sum_{\substack{-pq|h|/2<m,n\leq pq|h|/2 \\ mn\neq 0}} \frac{(pq,m,n)}{|m||n|} \Bigg]. \tag{3.8.18}$$

This in turn is bounded by

$$\frac{B^{2-1/d+\epsilon}\log^2 Q}{Q^2} \sum_{p,q\in\mathcal{P}} pq \ll_\epsilon Q^2 B^{2-1/d+\epsilon}. \tag{3.8.19}$$

Putting together equation (3.8.9) and equation (3.8.19), we get a final bound

$$M_{f,g}(B;k) \ll_\epsilon B^\epsilon \left(Q^2 B^{2-1/d} + \frac{B^2}{Q} \right) \ll B^{2-1/(3d)+\epsilon}, \tag{3.8.20}$$

where we take $Q = B^{1/(3d)}$ to balance the error terms. The result stated in Theorem 3.1.2 follows upon noting that the exponent here is strictly less than $(2-1/(50d))$.

Appendix A

Estimates for $r(n)$ and $r(n)r(n+h)$

In this appendix we sketch proofs for Lemmas 2.5.3, 2.5.4 and 2.5.5 contained in Chapter 2. The first follows immediately from the following two results, due to Tolev [27, Theorem] and Plaksin (cf. discussion just before [23, Lemma 4]) respectively.

Lemma A.0.1. *We have*

$$\sum_{\substack{n\leq N\\ n\equiv\Delta\ (mod\ Q)}} r(n) = \frac{\eta(Q,\Delta)}{Q^2}\pi N + O((Q^{\frac{1}{2}}+N^{\frac{1}{3}})(\Delta,Q)^{\frac{1}{2}}\tau^4(Q)\log^4 N), \tag{A.0.1}$$

where

$$\eta(Q,\Delta) = \#\{1\leq\alpha,\beta\leq Q : \alpha^2+\beta^2\equiv\Delta\ (mod\ Q)\}.$$

Lemma A.0.2. *We have*

$$\sum_{\substack{n\leq N\\ n\equiv\Delta\ (mod\ Q)}} r(n) = \frac{A(Q,\Delta)}{Q}\pi N + O(P(N;Q,\Delta)), \tag{A.0.2}$$

where

$$A(Q,\Delta) = \left[1+\sum_{\substack{k\\ 4|2^k|(Q,4\Delta)}}\chi\left(\frac{4\Delta}{2^k}\right)\right]\sum_{r|Q}\frac{\chi(r)}{r}c_r(\Delta), \tag{A.0.3}$$

and $P(N;Q,\Delta)$ satisfies

$$\int_1^N P^2(y;Q,\Delta)\mathrm{d}y \ll_\epsilon (QN)^\epsilon(N^{\frac{3}{2}}+QN).$$

Here $c_r(\Delta)=\sum_{(a,r)=1}e^{\frac{2\pi i a\Delta}{r}}$ denotes the Ramanujan sum.

Proof of Lemma 2.5.3. Equating (A.0.1) and (A.0.2), dividing through by πN, and letting $N \to \infty$ we see that

$$\frac{\eta(Q,\Delta)}{Q^2} = \frac{A(Q,\Delta)}{Q}$$

holds for any fixed Q, Δ. Thus we may write

$$\sum_{\substack{n\leq N \\ n\equiv\Delta \pmod Q}} r(n) = \frac{A(Q,\Delta)}{Q} + O((Q^{\frac{1}{2}} + N^{\frac{1}{3}})(\Delta,Q)^{\frac{1}{2}}\tau^4(Q)\log^4 N). \tag{A.0.4}$$

Let $Q = 4qd$ and $\Delta \pmod Q$ be the solution to the congruence system $\Delta \equiv a \pmod q$, $\Delta \equiv 1 \pmod 4$, and $\Delta \equiv 0 \pmod d$, where $(a,q) = (d,q) = 1$ and q, d are square-free and odd. Then by multiplicativity of the Ramanujan sum and our assumptions about Δ, q and d from (A.0.3) we obtain

$$A(Q,\Delta) = 2\sum_{r|q} \frac{\chi(r)\mu(r)}{r} \sum_{r|d} \frac{\chi(r)\varphi(r)}{r} = 2g_1(q)g_2(d), \tag{A.0.5}$$

and so we obtain the result of Lemma 2.5.3 on dividing through by $Q = 4qd$. □

For Lemma 2.5.4 we have the following result.

Lemma A.0.3. *Suppose that $(a,q) = (a+h,q) = (d_1,q) = (d_2,q) = (d_1,d_2) = 1, 4|h$ where d_1, d_2, q are square-free and odd, of size $\ll N^{O(1)}$. Then for $0 < h < N^{\frac{3}{4}}$ we have*

$$\sum_{\substack{n\leq N \\ n\equiv a \ (mod\ q) \\ n\equiv 1 \ (mod\ 4) \\ d_1|n, d_2|n+h}} r(n)r(n+h) = \frac{g_1(q)^2}{q}\Gamma(h,d_1,d_2,q)\pi^2 N + R_2(N,d_1,d_2,q), \tag{A.0.6}$$

where

$$R_2(N,d_1,d_2,q) \ll_\epsilon q^{\frac{1}{2}}d_1d_2N^{\frac{3}{4}+\epsilon} + d_1^{\frac{1}{2}}d_2^{\frac{1}{2}}N^{\frac{5}{6}+\epsilon},$$

where

$$\Gamma(h,d_1,d_2,q) = \frac{g_2(d_1)g_2(d_2)}{d_1d_2} \sum_{(r,2q)=1} \frac{c_r(h)}{r^2} \frac{(d_1,r)(d_2,r)}{\Psi(d_1,r)\Psi(d_2,r)} \chi[(d_1^2,r)]\chi[(d_2^2,r)]$$

and g_1 is the multiplicative function defined on primes by $g_1(p) = 1 - \frac{\chi(p)}{p}$ and $\Psi(d_1,r) = g_2((d_1, r/(r,d_1)))$.

Proof of Lemma 2.5.4. Under the additional assumption that $p|h \Rightarrow p|2q$, then we see for r considered in the sum $c_r(h) = \mu(r)$. But now restricting to square-free r, since d_1, d_2 are square-free $\Psi(d_1, r) = \Psi(d_2, r) = 1$. Thus in this case

$$\Gamma(h, d_1, d_2, q) = \frac{g_2(d_1)g_2(d_2)}{d_1 d_2} \sum_{(r,2q)=1} \frac{\mu(r)(d_1, r)(d_2, r)}{r^2} \chi[(d_1^2, r)]\chi[(d_2^2, r)]. \tag{A.0.7}$$

This is the form stated in Lemma 2.5.4. □

Now we briefly outline the proof of Lemma A.0.3. In [23, Lemma 4] a similar sum to (A.0.6) is considered, this time under the hypotheses $p|d_1, d_2 \Rightarrow p \equiv 3 \pmod 4$, $q = 1$ and the congruence $n \equiv 1 \pmod 4$ is omitted. The proof of Lemma A.0.3 is similar to the proof found there, with few minor changes. The key point is to note that, using the convolution identity $r = 4(\chi * 1)$ and complete multiplicativity of χ, for $n \equiv 1 \pmod 4$ we can write

$$\begin{aligned}\frac{r(n)}{4} = \sum_{m|n} \chi(m) &= \sum_{\substack{m|n \\ m\leq\sqrt{N}}} \chi(m) + \sum_{\substack{m|n \\ m>\sqrt{N}}} \chi(m) = \sum_{\substack{m|n \\ m\leq\sqrt{N}}} \chi(m) + \sum_{\substack{l|n \\ l<\frac{n}{\sqrt{N}}}} \chi(l) \\ &= 2 \sum_{\substack{m|n \\ m\leq\sqrt{N}}} \chi(m) - \sum_{\substack{m|n \\ \frac{n}{\sqrt{N}}\leq m\leq\sqrt{N}}} \chi(m). \end{aligned} \tag{A.0.8}$$

Using this we may expand out $r(n)$ in the sum (A.0.6). We obtain (after swapping the order of summation)

$$\sum_{\substack{n\leq N \\ n\equiv a \pmod q \\ n\equiv 1 \pmod 4 \\ d_1|n, d_2|n+h}} r(n)r(n+h) = 4 \sum_{m\leq\sqrt{N}} \chi(m) \Bigg[2 \sum_{\substack{n\leq N \\ n\equiv a \pmod q \\ n\equiv 1 \pmod 4 \\ d_1|n, d_2|n+h \\ m|n}} r(n+h) - \sum_{\substack{n\leq m\sqrt{N} \\ n\equiv a \pmod q \\ n\equiv 1 \pmod 4 \\ d_1|n, d_2|n+h \\ m|n}} r(n+h) \Bigg].$$

These congruences have a solution if and only if $(m, q) = 1$ and $(m, d_2)|h$. In this case we can use the Chinese Remainder Theorem and write

$$\begin{aligned}\sum_{\substack{n\leq N \\ n\equiv a \pmod q \\ n\equiv 1 \pmod 4 \\ d_1|n, d_2|n+h}} r(n)r(n+h) = 4 \sum_{\substack{m\leq\sqrt{N} \\ (m,q)=1 \\ (m,d_2)|h}} \chi(m) \Bigg[2 \sum_{\substack{n\leq N \\ n\equiv \Delta \pmod Q}} r(n) - \sum_{\substack{n\leq m\sqrt{N} \\ n\equiv \Delta \pmod Q}} r(n) \Bigg] \\ + O_\epsilon((N^{\frac{1}{2}} + h)N^\epsilon), \end{aligned} \tag{A.0.9}$$

where $Q = 4q[m, d_1, d_2]$ and $\Delta \pmod Q$ satisfies the congruence system $\Delta \equiv a + h \pmod q, \Delta \equiv 1 \pmod 4, \Delta \equiv h \pmod m, \Delta \equiv h \pmod{d_1}$ and $\Delta \equiv 0 \pmod{d_2}$.

The error term arises by estimating the intervals of length h left over: taking absolute values, using the divisor bound $r(n) \ll n^{\epsilon}$, and noting that in this regime $h \ll N^{3/4}$, we have to estimate sums of type

$$N^{\epsilon} \sum_{m \leq \sqrt{N}} \sum_{\substack{X < n \leq X+h \\ n \equiv h \pmod{m}}} 1.$$

Applying the standard estimate $h/m + O(1)$ to the inner sum and then carrying out the summation over m yields the desired estimate (after redefining our choice of ϵ).

Now the inner sums in (A.0.9) consist of estimating $r(n)$ in arithmetic progressions. It proves convenient to proceed using formula (A.0.4). We obtain

$$4\pi \sum_{\substack{m \leq \sqrt{N} \\ (m,q)=1 \\ (m,d_2)|h}} \chi(m) \left[\frac{2N - m\sqrt{N}}{Q} \right] A(Q, \Delta) + R_2(N; d_1, d_2, q) + O_{\epsilon}((N^{\frac{1}{2}} + h)N^{\epsilon}), \quad \text{(A.0.10)}$$

where R_2 is an error term. Using the fact $(\Delta, Q) \leq d_1 d_2 (m, h)$ and $Q \ll mqd_1 d_2$ one can show R_2 contributes

$$R_2(N; d_1, d_2, q) \ll q^{\frac{1}{2}} d_1 d_2 N^{\frac{3}{4}+\epsilon} + d_1^{\frac{1}{2}} d_2^{\frac{1}{2}} N^{\frac{5}{6}+\epsilon},$$

and so this error term dominates. Now one can estimate the main term in (A.0.10) using the same techniques found in [23, Lemma 4].

For Lemma 2.5.5 we have the following result.

Lemma A.0.4. *Let $(a, q) = (d, q) = 1$ where d, q are square-free and odd, of size $\ll N^{O(1)}$. Then we have*

$$\sum_{\substack{n \leq x \\ n \equiv a \pmod{q} \\ n \equiv 1 \pmod{4} \\ d|n}} r^2(n) = \frac{16 H(1, d, 4q)}{\varphi(4q)} \left[\log x + 2\gamma - 1 + \frac{H'(1, d, 4q)}{H(1, d, 4q)} \right] x + O_{\epsilon}(q x^{\frac{3}{4}+\epsilon}), \quad \text{(A.0.11)}$$

where

$$H(s, d, 4q) = \frac{L^2(s, \chi_4) G(s, 4q) A(s, d)}{\zeta(2s)},$$

$$G(s, 4q) = \prod_{p|4q} \left(1 - \frac{1}{p^s}\right) \left(1 + \frac{1}{p^s}\right)^{-1} \left(1 - \frac{\chi_4(p)}{p^s}\right)^2,$$

$$A(s, d) = \prod_{\substack{p|d \\ p \equiv 3 \pmod{4}}} \frac{1}{p^{2s}} \prod_{\substack{p|d \\ p \equiv 1 \pmod{4}}} \frac{4p^{2s} - 3p^s + 1}{p^{2s}(p^s + 1)}.$$

Proof of Lemma 2.5.5. One obtains the main term as stated in Lemma 2.5.5 by taking the logarithmic derivative of $H(s,d,4q)$ (taking an appropriate branch-cut) and evaluating at $s=1$. □

We now outline the proof of Lemma A.0.4. The proof uses a standard application of Perron's formula. The following lemma, which combines [26, Theorem II.8.20] and [26, Theorem II.8.22], will prove necessary.

Lemma A.0.5. *Let $\mathcal{L} = \log(|t|+Q+1)$ and let $\chi_Q \pmod Q$ be a Dirichlet character. For $\sigma \geq 1$ we have the following*

1. *If χ_Q^2 is complex then $L(s,\chi_Q^2)^{-1} \ll \mathcal{L}^7$.*
2. *If χ_Q^2 is real, non-trivial, then there exists an absolute constant $c_0 > 0$ such that*

$$L(s,\chi_Q^2)^{-1} \ll \begin{cases} \mathcal{L}^6(\mathcal{L}+1/|t|) & \text{if } |t| > c_0 Q^{-\frac{1}{2}}(\log 2Q)^{-2}, \\ Q^{\frac{1}{2}} & \text{if } |t| \leq c_0 Q^{-\frac{1}{2}}(\log 2Q)^{-2}. \end{cases}$$

Write $Q = 4q$ and let $\Delta \pmod Q$ be the unique solution to the congruences $\Delta \equiv a \pmod q$ and $\Delta \equiv 1 \pmod 4$. Since $(\Delta, Q) = 1$ by character orthogonality we can write

$$\sum_{\substack{n\leq x \\ n\equiv \Delta \pmod Q \\ d|n}} r^2(n) = \frac{1}{\varphi(Q)} \sum_{\chi_Q \pmod Q} \overline{\chi(\Delta)} \sum_{\substack{n\leq x \\ d|n}} r^2(n)\chi_Q(n).$$

We study these sums by considering their generating series

$$F_d(s,\chi_Q) = \sum_{n=1}^{\infty} \frac{r^2(dn)\chi_Q(dn)}{(dn)^s}$$

Write $F(s,\chi_Q) = F_1(s,\chi_Q)$. Then

$$F(s,\chi_Q) = 16L^2(s,\chi_Q)L^2(s,\chi_4\chi_Q)L(2s,\chi_Q^2)^{-1}.$$

Here χ_4 denotes the unique non-trivial character (mod 4), and $L(s,\chi_D)$ denotes the L series corresponding to the Dirichlet character $\chi_D \pmod D$. It follows that

$$\begin{aligned} \frac{F_d(s,\chi_Q)}{F(s,\chi_Q)} &= \prod_{p|d} \left(\sum_{k=1}^{\infty} \frac{r(p^k)^2\chi_Q(p^k)}{p^{ks}} \right) \left(\sum_{k=0}^{\infty} \frac{r(p^k)^2\chi_Q(p^k)}{p^{ks}} \right)^{-1} \\ &= \prod_{\substack{p|d \\ p\equiv 3 \pmod 4}} \frac{\chi_Q(p)^2}{p^{2s}} \prod_{\substack{p|d \\ p\equiv 1 \pmod 4}} \frac{\frac{4p^{2s}}{\chi_Q(p)^2} - \frac{3p^s}{\chi_Q(p)} + 1}{\frac{p^{2s}}{\chi_Q(p)^2}(\frac{p^s}{\chi_Q(p)}+1)} = A(s,d,Q) \end{aligned}$$

say, using the fact d is square-free and $(d,Q)=1$. We note the divisor bound $|r^2(n)\chi_q(n)| \leq \tau^2(n) \leq e^{C\frac{\log n}{\log\log n}}$ for some explicit $C>0$. We can apply an effective form of Perron's formula (for example [26, Corollary II.2.4]), averaging over the height T, to obtain

$$\sum_{\substack{n\leq x\\ n\equiv\Delta \pmod Q\\ d|n}} r^2(n) = I(T;Q,\Delta,d) + O\bigg(\frac{x(\log x)^2}{T} + e^{\frac{2C\log x}{\log\log x}}\bigg(1+\frac{x\log T}{T}\bigg)\bigg),$$

where

$$I = \frac{1}{\varphi(Q)}\sum_{\chi_Q \pmod Q}\overline{\chi_Q(\Delta)}\bigg[\frac{1}{T}\int_T^{2T}\bigg(\frac{1}{2\pi i}\int_{c-it_0}^{c+it_0}\frac{16L^2(s,\chi_Q)L^2(s,\chi_4\chi_Q)A(s,d,Q)x^s}{L(2s,\chi_Q^2)s}\mathrm{d}s\bigg)\mathrm{d}t_0\bigg].$$

Here $c=1+1/\log x$. We move the contour to the region defined by $[c-it_0, c+it_0]$, $[1/2+it_0, c+it_0]$, $[1/2-it_0, 1/2+it_0]$ and $[1/2-it_0, c+it_0]$. The integrand has a pole of order 2 at $s=1$, coming from the trivial character $\chi_0 \pmod Q$. The residue of this pole is

$$H(1,d,Q)\bigg(\log x + 2\gamma - 1 + \frac{H'(1,d,Q)}{H(1,d,Q)}\bigg)x,$$

where

$$\begin{aligned} H(s,d,Q) &= \frac{16L^2(s,\chi_4)G(s,Q)A(s,d)}{\zeta(2s)},\\ G(s,Q) &= \prod_{p|Q}\bigg(1-\frac{1}{p^s}\bigg)\bigg(1+\frac{1}{p^s}\bigg)^{-1}\bigg(1-\frac{\chi_4(p)}{p^s}\bigg)^2,\\ A(s,d) &= \prod_{\substack{p|d\\ p\equiv 3 \pmod 4}}\frac{1}{p^{2s}}\prod_{\substack{p|d\\ p\equiv 1 \pmod 4}}\frac{4p^{2s}-3p^s+1}{p^{2s}(p^s+1)}. \end{aligned}$$

We need bounds for the integrand in the region $\sigma \geq 1/2$ and $|t| \leq 2T$. One can easily check the trivial bound $|A(s,d,Q)| \ll 1$ (uniformly in d and q). We require a lower bound for $|L(2s,\chi_Q^2)|$ in this region. If χ_Q is real then χ_Q^2 is the trivial character, and so we have

$$L(2s,\chi_Q^2) = \zeta(2s)\prod_{p|Q}\bigg(1-\frac{1}{p^{2s}}\bigg).$$

In the region $\sigma \geq \frac{1}{2}$ we can bound the product from below by $\varphi(Q)/Q$. Standard bounds for $\zeta(s)$ on the 1-line (see for example [26, Theorem II.3.9]) then tell us that

$$L(2s,\chi_Q^2)^{-1} \ll \frac{Q}{\varphi(Q)}\log(|t|+2) \ll_\epsilon (QT)^\epsilon.$$

If χ_Q is complex then we have to be more careful. We use Lemma A.0.5, and see there is a minor technical complication where we must bound the contribution from $s = 1/2 + it$ with $|t| \leq 2c_0$ (say) separately (with this choice of cut-off we can use the bound $L(2s, \chi_Q^2) \ll (QT)^\epsilon$ uniformly in χ_Q for all the other contours). One can easily show the contribution from these values of s is $\ll Q^{\frac{1}{2}}$, which is small.

To bound the contribution from the other integrals, we can use the fourth-moment estimate for Dirichlet L-functions on the critical line in the form

$$\frac{1}{\varphi(D)T} \sum_{\chi \pmod D} \int_T^{2T} |L(1/2 + it, \chi)|^4 \mathrm{d}t \ll (DT)^\epsilon,$$

(cf. [6, Theorem 1]) together with the Cauchy-Schwarz inequality. One can show that, with the choice $T = x^{\frac{1}{4}}$, the contours contribute $\ll_\epsilon Qx^{\frac{3}{4}+\epsilon}$.

Appendix B

Auxiliary estimates for $\rho(n)$

In this appendix we sketch the proof of Lemma 2.5.6 appearing in Chapter 2. We use the Selberg-Delange method.

Lemma B.0.1 (Selberg-Delange method)**.** *Let $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet series such that the function $G(s;z) = F(s)\zeta(s)^{-z}$ can be analytically continued to the region*

$$\sigma > 1 - \frac{c_0}{1 + \log(2 + |t|)} \tag{B.0.1}$$

for some positive $c_0 > 0$ and $z \in \mathbb{C}$ with $|z| \leq A$, and moreover satisfies the bounds $|G(s;z)| \ll M(1+|t|)^{1-\delta}$ for some $\delta > 0$ in this region. Let $Z_1(s;z) = [\zeta(s)(s-1)]^z$, $Z_2(s;z) = \frac{Z_1(s;z)}{s}$ (both holomorphic in the disc $|s-1| < 1$) and let

$$G(s;z)Z_1(s;z) = \sum_{k=0}^{\infty} \mu_k(z)(s-1)^k,$$
$$G(s;z)Z_2(s;z) = \sum_{k=0}^{\infty} \eta_k(z)(s-1)^k$$

be the Taylor series in this region. Then for any $N \geq 0$ and $|z| \leq A$ we have

$$\sum_{n \leq x} \frac{a_n}{n} \log \frac{x}{n} = (\log x)^{z+1} \left[\sum_{k=0}^{N} \frac{\mu_k(z)}{\Gamma(z+2-k)(\log x)^k} + O(MR_N(x)) \right], \tag{B.0.2}$$

and moreover if $a_n > 0$ then we also have

$$\sum_{n \leq x} a_n = x(\log x)^{z-1} \left[\sum_{k=0}^{N} \frac{\eta_k(z)}{\Gamma(z-k)(\log x)^k} + O(MR_N(x)) \right], \tag{B.0.3}$$

where

$$R_N(x) = R_N(x; c_1, c_2) = e^{-c_1\sqrt{\log x}} + O\left(\frac{c_2 N + 1}{\log(x+1)} \right)^{N+1} \tag{B.0.4}$$

for some suitable constants $c_1, c_2 > 0$. These positive constants, and the implicit constants in the Landau symbol, depend at most on c_0, δ and A.

The second statement is exactly [26, Theorem II.5.2]. The first statement follows by the same proof with a few minor changes.

Lemma 2.5.6 follows from suitable applications of Lemma B.0.1. We sketch the details in each case.

Proof of Lemma 2.5.6. (i) For $X_{N,W}$ recall from (2.5.2) the definition

$$X_{N,W} = \sum_{\substack{a \leq v \\ (a,W)=1 \\ p|a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)}{a} \log \frac{v}{a}. \tag{B.0.5}$$

Consider the generating series, for $\sigma > 1$

$$h_1(W,s) = \sum_{\substack{n=1 \\ (n,W)=1 \\ p|n \Rightarrow p \equiv 1 \pmod 4}}^{\infty} \frac{\mu(n)}{n^s} = \prod_{\substack{p \nmid W \\ p \equiv 1 \pmod 4}} \left(1 - \frac{1}{p^s}\right) = \frac{K_1(s) G_1(W,s)}{(\zeta(s) L(s,\chi_4))^{\frac{1}{2}}},$$

where

$$K_1(s)^2 = \left(1 - \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^{2s}}\right)^{-1},$$

$$G_1(W,s) = \prod_{\substack{p|W \\ p \equiv 1 \pmod 4}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

(taking the positive determination of the square-root in the first instance). Both of these functions are analytic for $\sigma > 3/4$ (say). $K_1(s)$ is bounded in this region, and $G_1(W,s)$ satisfies

$$\begin{aligned} |G_1(W,s)| &\leq \prod_{\substack{p|W \\ p \equiv 1 \pmod 4}} \left(1 - \frac{1}{p^{\frac{3}{4}}}\right)^{-1} = \exp\left[- \sum_{\substack{p \leq D_0 \\ p \equiv 1 \pmod 4}} \log\left(1 - \frac{1}{p^{3/4}}\right)\right] \\ &= \exp \sum_{\substack{p \leq D_0 \\ p \equiv 1 \pmod 4}} \left[\frac{1}{p^{3/4}} + O\left(\frac{1}{p^{3/2}}\right)\right] \ll \exp \sum_{\substack{p \leq D_0 \\ p \equiv 1 \pmod 4}} \frac{D_0^{1/4}}{p} \\ &\ll \exp(D_0^{1/4} \log\log D_0). \end{aligned}$$

We remark that with the choice $D_0 = (\log\log N)^3$, we certainly have the bound

$$\exp(D_0^{1/4} \log\log D_0) \ll_\epsilon (\log N)^\epsilon$$

for any fixed $\epsilon > 0$, and using this estimate, it is a simple task to verify that all the error terms which follow are indeed controlled. (Recall $v = N^\theta$ for some fixed $\theta > 0$.)

From the classical zero-free region for Dirichlet L-functions, $L(s)^{-1}$ can be analytically continued to a region of the form (B.0.1) for some c_0 and moreover satisfies a bound $L(s)^{-1} \ll \log(2+|t|)$ in this region (cf. [8, Chapter 14]). Thus we can apply Lemma B.0.1 with $M = \exp(D_0^{1/4}\log\log D_0), z = -\frac{1}{2}, N = 0$ and some suitable choices of c_0, δ, to obtain

$$X_{N,W} = \frac{K_1(1)G_1(W)}{\Gamma(3/2)\sqrt{L(1,\chi_4)}}(\log v)^{\frac{1}{2}} + O\bigg(\frac{\exp(D_0^{\frac{1}{4}}\log\log D_0)}{(\log v)^{\frac{1}{2}}}\bigg).$$

Here we have written $G_1(W) = G_1(W,1)$ (and this convention will be continued below the fold). This simplifies to the stated result. Note that

$$G_1(W) = \prod_{\substack{p\le D_0\\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p}\right)^{-1} \asymp (\log D_0)^{\frac{1}{2}}$$

by Mertens' theorem.

(ii) For $Y_{N,W}$ recall from (2.5.3) the definition

$$Y_{N,W} = \sum_{\substack{a,b\le v\\ (a,W)=(b,W)=1\\ (a,b)=1\\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)}{g_7(a)g_7(b)}\log\frac{v}{a}\log\frac{v}{b}. \tag{B.0.6}$$

Take the sum over b on the inside. We can evaluate

$$\sum_{\substack{b\le v\\ (b,a\overline{W})=1\\ p|b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(b)}{g_7(b)}\log\frac{v}{b}$$

using the generating function, for $\sigma > 1$

$$h_2(aW,s) = \sum_{\substack{n=1\\ (n,aW)=1\\ p|n\Rightarrow p\equiv 1 \pmod 4}}^{\infty} \frac{\mu(n)n}{n^s g_7(n)} = h_1(aW,s)K_2(s)G_2(aW,s),$$

where

$$K_2(s) = \prod_{p \equiv 1 \pmod 4} \left(1 + \frac{1}{(p^s-1)(p+1)}\right),$$
$$G_2(aW, s) = \prod_{\substack{p \mid aW \\ p \equiv 1 \pmod 4}} \left(1 + \frac{1}{(p^s-1)(p+1)}\right)^{-1}.$$

Arguing as above, Lemma B.0.1 yields

$$Y_{N,W} = T_1 + T_2 + O(T_3),$$

this time taking $M = \exp(D_0^{1/4} \log\log D_0)$, $z = -1/2$ and $N = 1$. Here

$$T_3 = \frac{M}{(\log v)^{\frac{3}{2}}} \sum_{\substack{a \le v \\ (a,W)=1 \\ p \mid a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu^2(a)\tau(a)}{g_7(a)} \log\frac{v}{a} \ll \frac{M}{(\log v)^{\frac{1}{2}}} \prod_{\substack{p \le v \\ p \equiv 1 \pmod 4}} \left(1 + \frac{2}{p+1}\right)$$
$$\ll \frac{M}{(\log v)^{\frac{1}{2}}} \prod_{\substack{p \le v \\ p \equiv 1 \pmod 4}} \left(1 + \frac{1}{p}\right)^2 \ll M(\log v)^{\frac{1}{2}} = \exp(D_0^{1/4} \log\log D_0)(\log v)^{\frac{1}{2}}.$$

To evaluate T_2, we need a handle on the second Taylor series coefficient. With notation as in the statement of Lemma B.0.1, this is labelled $\mu_1(-1/2)$ and is precisely equal to

$$G(1)Z_1'(1; -1/2) + G'(1)Z_1(1; -1/2),$$

where

$$G(s) = \frac{K_1(s)G_1(aW, s)K_2(s)G_2(aW, s)}{L(s, \chi_4)^{1/2}}$$

(taking an appropriate branch-cut). Here all derivatives are taken with respect to s. By a series expansion, one can directly show that $Z_1(1; -1/2) = 1$ and $Z_1'(1; -1/2) = -\gamma/2$, where γ is the Euler-Mascheroni constant. We now note the following:

$$G_1(p)G_2(p) = \frac{g_7(p)}{p},$$
$$G_1'(d) = G_1(d) \sum_{\substack{p \mid d \\ p \equiv 1 \pmod 4}} \frac{\log p}{p-1},$$
$$G_2'(d) = G_2(d) \sum_{\substack{p \mid d \\ p \equiv 1 \pmod 4}} \frac{\log p}{p(p-1)}.$$

Here we have defined $G_i'(d) = \frac{\mathrm{d}G_i(d,s)}{\mathrm{d}s}\big|_{s=1}$ for $i \in \{1,2\}$. These results are valid for primes $p \equiv 1 \pmod 4$, and for any square-free d. Thus one can write T_2 as a finite linear combination

$$T_2 = \frac{1}{(\log v)^{\frac{1}{2}}} \sum_i c_i \alpha_i(W_1) R_i,$$

where $c_i \in \mathbb{R}$ are bounded,

$$\alpha_i(W_1) \in \left\{ \frac{g_7(W_1)}{W_1},\ \frac{g_7(W_1)}{W_1} \sum_{p \mid W_1} \frac{\log p}{p-1},\ \frac{g_7(W_1)}{W_1} \sum_{p \mid W_1} \frac{\log p}{p(p-1)} \right\},$$

and R_i is one of

$$\sum_{\substack{a \leq v \\ (a,W)=1 \\ p \mid a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)}{a} \log \frac{v}{a} \ll (\log D_0)^{1/2} (\log v)^{\frac{1}{2}}$$

or

$$\sum_{\substack{D_0 < q < v \\ q \equiv 1 \pmod 4}} \frac{\log q}{q-1} \sum_{\substack{a \leq v \\ (a,W)=1 \\ q \mid a \\ p \mid a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)}{a} \log \frac{v}{a} \ll \exp(D_0^{1/4} \log\log D_0)(\log v)^{1/2},$$

or finally

$$\sum_{\substack{D_0 < q < v \\ q \equiv 1 \pmod 4}} \frac{\log q}{q(q-1)} \sum_{\substack{a \leq v \\ (a,W)=1 \\ q \mid a \\ p \mid a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)}{a} \log \frac{v}{a} \ll \frac{(\log D_0)^{3/2} (\log v)^{1/2}}{D_0^2}.$$

Here q denotes a prime variable (a convention that will also be used below the fold). The first estimate follows directly from our expression for $X_{N,W}$ found above. For the last two estimates, we note that the inner sum appearing in both is precisely $X_{N,W} - X_{N,qW}$, and from our work above it follows that

$$\begin{aligned} X_{N,W} - X_{N,qW} &= \frac{K_1(1)}{\Gamma(3/2)\sqrt{L(1,\chi_4)}} (\log v)^{\frac{1}{2}} (G_1(W) - G_1(qW)) + O\left(\frac{\exp(D_0^{\frac{1}{4}} \log\log D_0)}{(\log v)^{\frac{1}{2}}} \right) \\ &\ll \frac{(\log D_0)^{\frac{1}{2}} (\log v)^{\frac{1}{2}}}{q} + \frac{\exp(D_0^{\frac{1}{4}} \log\log D_0)}{(\log v)^{\frac{1}{2}}}. \end{aligned}$$

Now, standard estimates for sums over primes such as

$$\sum_{\substack{q > D_0 \\ q \equiv 1 \pmod 4}} \frac{\log q}{q(q-1)} \ll \frac{\log D_0}{D_0},$$

yields the results stated.

Now, using the fact

$$\sum_{p|W_1} \frac{\log p}{p-1} \ll \log D_0,$$

and

$$\frac{g_7(W_1)}{W_1} = \prod_{\substack{p \le D_0 \\ p \equiv 1 \pmod 4}} \left(1 + \frac{1}{p}\right) \ll (\log D_0)^{\frac{1}{2}},$$

it follows that the total contribution from T_2 is

$$T_2 \ll (\log D_0)^{3/2} \exp(D_0^{1/4} \log\log D_0)(\log v)^{1/2}$$

which is negligible.

Finally, we can write

$$T_1 = \frac{K_1(1)K_2(1)G_1(W_1)G_2(W_1)(\log v)^{\frac{1}{2}}}{\Gamma(3/2)\sqrt{L(1,\chi_4)}} \sum_{\substack{a \le v \\ (a,\widetilde{W})=1 \\ p|a \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)}{a} \log \frac{v}{a}$$

This last sum is exactly $X_{N,W}$. Using our bound from part (i), and also the fact

$$K_2(1)G_2(W_1) = \prod_{\substack{p > D_0 \\ p \equiv 1 \pmod 4}} \left(1 + \frac{1}{p^2-1}\right) = 1 + O(D_0^{-1}),$$

we arrive at a final estimate of

$$Y_{N,W} = (1 + O(D_0^{-1}))\left[\frac{K_1(1)G_1(W)}{\Gamma(3/2)\sqrt{L(1,\chi_4)}}\right]^2 \log v + O((\log D_0)^{3/2} \exp(D_0^{1/4} \log\log D_0)(\log v)^{1/2}).$$

(iii) For $Z_{N,W}^{(1)}$ recall from (2.5.4) the definition

$$Z_{N,W}^{(1)} = \sum_{\substack{a,b \le v \\ (a,W)=(b,W)=1 \\ p|a,b \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log \frac{v}{a} \log \frac{v}{b}. \tag{B.0.7}$$

We write this as

$$\sum_{\substack{a\le v\\(a,W)=1\\p|a\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)g_4(a)}{g_2(a)a}\log\frac{v}{a}\sum_{d|a}\frac{d}{g_4(d)}\sum_{\substack{b\le v\\(b,W)=1\\(b,a)=d\\p|b\Rightarrow p\equiv 1 \pmod 4}}\frac{\mu(b)g_4(b)}{g_2(b)b}\log\frac{v}{b}.$$

Now substitute $b=md$. The inner sums can be rewritten as

$$\sum_{d|a}\frac{\mu(d)}{g_2(d)}\sum_{\substack{m\le v/d\\(m,aW)=1\\p|m\Rightarrow p\equiv 1 \pmod 4}}\frac{\mu(m)g_4(m)}{g_2(m)m}\log\frac{v}{md},$$

where we have used the fact a is square-free. To handle the inner sum we consider the generating series

$$h_3(aW,s)=\sum_{\substack{n=1\\(n,aW)=1\\p|n\Rightarrow p\equiv 1 \pmod 4}}^{\infty}\frac{\mu(n)g_4(n)}{n^s g_2(n)}=\frac{K_3(s)K_4(s)G_3(aW,s)G_4(aW,s)}{\zeta(s)L(s,\chi_4)},$$

where

$$\begin{aligned}
K_3(s)&=\left(1-\frac{1}{2^s}\right)^{-1}\prod_{p\equiv 3 \pmod 4}\left(1-\frac{1}{p^{2s}}\right)^{-1}\prod_{p\equiv 1 \pmod 4}\left(1-\frac{1}{(p^s-1)^2}\right),\\
K_4(s)&=\prod_{p\equiv 1 \pmod 4}\left(1+\frac{5p-3}{(p+1)(2p-1)(p^s-2)}\right),\\
G_3(aW,s)&=\prod_{\substack{p|aW\\p\equiv 1 \pmod 4}}\left(1-\frac{2}{p^s}\right)^{-1},\\
G_4(aW,s)&=\prod_{\substack{p|aW\\p\equiv 1 \pmod 4}}\left(1+\frac{5p-3}{(p+1)(2p-1)(p^s-2)}\right)^{-1}.
\end{aligned}$$

These four functions are analytic in the region $\sigma > 3/4$ (say), where they all satisfy the bound $O(1)$ except for G_3. Since $(a,W)=1$, by multiplicativity we can write $G_3(aW,s)=G_3(a,s)G_3(W,s)$. As above, we can bound $|G_3(W,s)|\ll \exp(D_0^{1/4}\log\log D_0)$ in this region. On the other hand, note that

$$1\le\left(1-\frac{2}{p^{3/4}}\right)^{-1}\le 2$$

whenever $p\ge 7$. Since we are assuming a is square-free, it follows that we can bound $|G_3(a,s)|\ll\tau(a)$.

By similar arguments to part (i) we can apply Lemma B.0.1 taking $z = -1, M = \tau(a)\exp(D_0^{1/4}\log\log D_0)$ and suitable δ, c_0. Note that for $N \geq 1$ the terms $\mu_k(z)(\log x)^{z+1-k}/\Gamma(z+2-k)$ are 0 for $1 \leq k \leq N$. Hence we can choose $N = \lfloor (\log x)/ec_1 \rfloor$ (for some suitable $c_1 > 0$) to balance the error terms, yielding a stronger error term of the form $O(Me^{-c_1\sqrt{\log x}})$. Using this choice of N we obtain

$$\sum_{\substack{m\leq v/d\\(m,aW)=1\\p|m\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(m)g_4(m)}{g_2(m)m}\log\frac{v}{md} = \frac{K_3(1)K_4(1)G_3(aW)G_4(aW)}{L(1,\chi_4)} + O\left(Me^{-c_1\sqrt{\log v/d}}\right).$$

This error term contributes

$$\ll \exp(D_0^{1/4}\log\log D_0) \sum_{\substack{a\leq v\\p|a\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu^2(a)g_4(a)\tau(a)}{g_2(a)a}\log\frac{v}{a}\sum_{d|a}\frac{\mu^2(d)}{g_2(d)}e^{-c_1\sqrt{\log v/d}}.$$

Swapping sums yields

$$\sum_{\substack{d\leq v\\p|d\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu^2(d)g_4(d)\tau(d)}{g_2(d)^2 d}e^{-c_1\sqrt{\log v/d}} \sum_{\substack{m\leq v/d\\(m,d)=1\\p|m\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu^2(m)g_4(m)\tau(m)}{g_2(m)m}\log\frac{v}{md}$$

The inner sum can be bounded by

$$\ll \log\frac{v}{d}\prod_{\substack{p\leq v/d\\p\equiv 1 \pmod 4}}\left(1+\frac{2(4p^2-3p+1)}{p(p+1)(2p-1)}\right) \ll \log\frac{v}{d}\prod_{\substack{p\leq v/d\\p\equiv 1 \pmod 4}}\left(1+\frac{4}{p}\right),$$
$$\ll \log\frac{v}{d}\prod_{\substack{p\leq v/d\\p\equiv 1 \pmod 4}}\left(1+\frac{1}{p}\right)^4 \ll \left(\log\frac{v}{d}\right)^3 \ll e^{c_2\sqrt{\log v/d}}$$

for some suitably small $c_2 > 0$. Note this final bound is valid for all $d \leq v$. Using the fact $g_4(d)/g_2(d)^2 \leq 1$, we see the total error is

$$\ll \exp(D_0^{1/4}\log\log D_0) \sum_{\substack{d\leq v\\p|d\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu^2(d)\tau(d)}{d}e^{-c_3\sqrt{\log v/d}} \tag{B.0.8}$$

for some $0 < c_3 < c_1$. For this sum, we use the generating series, for $\sigma > 1$

$$\sum_{\substack{n=1\\p|n\Rightarrow p\equiv 1 \pmod 4}}^{\infty} \frac{\mu^2(n)\tau(n)}{n^s} = \prod_{p\equiv 1 \pmod 4}\left(1+\frac{2}{p^s}\right) = \frac{\zeta(s)L(s,\chi_4)K(s)}{\zeta(2s)L(2s,\chi_4)},$$

where

$$K(s) = \left(1+\frac{1}{2^s}\right)^{-1} \prod_{p\equiv 3 \pmod 4} \left(1+\frac{1}{p^{2s}}\right)^{-1} \prod_{p\equiv 1 \pmod 4} \left(1+\frac{1}{p^s(p^s+2)}\right).$$

By the second part of Lemma B.0.1, taking $z = 1$ and $N = \lfloor (\log x)/ec_4 \rfloor$ for some suitable $c_4 > 0$ we get

$$\sum_{\substack{d\le v \\ p|d \Rightarrow p\equiv 1 \pmod 4}} \mu^2(d)\tau(d) = \frac{L(1,\chi_4)K(1)}{\zeta(2)L(2,\chi_4)} v + O(ve^{-c_4\sqrt{\log v}}).$$

Now by splitting the sum at $v^{1-\epsilon}$ and using partial summation one can show that

$$\sum_{\substack{d\le v \\ p|d \Rightarrow p\equiv 1 \pmod 4}} \frac{\mu^2(d)\tau(d)}{d} e^{-c_3\sqrt{\log v/d}} \ll 1 + (\epsilon + e^{-c_3\sqrt{\epsilon \log v}}) \log v.$$

Hence, taking $\epsilon = \frac{(\log\log v)^3}{\log v}$, we see the error (B.0.8) is $O(\exp(D_0^{1/4}\log\log D_0)(\log\log v)^3)$, which is small. Let $\gamma_1(a) = \sum_{d|a} \mu(d)/g_2(d)$. We obtain a main term

$$\frac{K_3(1)K_4(1)G_3(W)G_4(W)}{L(1,\chi_4)} \sum_{\substack{a\le v \\ (a,W)=1 \\ p|a \Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)g_4(a)\gamma_1(a)G_3(a)G_4(a)}{g_2(a)a} \log\frac{v}{a}.$$

For this sum we consider the generating series, for $\sigma > 1$

$$h_4(W,s) = \sum_{\substack{n=1 \\ (n,W)=1 \\ p|n \Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(n)g_4(n)\gamma_1(n)G_3(n)G_4(n)}{n^s g_2(n)} = h_1(W,s)K_5(s)G_5(W,s).$$

where

$$K_5(s) = \prod_{p\equiv 1 \pmod 4} \left(1 - \frac{(p-1)^2}{(p^s-1)(2p-1)(2p^2-p+1)}\right),$$

$$G_5(W,s) = \prod_{\substack{p|W \\ p\equiv 1 \pmod 4}} \left(1 - \frac{(p-1)^2}{(p^s-1)(2p-1)(2p^2-p+1)}\right)^{-1}.$$

Applying Lemma B.0.1 with $N = 0$ gives

$$Z_{N,W}^{(1)} = C_W(\log v)^{\frac{1}{2}} + O(\exp(D_0^{1/4}\log\log D_0)(\log\log v)^3),$$

where

$$C_W = \frac{K_1(1)K_3(1)K_4(1)K_5(1)G_1(W)G_3(W)G_4(W)G_5(W)}{\Gamma(3/2)L(1,\chi_4)^{\frac{3}{2}}} \tag{B.0.9}$$

which reduces to the stated result (note that

$$K_3(1)G_3(W) = \frac{A^2}{g_1(W_1)^2} \prod_{\substack{p>D_0 \\ p\equiv 1 \pmod 4}} \left(1 - \frac{1}{(p-1)^2}\right) = \frac{A^2}{g_1(W_1)^2}(1 + O(D_0^{-1}))$$

to get the form stated). We note for future reference that $|C_W| \asymp (\log D_0)^{3/2}$.

(iv) For $Z^{(2)}_{N,W}$ recall from (2.5.5) the definition

$$Z^{(2)}_{N,W} = \sum_{\substack{a,b\le v \\ (a,W)=(b,W)=1 \\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log\frac{v}{a}\log\frac{v}{b}\sum_{p|[a,b]} g_6(p). \tag{B.0.10}$$

We can write

$$\begin{aligned} Z^{(2)}_{N,W} &= \sum_{\substack{D_0<q\le v \\ q\equiv 1 \pmod 4}} g_6(q) \sum_{\substack{a,b\le v \\ (a,W)=(b,W)=1 \\ q|[a,b] \\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log\frac{v}{a}\log\frac{v}{b} \\ &= \sum_{\substack{D_0<q\le v \\ q\equiv 1 \pmod 4}} g_6(q)\Big[T_1 + T_2 - T_3\Big]. \end{aligned}$$

where q is prime, and

$$\begin{aligned} T_1 &= \sum_{\substack{a,b\le v \\ (a,W)=(b,W)=1 \\ q|a \\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log\frac{v}{a}\log\frac{v}{b}, \\ T_2 &= \sum_{\substack{a,b\le v \\ (a,W)=(b,W)=1 \\ q|b \\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log\frac{v}{a}\log\frac{v}{b}, \\ T_3 &= \sum_{\substack{a,b\le v \\ (a,W)=(b,W)=1 \\ q|a,b \\ p|a,b\Rightarrow p\equiv 1 \pmod 4}} \frac{\mu(a)\mu(b)g_4([a,b])}{g_2(a)g_2(b)[a,b]} \log\frac{v}{a}\log\frac{v}{b}. \end{aligned}$$

T_1 can be evaluated similarly to part (iii) to give

$$T_1 = \frac{C_W\beta_1(q)}{q}(\log v/q)^{\frac{1}{2}} + O\left(\frac{\exp(D_0^{1/4}\log\log D_0)(\log\log v)^3}{q}\right),$$

where

$$\beta_1(q) = \frac{\mu(q)g_4(q)\gamma_1(q)G_1(q)G_3(q)G_4(q)G_5(q)}{g_2(q)} = -\frac{q(4q^2-3q+1)}{2(q-1)(2q^2-2q+1)}.$$

T_2 can be evaluated similarly. For T_3, write $a = a'q, b = b'q$ then $[a,b] = [qa', qb'] = q[a',b']$ so that

$$T_3 = \frac{\mu^2(q)g_4(q)}{g_2(q)^2 q} \sum_{\substack{a',b' \le v/q \\ (a',qW)=(b',qW)=1 \\ p|a',b' \Rightarrow p \equiv 1 \pmod 4}} \frac{\mu(a')\mu(b')g_4([a',b'])}{g_2(a')g_2(b')[a',b']} \log\frac{v}{a'} \log\frac{v}{b'}.$$

This is the same form as $Z^{(1)}_{N,W}$. By the same considerations as above we obtain

$$T_3 = \frac{C_W \beta_2(q)}{q} (\log v/q)^{\frac{1}{2}} + O\bigg(\frac{\exp(D_0^{1/4}\log\log D_0)(\log\log v)^3}{q}\bigg),$$

where

$$\beta_2(q) = \frac{\mu^2(q)g_4(q)G_1(q)G_3(q)G_4(q)G_5(q)}{g_2(q)^2} = \frac{q^2(4q^2-3q+1)}{2(q-1)^2(2q^2-2q+1)}.$$

Thus we obtain

$$Z^{(2)}_{N,W} = C_W \sum_{\substack{D_0 < q \le v \\ q \equiv 1 \pmod 4}} \frac{2\beta_1(q) - \beta_2(q)}{q} g_6(q) (\log(v/q))^{\frac{1}{2}} + O\bigg(\exp(D_0^{1/4}\log\log D_0)(\log\log v)^3 \sum_{\substack{D_0 < q \le v \\ q \equiv 1 \pmod 4}} \frac{g_6(q)}{q}\bigg),$$

where C_W is defined as in (B.0.9). Recalling the definition of $g_6(q)$, we see the error term contributes

$$\ll \exp(D_0^{1/4}\log\log D_0)(\log\log v)^3 \log v.$$

Now note that

$$\frac{2\beta_1(q) - \beta_2(q)}{q} g_6(q) = -\frac{(3q-2)(2q+1)\log q}{2(q+1)(2q^2-2q+1)} = -\frac{3\log q}{2q} + O\bigg(\frac{\log q}{q^2}\bigg)$$

This error contributes

$$\ll C_W \sum_{\substack{D_0 < q \le v \\ q \equiv 1 \pmod 4}} \frac{\log q}{q^2} (\log v)^{\frac{1}{2}} \ll C_W (\log v)^{\frac{1}{2}}$$

which is small. We are left with a main term

$$-\frac{3C_W}{2} \sum_{\substack{D_0 < q \le v \\ q \equiv 1 \pmod 4}} \frac{\log q}{q} \bigg(\log\frac{v}{q}\bigg)^{\frac{1}{2}}.$$

By partial summation one can show

$$\sum_{\substack{D_0<q\le v\\ q\equiv 1 \pmod 4}} \frac{\log q}{q}\left(\log\frac{v}{q}\right)^{\frac{1}{2}} = \frac{1}{3}(\log v)^{\frac{3}{2}} + O((\log v)^{\frac{1}{2}}\log D_0),$$

so that

$$Z^{(2)}_{N,W} = -\frac{C_W}{2}(\log v)^{\frac{3}{2}} + O(\exp(D_0^{1/4}\log\log D_0)(\log\log v)^3\log v).$$

This simplifies to the stated result.

□

References

[1] R. C. Baker, M. Munsch, and I. E. Shparlinski. Additive energy and a large sieve inequality for sparse sequences. *Mathematika*, 68(2):362–399, 2022.

[2] W. D. Banks, T. Freiberg, and J. Maynard. On limit points of the sequence of normalised prime gaps. *Proc. Lond. Math. Soc.*, 113(4):515–539, 2016.

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

[4] T. Browning. The polynomial sieve and equal sums of like polynomials. *IMRN.*, 2015(7):1987–2019, 2015.

[5] T. Browning and D. R. Heath-Brown. The density of rational points on non-singular hypersurfaces, I. *Bulletin of the LMS.*, 38(3):401–410, 2006.

[6] H. M. Bui and D. R. Heath-Brown. A note on the fourth moment of Dirichlet L-functions. *Acta Arith.*, 141:335–344, 2010.

[7] C. Chen, B. Kerr, J. Maynard, and I. E. Shparlinski. Metric theory of Weyl sums. *Math. Ann.*, 2022.

[8] H. Davenport. *Multiplicative number theory.* Springer GTM, 3 edition, 2000.

[9] P. Deligne. La conjecture de Weil. *I. Inst. Hautes Etudes Sci. Publ. Math.*, 48:273–307, 1974.

[10] D. A. Goldston, S. W. Graham, J. Pintz, and C. Y. Yıldırım. Small gaps between products of two primes. *Proc. Lond. Math. Soc.*, 98(3):741–774, 2009.

[11] D. A. Goldston, J. Pintz, and C. Y. Yıldırım. Primes in tuples I. *Ann. Math.*, 170(2):819–862, 2009.

[12] D. R. Heath-Brown. The square sieve and consecutive square-free numbers. *Math. Annalen.*, 266:251–259, 1984.

[13] D. R. Heath-Brown. The density of rational points on curves and surfaces. *Ann. Math.*, 155(2):553–598, 2002.

[14] C. Hooley. On the intervals between numbers that are sums of two squares. *Acta Math.*, 127:279–297, 1971.

[15] C. Hooley. On the numbers that are representable as a sum of two cubes. *J. für die Reine und Angew. Math.*, 341:146–173, 1980.

[16] C. Hooley. On another sieve method and the numbers that are the sum of two hth powers. *Proceedings of the LMS.*, 43:73–109, 1981.

[17] C. Hooley. *On exponential sums and certain of their applications*, page 92–122. London Mathematical Society Lecture Note Series. Cambridge University Press, 1982.

[18] C. Hooley. On another sieve method and the numbers that are the sum of two hth powers II. *J. für die Reine und Angew. Math.*, 475:55–76, 1996.

[19] D. Jakobson. Quantum limits on flat tori. *Ann. Math.*, 145(2):235–266, 1997.

[20] O. Marmon. Sums and differences of four kth powers. *Monat. Math.*, 164:55–74, 2011.

[21] J. Maynard. Small gaps between primes. *Ann. Math.*, 181(1):383–413, 2015.

[22] R. Munshi. Density of rational points on cyclic covers of pn. *J. Th´eorie Nombres Bordeaux*, 21:335–341, 2009.

[23] V. A. Plaksin. The distribution of numbers representable as the sum of two squares. *Math. USSR-Izvestiya*, 31(1):171–191, 1988.

[24] D. H. J. Polymath. Variants of the selberg sieve, and bounded intervals containing many primes. *Mathematical Sciences.*, 1(12), 2014.

[25] A. Selberg. *On elementary methods in prime number-theory and their limitations*, page 388–397. London Mathematical Society Lecture Note Series. Springer-Verlag, 1989.

[26] G. Tenenbaum. *Introduction to analytic and probabilistic number theory.* American Mathematical Society Graduate Studies in Mathematics, 3 edition, 2015.

[27] D. I. Tolev. On the remainder term in the circle problem in an arithmetic progression. *Proc. Steklov Inst. Math.*, 276:261–274, 2012.

[28] A. Weil. Sur les courbes algébriques et les variétés que s'en déduisent. *Actualités Sci. Indust.*, 1041, 1948.

[29] Y. Zhang. Bounded gaps between primes. *Ann. Math.*, 179:1121–1174, 2014.