Representation Numbers of Quadratic Forms

Nuno Miguel Arala Santos

Born 13th February 1997 in Porto, Portugal

Master's Thesis Mathematics

Advisor: Prof. Valentin Blomer

Second Advisor: Dr. Edgar Assing

MATHEMATISCHES INSTITUT

MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT DER

RHEINISCHEN FRIEDRICH-WILHELMS-UNIVERSITÄT BONN

Abstract

In his paper [1], Heath-Brown developed a new form of the Hardy-Littlewood Circle Method, and then showed how it could be used to estimate representation numbers of quadratic forms. However, it is not clear from the paper how the error terms obtained depend on the quadratic forms under consideration. After reviewing Heath-Brown's method, we prove estimates along the same lines and make explicit the dependence of the error terms on the quadratic forms, making the result more suitable for certain applications.

Notation

Given a point/vector $x \in \mathbb{R}^n$, we denote by $x_1, \ldots, x_n$ its coordinates.

For us, a smooth function is an infinitely differentiable function. Given such a function w, defined in $\mathbb{R}^n$ and with compact support, we define, for each non-negative integer N,

$$|w|_N = \sum_{i_1 + \cdots + i_n \leq N} \max_{x \in \mathbb{R}^n} \left| \frac{\partial^{i_1 + \cdots + i_n} w(x)}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}} \right|.$$

We use $\mathbb{Q}_p$ and $\mathbb{Z}_p$ to denote the p-adic numbers and the p-adic integers, respectively.

Contents

1 Introduction

The Hardy-Littlewood Circle Method was introduced in the early 20th century, and has since proved to be a tool of fundamental importance in a range of problems in number theory. Perhaps its most famous application is to Waring's problem, which asks whether, for each positive integer k, there is a positive integer s such that every positive integer N can be written as a sum of at most s positive k-th powers. The answer turns out to be affirmative, generalizing, for instance, Lagrange's classical theorem that every positive integer is a sum of four squares. It was in fact in the context of Waring's problem that Hardy and Littlewood originally developed the method.

We sketch the main idea behind the method using Waring's problem as an example, as seems appropriate. For an integer n, define

$$\delta_n = \begin{cases} 1, \text{ if } n = 0 \\ 0, \text{ if } n \neq 0. \end{cases}$$

The Hardy-Littlewood Circle Method is based on the following observation.

Proposition 1.0.1. *For any integer n we have*

$$\delta_n = \int_0^1 e(n\alpha)d\alpha. \tag{1.1}$$

One may now attempt to count representations of a positive integer N as a sum of s non-negative k-th powers as follows. Note that for every such representation, say $N = x_1^k + \cdots + x_s^k$, each x_i lies in the interval $[0, N^{\frac{1}{k}}]$. One therefore has

$$
\begin{aligned}
&\#\{(x_1, \ldots, x_s) \in (\mathbb{Z}_{\geq 0})^s : x_1^k + \cdots + x_s^k = N\} \\
&= \sum_{0 \leq x_i \leq N^{\frac{1}{k}}} \delta_{N - x_1^k - \cdots - x_s^k} \\
&= \sum_{0 \leq x_i \leq N^{\frac{1}{k}}} \int_0^1 e((N - x_1^k - \cdots - x_s^k)\alpha)d\alpha \\
&= \int_0^1 \sum_{0 \leq x_i \leq N^{\frac{1}{k}}} e((N - x_1^k - \cdots - x_s^k)\alpha)d\alpha \\
&= \int_0^1 e(N\alpha) \left(\sum_{0 \leq x \leq N^{\frac{1}{k}}} e(-x^k\alpha) \right)^s d\alpha.
\end{aligned}
$$

Several ingeneous ideas make the estimation of this integral possible. The behaviour of the integrand around some value of the parameter α is essentially determined by how close α is to a rational number with small denominator:

- If α is "close" (in a sense we do not make precise here) to a rational number $\frac{a}{q}$ where the denominator q is much smaller than $N^{\frac{1}{k}}$, then we expect the exponential sum $\sum_{0 \le x \le N^{\frac{1}{k}}} e(-x^k \alpha)$ to be approximately equal to $\sum_{0 \le x \le N^{\frac{1}{k}}} e(-ax^k/q)$. However the summand is now periodic modulo q, and hence this sum consists essentially of $\sim \frac{N^{\frac{1}{k}}}{q}$ copies of the sum $\sum_{0 \le x < q} e(-ax^k/q)$. We conclude that

$$\sum_{0 \le x \le N^{\frac{1}{k}}} e(-x^k \alpha) \sim \frac{N^{\frac{1}{k}}}{q} \sum_{0 \le x < q} e\left(-\frac{ax^k}{q}\right).$$

   Sums like the one on the right hand side are well understood.

- Otherwise, if α is "highly irrational", we expect the values of $-x^k \alpha \pmod 1$ to be randomly distributed along $\mathbb{R}/\mathbb{Z}$, and hence we expect a lot of cancelation to occur in the sum $\sum_{0 \le x \le N^{\frac{1}{k}}} e(-x^k \alpha)$, so it should be small (the quasi-periodicity prevented this from happening in the first case).

We call the regions of the first type the *major arcs*, and those of the second type the *minor arcs*. At least when s is large compared to k, the bulk of the integral comes from the contribution of the major arcs. The estimation of the error term coming from the minor arcs is usually the most delicate part of the argument. Nevertheless (when s is large compared to k) it is possible, using these ideas, to estimate the above integral to a good degree of accuracy, and to conclude that, for s large enough, the number $\#\{(x_1, \ldots, x_s) \in (\mathbb{Z}_{\ge 0})^s : x_1^k + \cdots + x_s^k = N\}$ is always strictly positive.

Let us say some words about the estimate that the circle method gives for this number, since it displays a phenomenon which will show up again in our work. The main term (for s large enough in terms of k) turns out to be

$$\Sigma_{k,s}(N) N^{s/k-1}, \quad \text{where} \quad \Sigma_{k,s}(N) = \beta_\infty \prod_{p \text{ prime}} \beta_p(N). \tag{1.2}$$

Here β_∞ is the surface area of the set $\{(x_1, \ldots, x_s) : x_1^k + \cdots + x_s^k = 1\}$, and

$$\beta_p(N) = \lim_{\nu \to \infty} p^{-\nu(s-1)} \#\{(x_1, \ldots, x_s) \in (\mathbb{Z}/p^\nu\mathbb{Z})^s : x_1^k + \cdots + x_s^k \equiv N \pmod{p^\nu}\}.$$

So the number of ways N can be written as a sum of s positive k-th powers has order of magnitude $N^{s/k-1}$, with fluctuations depending on the availability of solutions to $x_1^k + \cdots + x_s^k = N$ over $\mathbb{R}$ and over the rings $\mathbb{Z}_p$ of p-adic integers.

Several variants of the Hardy-Littlewood method have been developed over time. These are based on different formulas for δ_n of varied analytic flavour, such as (1.1). Of particular interest to us is the method Heath-Brown develops in [1]. This is based on the fact (which has essentially appeared in [2]) that there exist an infinitely differentiable function h defined on $\mathbb{R}_{>0} \times \mathbb{R}$ and a collection of constants (c_Q) indexed by the reals greater than 1 such that, for any $Q > 1$, c_Q is close to 1 and we have

$$\delta_n = c_Q Q^{-2} \sum_{q=1}^{\infty} \sideset{}{^*}\sum_{a \pmod q} e\left(\frac{an}{q}\right) h\left(\frac{q}{Q}, \frac{n}{Q^2}\right). \tag{1.3}$$

We will see how to construct such a function h in §2.1.

This identity can be used to count solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ of equations of the form $F(x_1, \ldots, x_n) = 0$, where m is an integer and F is a homogeneous polynomial with integer coefficients. In this thesis we shall focus on the case $F = F^{(0)} - m$, where $F^{(0)}$ is a quadratic form with integer coefficients and m is an nonzero integer; except for Chapter 2, we assume this to be the case from now on. We also define $G(x)$ to be $F^{(0)}(x) - 1$.

There is however an important difference between the counting procedure adopted by Heath-Brown and the one we sketched before. Heath-Brown's method works best when one attempts to count solutions *weighted by a smooth weight function*. The reason is that, in order to pass from (1.3) to a formula for the number of solutions to $F(x) = 0$, one would like to use the Poisson summation formula, so some smoothness condition is required of our summands. So even if one's ultimate goal is to compute the *unweighted* number of solutions, one should first study the weighted version of the problem and then choose a weight that approximates the characteristic function of the subset of $\mathbb{R}^n$ where one is looking for solutions.

Thus let w be a compactly supported smooth function defined on $\mathbb{R}^n$, and let

$$N^{(0)}(F, w) = \sum_{\substack{x \in \mathbb{Z}^n \\ F(x) = 0}} w\left(\frac{x}{\sqrt{m}}\right)$$

be the number of solutions to $F(x) = 0$ weighted by the smooth weight whose value at x is $w(m^{-1/2}x)$. The use of $w(m^{-1/2}x)$ instead of the perhaps more natural $w(x)$ corresponds essentially to normalizing the equation $F^{(0)}(x) = m$ by rewriting it as $F^{(0)}(x/\sqrt{m}) = 1$; so we will usually pick smooth weights w supported around the set $\{x \in \mathbb{R}^n : F^{(0)}(x) = 1\}$, which does not depend on m. We rewrite the right hand side above as $\sum_{x \in \mathbb{Z}^n} w(x)\delta_{F(x)}$ and, using (1.3) and Poisson Summation (the details will be shown in §2.3), we arrive at

$$N(F, w) = c_Q Q^{-2} \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c)$$

where

$$S_q(c) = \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, q)} \sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{aF(b) + c \cdot b}{q}\right)$$

and

$$I_q(c) = \int_{\mathbb{R}^n} w\left(\frac{x}{\sqrt{m}}\right) h\left(\frac{q}{Q}, \frac{F(x)}{Q^2}\right) e\left(\frac{-c \cdot x}{q}\right) dx.$$

In the course of the argument we will choose $Q = \sqrt{m}$. Now a lot of the subsequent work consists of studying and estimating the exponential sums $S_q(c)$ and the exponential integrals $I_q(c)$ with care. Using this approach, Heath-Brown arrives in [1] at the following result.

Theorem 1.0.2. *Let $n \geq 4$ be an integer, let $F^{(0)}$ be a positive-definite quadratic form in n variables and let m be a positive integer. Then we have*

$$\#\{x \in \mathbb{Z}^n : F^{(0)}(x) = m\} = \sigma_\infty(F^{(0)}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1} + O_{F^{(0)},\varepsilon}\left(m^{\frac{n-1}{4}+\varepsilon}\right),$$

where $\sigma_\infty(F^{(0)})$ is the singular integral, *defined by*

$$\sigma_\infty(F^{(0)}) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} 1 dx$$

and $\sigma_p(F^{(0)}, m)$ *is the p-adic density of solutions to* $F^{(0)}(x) = m$, *given by*

$$\sigma_p(F^{(0)}, m) = \lim_{\nu \to \infty} p^{-\nu(n-1)} \#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \pmod{p^\nu}\}.$$

Moreover, if $n \geq 5$ *and the equation* $F^{(0)}(x) = m$ *has a solution in the ring of p-adic integers* $\mathbb{Z}_p$ *for every prime* p, *then we have*

$$1 \ll_{F^{(0)}} \prod_{p \ prime} \sigma_p(F^{(0)}, m) \ll_{F^{(0)}} 1.$$

One should note the similarity between the output of Theorem 1.0.2 and (1.2). They are both quantitative versions of a *local-global principle*. Such situations are familiar in quadratic form theory due to the celebrated Hasse-Minkowski theorem which states that a quadratic form has a non-trivial zero over $\mathbb{Q}$ if and only if it has a non-trivial zero over $\mathbb{R}$ and over every $\mathbb{Q}_p$. For another example of a quantitative version of a local-global principle arising in Analytic Number Theory, we refer to Section 11.2 of [3], on Siegel's mass formula.

For $n \geq 5$, Theorem 1.0.2 implies that the order of magnitude of $\#\{x \in \mathbb{Z}^n : F^{(0)}(x) = m\}$, as m ranges over the positive integers for which $F^{(0)}(x) = m$ is solvable in $\mathbb{Z}$, is $m^{n/2-1}$. We remark here that this is false for $n = 4$. In that case, we can take, for example,

$$F^{(0)}(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

and then, by a celebrated result of Jacobi,

$$\#\{x \in \mathbb{Z}^4 : F^{(0)}(x) = m\} = 8 \sum_{4 \nmid d \mid m} d.$$

This decays drastically when m has few odd divisors, and in particular the above identity shows that 2^k can be written as a sum of four squares in exactly 24 ways, for $k \geq 1$ (though this can also of course be shown elementarily).

The error term appearing in the statement of Theorem 1.0.2 is quite satisfactory. It has however the disadvantage that its dependence on the underlying form $F^{(0)}$ is not specified. The purpose of this work is to give another version of Theorem 1.0.2 where the error term is given uniformly in $F^{(0)}$. For simplicity, we will restrict to the case where $F^{(0)}$ is a diagonal form, given by

$$F^{(0)}(x) = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$$

for some positive integers $\lambda_1, \ldots, \lambda_n$. More specifically, we will prove the following:

Theorem 1.0.3. *Let* $n \geq 4$ *be an integer, let* $F^{(0)}$ *be a positive-definite quadratic form in* n *variables and let* m *be a positive integer. Then we have*

$$\#\{x \in \mathbb{Z}^n : F^{(0)}(x) = m\} = \sigma_\infty(F^{(0)}) \prod_{p \ prime} \sigma_p(F^{(0)}, m) m^{\frac{m}{2}-1} + O_\varepsilon \left(\Delta^{\frac{n+3}{2}} |\lambda|^{1+100n^2/\varepsilon} m^{\frac{n-1}{4}+\varepsilon} \right),$$

where $\Delta = 2\lambda_1 \cdots \lambda_n$, *and the singular integral* $\sigma_\infty(F^{(0)})$ *and the p-adic densities* $\sigma_p(F^{(0)}, m)$ *are defined as in the statement of Theorem 1.0.2.*

In Chapter 2 we develop in detail Heath-Brown's variant of the circle method and use it to obtain an expression for the number of solutions of a polynomial equation in terms of some exponential sums and exponential integrals (here the work done in [1] is mostly left unchanged). In Chapter 3 we study these exponential sums and exponential integrals in detail in the context of quadratic forms.

2 The Method

In this chapter we explain in detail the ideas behind (1.3), and show how it can be used to count weighted solutions to polynomial equations in $\mathbb{Z}^n$.

§2.1 The delta symbol

In order to construct a function h such that (1.3) holds, we shall need a function $\omega \in C^\infty(\mathbb{R})$ taking only non-negative real values and such that $\omega(x) > 0$ if and only if $x \in (1/2, 1)$, with

$$\int_{-\infty}^{\infty} \omega(x)dx = 1.$$

That such a function exists is standard. It can, however, be explicitly constructed as follows: defining

$$w_0(x) = \begin{cases} \exp\left(\frac{-1}{1-x^2}\right) & \text{if } |x| < 1 \\ 0 \text{ if } |x| \geq 1 \end{cases}$$

and setting $c_0 = \int_{-\infty}^{\infty} w_0(x)dx$, we may take

$$\omega(x) = \frac{4}{c_0} w_0(4x - 3).$$

We emphasize nevertheless that everything that follows works for any choice of ω with the stated properties.

Define now $h : \mathbb{R}_{>0} \times \mathbb{R} \to \mathbb{R}$ by

$$h(x, y) = \sum_{j=1}^{\infty} \frac{1}{xj}\left(\omega(xj) - \omega\left(\frac{|y|}{xj}\right)\right).$$

The main claim here is that (1.3) holds with this choice of the function h. We will prove in Lemma 2.2.2 that h is smooth.

Lemma 2.1.1. *For each real number $Q > 1$ there exists a constant c_Q, satisfying $c_Q = 1 + O_N(Q^{-N})$ for every $N > 0$, such that the equality*

$$\delta_n = c_Q Q^{-2} \sum_{q=1}^{\infty} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\ q)} e\left(\frac{an}{q}\right) h\left(\frac{q}{Q}, \frac{n}{Q^2}\right)$$

holds for every integer n.

Proof. Define c_Q by

$$c_Q = Q\left(\sum_{l=1}^{\infty} \omega\left(\frac{l}{Q}\right)\right)^{-1}.$$

The denominator is nonzero because ω is non-negative everywhere, and moreover the summand $\omega((\lceil Q \rceil - 1)/Q)$ is strictly positive since $1/2 < (\lceil Q \rceil - 1)/Q < 1$ for every $Q > 1$.

We begin by proving that $c_Q = 1 + O_N(Q^{-N})$ for every $N > 0$ (we may, of course, assume N is an integer greater than 1, which we do now). For this we apply the Poisson summation formula to the function $\omega_Q(x) = \omega(x/Q)$. This yields

$$\sum_{l \in \mathbb{Z}} \omega_Q(l) = \sum_{k \in \mathbb{Z}} \widehat{\omega_Q}(k)$$

which, using the fact that ω is supported on the positive real axis and unraveling the definition of the Fourier transform, yields

$$\sum_{l=1}^{\infty} \omega\left(\frac{l}{Q}\right) = \sum_{k \in \mathbb{Z}} \int_{-\infty}^{\infty} \omega\left(\frac{x}{Q}\right) e(-kx) dx. \tag{2.1}$$

The summand corresponding to $k = 0$ is

$$\int_{-\infty}^{\infty} \omega\left(\frac{x}{Q}\right) dx = Q \int_{-\infty}^{\infty} \omega(x) = 1.$$

For $k \neq 0$, we integrate by parts N times, showing that

$$\int_{-\infty}^{\infty} \omega\left(\frac{x}{Q}\right) e(-kx) dx = \frac{1}{(kQ)^N} \int_{-\infty}^{\infty} \omega^{(N)}\left(\frac{x}{Q}\right) e(-kx) dx$$

and hence

$$\left| \int_{-\infty}^{\infty} \omega\left(\frac{x}{Q}\right) e(-kx) dx \right| \leq \frac{1}{|k|^N Q^N} \int_{-\infty}^{\infty} \left| \omega^{(N)}\left(\frac{x}{Q}\right) e(-kx) \right| dx$$

$$= \frac{1}{|k|^N Q^N} \int_{-\infty}^{\infty} \left| \omega^{(N)}\left(\frac{x}{Q}\right) \right| dx$$

$$= \frac{Q}{|k|^N Q^N} \int_{-\infty}^{\infty} |\omega^{(N)}(x)| dx = O_N\left(\frac{Q}{|k|^N Q^N}\right).$$

It follows from (2.1) that

$$\sum_{l=1}^{\infty} \omega\left(\frac{l}{Q}\right) = Q + \sum_{k \neq 0} O_N\left(\frac{Q}{|k|^N Q^N}\right) = Q + O_N\left(Q^{1-N} \sum_{k \neq 0} \frac{1}{|k|^N}\right) = Q + O_N(Q^{1-N})$$

in view of the fact that $\sum_{k \neq 0} 1/|k|^N$ converges. Now by the definition of c_Q we have

$$c_Q = Q(Q + O_N(Q^{1-N}))^{-1} = 1 + O_N(Q^{-N})$$

as desired.

We prove now the desired formula for δ_n. We consider the sum

$$\sum_{l | n} \left(\omega\left(\frac{l}{Q}\right) - \omega\left(\frac{|n|/l}{Q}\right) \right)$$

where l ranges over the *positive* divisors of the integer n.

- If $n \neq 0$, then the values taken by $|n|/l$ as l ranges over the positive divisors of n are again the positive divisors of n. Therefore the above sum equals 0.

- If $n = 0$, the above sum equals

$$\sum_{l=1}^{\infty} \omega\left(\frac{l}{Q}\right) = c_Q^{-1} Q$$

by the definition of c_Q.

We obtain

$$\delta_n = c_Q Q^{-1} \sum_{l \mid n} \left(\omega\left(\frac{l}{Q}\right) - \omega\left(\frac{|n|/l}{Q}\right) \right).$$

In order to obtain a sum where l ranges over all positive integers, we use the fact that

$$\frac{1}{l} \sum_{b \,(\mathrm{mod}\, l)} e\left(\frac{bn}{l}\right) = \begin{cases} 1 \text{ if } l \mid n \\ 0 \text{ otherwise} \end{cases}$$

and hence

$$\delta_n = c_Q Q^{-1} \sum_{l=1}^{\infty} \frac{1}{l} \sum_{b \,(\mathrm{mod}\, l)} e\left(\frac{bn}{l}\right) \left(\omega\left(\frac{l}{Q}\right) - \omega\left(\frac{|n|/l}{Q}\right) \right).$$

We now observe that for every positive integer l and for every $b \,(\mathrm{mod}\, l)$ there exist unique integers j and q and a unique $a \,(\mathrm{mod}\, q)$, with $(a,q) = 1$, such that $l = qj$ and $b = aj$ (this amounts to writing the fraction b/l in lowest terms as a/q). Since in this setting we have $e(bn/l) = e(an/q)$, we obtain

$$\delta_n = c_Q Q^{-1} \sum_{q=1}^{\infty} \sum_{a \,(\mathrm{mod}\, q)}^{*} e\left(\frac{an}{q}\right) \sum_{j=1}^{\infty} \frac{1}{qj} \left(\omega\left(\frac{qj}{Q}\right) - \omega\left(\frac{|n|/qj}{Q}\right) \right)$$

$$= c_Q Q^{-2} \sum_{q=1}^{\infty} \sum_{a \,(\mathrm{mod}\, q)}^{*} e\left(\frac{an}{q}\right) \sum_{j=1}^{\infty} \frac{Q}{qj} \left(\omega\left(\frac{qj}{Q}\right) - \omega\left(\frac{|n|/qj}{Q}\right) \right).$$

But by definition of h it is clear that

$$\sum_{j=1}^{\infty} \frac{Q}{qj} \left(\omega\left(\frac{qj}{Q}\right) - \omega\left(\frac{|n|/qj}{Q}\right) \right) = h\left(\frac{q}{Q}, \frac{n}{Q^2}\right),$$

establishing the Lemma. $\qquad \square$

§2.2 Properties of the function h

In this section we establish key properties of the function h, and in particular we show that it is smooth. There are two main further results in this section: Lemma 2.2.8, which establishes a crucial estimate for the derivatives of h, and Lemma 2.2.12, which shows that, for small values of x and for a resanonable function f, the integral $\int_{\mathbb{R}} f(y) h(x, y) dy$ is close to $f(0)$. We begin with a simple observation regarding the support of h.

Lemma 2.2.1. *Whenever $h(x, y) \neq 0$ we have $x < 1$ or $|y| \geq \frac{x}{2}$.*

Proof. Suppose that $x \geq 1$ and $|y| < \frac{x}{2}$. Then $xj \geq 1$ for every $j \geq 1$, and hence $\omega(xj) = 0$. Similarly, $|y|/xj \leq \frac{1}{2}$ for every $j \geq 1$, hence $\omega(|y|/xj) = 0$. It follows from the definition of h that $h(x, y) = 0$. $\qquad \square$

Our next proposition shows the promised smoothness of h.

Lemma 2.2.2. *The function h is smooth, and moreover its derivatives can be computed by termwise differentiation.*

Proof. The key observation is that, despite the fact that f is defined by an infinite sum, this sum is *locally* finite. Hence, locally, h is given by a finite sum of smooth functions, and therefore it is smooth as well.

We formalize this as follows. Take any $(x_0, y_0) \in \mathbb{R}_{>0} \times \mathbb{R}$ and consider the open set

$$U = \left\{ (x, y) \in \mathbb{R}_{>0} \times \mathbb{R} : |x - x_0| < \frac{x_0}{2} \text{ and } |y - y_0| < 1 \right\}.$$

Then U is an open neighborhood of (x_0, y_0). Moreover,

- If $(x, y) \in U$, then $x \geq \frac{x_0}{2}$, hence for $j \geq \frac{2}{x_0}$ we have $xj \geq 1$ and $\omega(xj) = 0$.

- If $(x, y) \in U$, then $|y| \leq |y_0| + 1$, and using again the fact that $x \geq \frac{x_0}{2}$ we get

$$\frac{|y|}{x} \leq \frac{2(|y_0| + 1)}{x_0}.$$

Therefore if $j \geq 4(|y_0| + 1)/x_0$ we have $|y|/xj \leq \frac{1}{2}$, and $\omega(|y|/xj) = 0$.

It follows from the definition of h that

$$h(x, y) = \sum_{j < 4(|y_0|+1)/x_0} \frac{1}{xj} \left(\omega(xj) - \omega\left(\frac{|y|}{xj} \right) \right)$$

for $(x, y) \in U$. Since the above sum is a finite sum of smooth functions (note that $\omega(|y|/xj)$ is smooth since ω vanishes on a neighborhood of 0), it follows that h is smooth in a neighborhood of (x_0, y_0), and its derivatives can be computed by termwise differentiation there. Since smoothness is a local property and this holds for every $(x_0, y_0) \in \mathbb{R}_{>0} \times \mathbb{R}$, it follows that h is smooth and its derivatives can be computed by termwise differentiation. $\square$

For some of our next results we need a preliminary observation. From the classical fact that

$$\sum_{0 < j \leq x} \frac{1}{j} = \log(x) + \gamma + O\left(\frac{1}{x} \right)$$

it follows that

$$\sum_{a < j \leq 2a} \frac{1}{j} = \sum_{0 < j \leq 2a} \frac{1}{j} - \sum_{0 < j \leq a} \frac{1}{j} = \log(2) + O\left(\frac{1}{x} \right) = O(1). \tag{2.2}$$

Proposition 2.2.3. *We have $h(x, y) \ll x^{-1}$.*

Proof. We write

$$h(x, y) = x^{-1} \left(\sum_{j \geq 1} \frac{1}{j} \omega(xj) - \sum_{j \geq 1} \frac{1}{j} \omega\left(\frac{|y|}{xj} \right) \right)$$

and observe that $\omega(xj)$ is nonzero only when $1/2 < xj < 1$, i.e., when $1/2x < j < 1/x$; similarly $\omega(|y|/xj)$ is nonzero only when $1/2 < |y|/xj < 1$, i.e., when $|y|/x < j < 2|y|/x$. Since $\omega \ll 1$, we obtain

$$h(x, y) \ll x^{-1} \left(\sum_{1/2x < j < 1/x} \frac{1}{j} + \sum_{|y|/x < j < 2|y|/x} \frac{1}{j} \right) \ll x^{-1}$$

by (2.2). $\square$

Proposition 2.2.4. *Set*

$$h_1(x, y) = \sum_{j=1}^{\infty} \frac{1}{xj} \omega(xj).$$

Then we have

$$\frac{\partial^m h_1(x, y)}{\partial x^m} \ll_m x^{-m-1}.$$

Proof. We begin by observing that, for any integer $t \geq 0$, the function

$$x \mapsto x^t \omega^{(t)}(x)$$

is continuous and compactly supported, hence bounded. It follows that $x^t \omega^{(t)}(x) \ll 1$. Now we compute

$$\frac{\partial^t \omega(xj)}{\partial x^t} = j^t \omega^{(t)}(xj) = j^t O_t \left(\frac{1}{(xj)^t} \right) = O_t(x^{-t}).$$

It follows, using Leibniz' formula, that

$$\frac{\partial^m}{\partial x^m}(x^{-1}\omega(xj)) = \sum_{k=0}^{m} \binom{m}{k} \frac{\partial^{m-k}}{\partial x^{m-k}}(x^{-1}) \frac{\partial^k}{\partial x^k}(\omega(xj))$$

$$\ll_m \sum_{k=0}^{m} x^{-m+k-1} \frac{\partial^k}{\partial x^k}(\omega(xj))$$

$$\ll_m \sum_{k=0}^{m} x^{-m+k-1} x^{-k} \ll_m x^{-m-1}.$$

We now have

$$\frac{\partial^m}{\partial x^m} h_1(x, y) = \sum_{j \geq 1} \frac{1}{j} \frac{\partial^m}{\partial x^m}(x^{-1}\omega(xj))$$

where the summands are only nonzero when $1/2 < xj < 1$, i.e, when $1/2x < j < 1/x$. Using the previous estimate we obtain

$$\frac{\partial^m}{\partial x^m} h_1(x, y) \ll_m \sum_{1/2x < j < 1/x} \frac{1}{j} x^{-m-1} \ll_m x^{-m-1}$$

by (2.2). $\qquad\square$

Proposition 2.2.5. *We have*

$$\frac{\partial^{m+n} h(x, y)}{\partial x^m \partial y^n} \ll_{m,n} x^{-m-1}|y|^{-n}$$

for every non-negative integers m and n.

Proof. Setting

$$h_2(x, y) = \sum_{j \geq 1} \frac{1}{xj} \omega \left(\frac{|y|}{xj} \right)$$

so that $h = h_1 - h_2$, we prove that both $\partial^{m+n} h_1(x, y)/\partial x^m \partial y^n$ and $\partial^{m+n} h_2(x, y)/\partial x^m \partial y^n$ are bounded by the expression above.

For the former, we note that $h_1(x,y)$ does not depend on y. Hence $\partial^{m+n}h_1(x,y)/\partial x^m \partial y^n$ can only be nonzero if $n = 0$. In this case we have

$$\frac{\partial^{m+n}h_1(x,y)}{\partial x^m \partial y^n} \ll_m x^{-m-1}$$

by Proposition 2.2.4, which is precisely the desired bound.

We proceed to bounding $\partial^{m+n}h_2(x,y)/\partial x^m \partial y^n$. Since h_2 is even with respect to the second variable and vanishes when the $|y| < x/2$, we may assume without loss of generality that $y > 0$. We claim that there exist constants $c_{m,n,t}$ $(0 \le t \le m)$ such that

$$\frac{\partial^{m+n}}{\partial x^m \partial y^n}\left(x^{-1}\omega\left(\frac{y}{xj}\right)\right) = x^{-m-1}y^{-n}\sum_{t=0}^{m} c_{m,n,t}\left(\frac{y}{xj}\right)^{n+t}\omega^{(n+t)}\left(\frac{y}{xj}\right).$$

The proof is a straightforward induction on m: if $m = 0$, it is clear that

$$\frac{\partial^{n}}{\partial y^n}\left(x^{-1}\omega\left(\frac{y}{xj}\right)\right) = x^{-1}(xj)^{-n}\omega^{(n)}\left(\frac{y}{xj}\right) = x^{-1}y^{-n}\left(\frac{y}{xj}\right)^{n}\omega^{(n)}\left(\frac{y}{xj}\right)$$

as desired. For the induction step, we easily compute

$$\frac{\partial^{m+1+n}}{\partial x^{m+1} \partial y^n}\left(x^{-1}\omega\left(\frac{y}{xj}\right)\right) = \frac{\partial}{\partial x}\left(x^{-m-1}y^{-n}\sum_{t=0}^{m} c_{m,n,t}\left(\frac{y}{xj}\right)^{n+t}\omega^{(n+t)}\left(\frac{y}{xj}\right)\right) =$$

$$x^{-m-2}y^{-n}\sum_{t=0}^{m}\left((-m-1-n-t)c_{m,n,t}\left(\frac{y}{xj}\right)^{n+t}\omega^{(n+t)}\left(\frac{y}{xj}\right) - c_{m,n,t}\left(\frac{y}{xj}\right)^{n+t+1}\omega^{(n+t+1)}\left(\frac{y}{xj}\right)\right),$$

which has the desired form.

Using $(y/xj)^{n+t}\omega^{(n+t)}(y/xj) \ll_{t,n} 1$, it follows from the Claim that

$$\frac{\partial^{m+n}}{\partial x^m \partial y^n}\left(x^{-1}\omega\left(\frac{y}{xj}\right)\right) \ll_{m,n} x^{-m-1}y^{-n}.$$

We now have

$$\frac{\partial^{m+n}h_2(x,y)}{\partial x^m \partial y^n} = \sum_{j \ge 1}\frac{1}{j}\frac{\partial^{m+n}}{\partial x^m \partial y^n}\left(x^{-1}\omega\left(\frac{y}{xj}\right)\right)$$

but the summand can only be nonzero for $1/2 < y/xj < 1$, i.e., for $y/x < j < 2y/x$. We conclude that

$$\frac{\partial^{m+n}h_2(x,y)}{\partial x^m \partial y^n} \ll_{m,n} \sum_{y/x<j<2y/x}\frac{1}{j}x^{-m-1}y^{-n} \ll_{m,n} x^{-m-1}y^{-n}$$

in light of (2.2). $\square$

In order to prove our next estimate we shall introduce an integral representation for $h(x,y)$. The idea is to use Euler-Maclaurin summation to approximate the sums $h_1(x,y)$ and $h_2(x,y)$ by the corresponding integrals. These integrals turn out to be equal, hence they cancel and we are only left with the error terms given by the Euler-Maclaurin summation formula.

We recall the statement of the Euler-Maclaurin summation formula:

Fact 2.2.6 (Euler-Maclaurin summation)**.** Let $a < b$ be real numbers and $f \in C^\infty([a, b])$ a smooth function. For any $N \geq 2$ we have

$$\sum_{a < k \leq b} f(k) = \int_a^b f(x)dx + \left(a - \lfloor a \rfloor - \frac{1}{2}\right)f(a) - \left(b - \lfloor b \rfloor - \frac{1}{2}\right)f(b)$$

$$+ \sum_{j=2}^{N} \frac{(-1)^j}{j!}\left(P_j(b)f^{(j-1)}(b) - P_j(a)f^{(j-1)}(a)\right)$$

$$- \frac{(-1)^N}{N!}\int_a^b P_N(x)f^{(N)}(x)dx.$$

Here $P_n(x) = B_n(\{x\})$, where the polynomials B_n are the *Bernoulli polynomials* defined by the formal equality

$$\frac{te^{tx}}{e^t - 1} = \sum_{k \geq 0} \frac{B_k(x)}{k!}t^k.$$

Proposition 2.2.7. *For any $K, N \geq 2$, we have the identity*

$$h(x, y) = -\frac{(-1)^N}{N!}x^{N-1}\int_{1/2}^1 P_N\left(\frac{u}{x}\right)w^{(N)}(u)du$$

$$+ \frac{(-1)^K}{K!}\frac{x^{K-1}}{|y|^K}\int_1^2 P_K\left(\frac{u|y|}{x}\right)\frac{d^K}{du^K}\left(\frac{w(u^{-1})}{u^2}\right)du,$$

where $w(u) = \omega(u)/u$.

Proof. We note that

$$h_1(x, y) = \sum_{1/2x < j \leq 1/x} \frac{\omega(xj)}{xj}$$

since $\omega(xj)$ can only be nonzero when $1/2 < xj < 1$. Hence the Euler-Maclaurin summation formula of Fact 2.2.6 yields

$$h_1(x, y) = \int_{1/2x}^{1/x} \frac{\omega(xt)}{xt}dt - \frac{(-1)^N}{N!}\int_{1/2x}^{1/x} P_N(t)\frac{\partial^N}{\partial t^N}\left(\frac{\omega(xt)}{xt}\right)dt,$$

since all derivatives of $\omega(xt)/xt$ vanish at $t = 1/2x$ and $t = 1/x$. Making the variable change $t = u/x$ on both integrals, we obtain

$$h_1(x, y) = \frac{1}{x}\int_{1/2}^1 w(u)du - \frac{(-1)^N}{N!}x^{N-1}\int_{1/2}^1 P_N\left(\frac{u}{x}\right)w^{(N)}(u)du. \tag{2.3}$$

Similarly we have

$$h_2(x, y) = \sum_{|y|/x < j \leq 2|y|/x} \frac{\omega(|y|/xj)}{xj}$$

and hence the Euler-Maclaurin summation formula yields

$$h_2(x, y) = \int_{|y|/x}^{2|y|/x} \frac{\omega(|y|/xt)}{xt}dt - \frac{(-1)^K}{K!}\int_{|y|/x}^{2|y|/x} P_K(t)\frac{\partial^K}{\partial t^K}\left((xt)^{-1}\omega\left(\frac{|y|}{xt}\right)\right)dt.$$

We now perform the variable changes $t = |y|/xu$ on the first summand and $t = u|y|/x$ on the second summand, obtaining

$$h_2(x, y) = \frac{1}{x} \int_{1/2}^1 w(u) du - \frac{(-1)^K}{K!} \frac{x^{K-1}}{|y|^K} \int_1^2 P_K\left(\frac{u|y|}{x}\right) \frac{d^K}{du^K}\left(\frac{w(u^{-1})}{u^2}\right) du. \qquad (2.4)$$

Subtracting (2.4) from (2.3) yields the proposition. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

We are now in a position to state and prove our main estimate for the derivatives of h. This will be crucial for the estimation of the exponential integrals we will encounter later.

Lemma 2.2.8. *We have*

$$\frac{\partial^{m+n} h(x,y)}{\partial x^m \partial y^n} \ll_{N,m,n} x^{-1-m-n}\left(x^N + \min\left\{1, \left(\frac{x}{|y|}\right)^N\right\}\right)$$

for every non-negative integers m, n and N. Moreover, if $n \neq 0$, the same holds without the summand x^N on the right hand side.

Proof. We split the proof into three cases. The first two cases are easily covered by previous work. The third case is where the integral representation of Proposition 2.2.7 comes in.

Case 1: $x > |y|$.
    If $x \geq 1$ then the result is obvious if $|y| \leq x/2$, since in that case all derivatives of h vanish at (x,y) by Proposition 2.2.1. If $|y| > x/2$ we have by Proposition 2.2.5

$$\frac{\partial^{m+n} h(x,y)}{\partial x^m \partial y^n} \ll_{m,n} x^{-m-1}|y|^{-n} \leq x^{-m-1}\left(\frac{x}{2}\right)^{-n} \ll_{m,n} x^{-m-1-n}.$$

This implies the proposition in this case.
    If $x < 1$ then the previous argument works as well provided that $|y| > x/2$; the only difference is that now we have to address the case $|y| \leq x/2$ as well. If this happens, then $h(x,y) = h_1(x,y)$ since $h_2(x,y)$ vanishes. Since $h_1(x,y)$ only depends on x, the derivative we want to estimate vanishes if $n \neq 0$. Therefore it suffices to consider the case $n = 0$. Proposition 2.2.5 yields

$$\frac{\partial^m h(x,y)}{\partial x^m} \ll_m x^{-m-1}$$

and we are again done.

Case 2: $n = 0$ and $x \geq 1$.
    Then by Proposition 2.2.5 we have

$$\frac{\partial^m h(x,y)}{\partial x^m} \ll_m x^{-m-1} \leq x^{-m-1+N}$$

implying the proposition again.

Case 3: $x \leq |y|$, and $x < 1$ if $n = 0$.
    To simplify notation, assume without loss of generality that $y > 0$. We first claim that there exist constants $c_{k,l,j}$, for every $k, l \geq 0$ and $l \leq j \leq k + l$, such that the identity

$$\frac{\partial^{k+l} P_M(uy/x)}{\partial x^k \partial y^l} = x^{-k} y^{-l} \sum_{j=l}^{k+l} c_{k,l,j} \left(\frac{uy}{x}\right)^j P_M^{(j)}\left(\frac{uy}{x}\right) \qquad (2.5)$$

holds. We use induction on k. For $k = 0$, we immediately see that

$$\frac{\partial^l P_M(uy/x)}{\partial y^l} = \left(\frac{u}{x}\right)^l P_M^{(l)}\left(\frac{uy}{x}\right) = y^{-l}\left(\frac{uy}{x}\right)^l P_M^{(l)}\left(\frac{uy}{x}\right)$$

which has the desired form. Assuming now the statement holds for a given k, we compute

$$\frac{\partial^{k+1+l}}{\partial x^{k+1}\partial y^l} = \frac{\partial}{\partial x}\left(x^{-k}y^{-l}\sum_{j=l}^{k+l} c_{k,l,j}\left(\frac{uy}{x}\right)^j P_M^{(j)}\left(\frac{uy}{x}\right)\right)$$

$$= x^{-k-1}y^{-l}\sum_{j=l}^{k+l}\left((-k-j)c_{k,l,j}\left(\frac{uy}{x}\right)^j P_M^{(j)}\left(\frac{uy}{x}\right) - c_{k,l,j}\left(\frac{uy}{x}\right)^{j+1} P_M^{(j+1)}\left(\frac{uy}{x}\right)\right),$$

which again has the desired form.

We note that, specializing $y = 1$ and $l = 0$ in (2.5), we obtain the identity

$$\frac{\partial^k P_M(u/x)}{\partial x^k} = x^{-k}\sum_{j=0}^{k} c_{k,j}\left(\frac{u}{x}\right)^j P_M^{(j)}\left(\frac{u}{x}\right) \tag{2.6}$$

with $c_{k,j} = c_{k,0,j}$. We now compute the derivatives of h using Proposition 2.2.7, setting $K = N = M$ there. The first summand in Proposition 2.2.7 only contributes when $n = 0$, in which case[1] its m-th derivative contributes

$$\ll_m \sum_{k=0}^{m}\frac{\partial^{m-k}x^{M-1}}{\partial x^{m-k}}\int_{1/2}^{1}\frac{\partial^k P_M(u/x)}{\partial x^k}w^{(M)}(u)\,du$$

$$\ll_m \sum_{k=0}^{m} x^{M-1-m+k}\int_{1/2}^{1}\left(x^{-k}\sum_{j=0}^{k} c_{k,j}\left(\frac{u}{x}\right)^j P_M^{(j)}\left(\frac{u}{x}\right)\right)w^{(M)}(u)\,du$$

$$= \sum_{j=0}^{m} x^{M-1-m+j}\left(\sum_{k=j}^{m} c_{k,j}\right)\int_{1/2}^{1} u^j P_M^{(j)}\left(\frac{u}{x}\right)w^{(M)}(u)\,du$$

$$\ll_{M,m} \sum_{j=0}^{m} x^{M-1-m+j} \ll_{M,m} x^{M-1-m}(1 + x^{-m}).$$

Since by assumption $x < 1$ if $n = 0$, we have $1 \ll x^{-m}$ and hence we obtain a bound $O_{M,m}(x^{M-1-2m})$ for the contribution of the first summand of Proposition 2.2.7. Choosing $M = N + m$ we obtain a bound $O_{N,m}(x^{N-1-m})$ for the contribution of the first summand of Proposition 2.2.7 if $n = 0$, and a bound 0 otherwise.

We turn now to the second summand, whose contribution we estimate similarly. The deriv-

---

[1] Observe that by Leibniz' rule we have $\partial^m fg/\partial x^m \ll \sum_{k=0}^{m}(\partial^{m-k}f/\partial x^{m-k})\cdot(\partial^k g/\partial x^k)$.

ative $\frac{\partial^{m+n}}{\partial x^m \partial y^n}$ of the second summand is

$$\ll_{M,m,n} \sum_{k=0}^{m} \sum_{l=0}^{n} \frac{\partial^{m-k+n-l} x^{M-1} y^{-M}}{\partial x^{m-k} \partial y^{n-l}} \int_{1}^{2} \frac{\partial^{k+l} P_M(uy/x)}{\partial x^k \partial y^l} \frac{d^M}{du^M} \left(\frac{w(u^{-1})}{u^2} \right) du$$

$$\ll_{M,m,n} \sum_{k=0}^{m} \sum_{l=0}^{n} x^{M-1-m} y^{-M-n} \int_{1}^{2} \left(\sum_{j=l}^{k+l} c_{k,l,j} \left(\frac{uy}{x} \right)^j P_M^{(j)} \left(\frac{uy}{x} \right) \right) \frac{d^M}{du^M} \left(\frac{w(u^{-1})}{u^2} \right) du$$

$$= \sum_{j=0}^{m+n} x^{-m-1} y^{-n} \left(\frac{y}{x} \right)^{-M+j} \left(\sum_{l=0}^{j} \sum_{k=j-l}^{m} c_{k,l,j} \right) \int_{1}^{2} u^j P_M^{(j)} \left(\frac{uy}{x} \right) \frac{d^M}{du^M} \left(\frac{w(u^{-1})}{u^2} \right) du$$

$$\ll_{M,m,n} \sum_{j=0}^{m+n} x^{-m-1} y^{-n} \left(\frac{y}{x} \right)^{-M+j} \ll_{M,m,n} x^{-m-1} y^{-n} \left(\frac{y}{x} \right)^{-M+m+n},$$

where we used the assumption $y/x \geq 1$ in the last inequality. Since $y^{-n} \leq x^{-n}$ by the same assumption, setting $M = N + m + n$ we obtain a bound $O_{N,m,n}(x^{-1-m-n}(x/y)^N)$ for the contribution of the second summand of Proposition 2.2.7.

Now we put together the two bounds:

- If $n \neq 0$, only the second summand contributes, and the bound $O_{N,m,n}(x^{-1-m-n}(x/y)^N)$ is precisely the desired one.

- If $n = 0$, the first summand contributes $O_{N,m}(x^{N-1-m})$ and the second summand contributes $O_{N,m}(x^{-1-m}(x/y)^N)$, hence the total contribution is

$$x^{-1-m} \left(x^N + \left(\frac{x}{y} \right)^N \right)$$

which is again the desired bound.

$\square$

Our next main result on the function h is that, for small x, the function $y \mapsto h(x, y)$ behaves like a delta function, in the sense that

$$\int_{\mathbb{R}} f(y) h(x, y) dy$$

is close to $f(0)$ for any well-behaved f (this will made precise in the statement of Lemma 2.2.12).

The strategy of the proof will be to prove this first for $f(y) = y^n$, where n is a non-negative integer (this is the content of Proposition 2.2.10 and Proposition 2.2.11), and then to extend to all resonable functions f by writing $f(y)$ as a Taylor series centered at 0. We prove an auxiliary proposition first.

Proposition 2.2.9. *Let $\eta : \mathbb{R} \to \mathbb{R}$ be a smooth function supported in the interval $[1/2, 1]$. Then we have*

$$Y \int_{0}^{\infty} \frac{\eta(u)}{u} du - \sum_{j \geq 1} \int_{0}^{Y/j} \eta(u) du = \frac{1}{2} \int_{0}^{\infty} w(u) du + O_{N,\eta}(Y^{-N})$$

for every $N > 0$.

Proof. In what follows, let $M = N + 1$. We will treat the sum appearing in the statement using Euler-Maclaurin summation: the first term on the left hand side will be the approximating integral, while the right hand side consists of error terms. For every real number $t > 0$, define

$$\phi(t) = \int_0^{Y/t} \eta(u)du.$$

It is clear that $\phi(t)$ vanishes for $t \geq 2Y$, since for such t we have $Y/t < 1/2$ and hence η vanishes on the interval $[0, Y/t]$. We now claim that, for any $k \geq 1$, we have an identity

$$\phi^{(k)}(t) = \sum_{j=1}^{k} c_{j,k} \frac{Y^j}{t^{j+k}} \eta^{(j)}\left(\frac{Y}{t}\right) \tag{2.7}$$

for some constants $c_{j,k}$ ($1 \leq j \leq k$). We prove this by induction on k. For $k = 1$, it follows from the Fundamental Theorem of Calculus that

$$\phi'(t) = -\frac{Y}{t^2}\eta\left(\frac{Y}{t}\right).$$

Assume now (2.7) holds for some k. We then have

$$\phi^{(k+1)}(t) = \frac{d}{dt}\left(\sum_{j=1}^{k} c_{j,k} \frac{Y^j}{t^{j+k}} \eta^{(j)}\left(\frac{Y}{t}\right)\right)$$

$$= \sum_{j=1}^{k}\left(-(t+k)c_{j,k}\frac{Y^j}{t^{j+k+1}}\eta^{(j)}\left(\frac{Y}{t}\right) - c_{j,k}\frac{Y^{j+1}}{t^{(j+1)+(k+1)}}\eta^{(j+1)}\left(\frac{Y}{t}\right)\right),$$

which has the form indicated in (2.7).

We may now deduce that, when $Y \leq t \leq 2Y$ (which is precisely when $\phi^{(k)}(t)$ may be nonzero), we have

$$\phi^{(k)}(t) \ll \sum_{j=1}^{k} c_{j,k} \frac{Y^j}{Y^{j+k}} \eta^{(j)}\left(\frac{Y}{t}\right) \ll_{k,\eta} Y^{-k}. \tag{2.8}$$

We are now ready to use Euler-Maclaurin summation to relate the sum $\sum_{j\geq 1} \phi(j)$ to the corresponding integral. The Euler-Maclaurin summation formula (fact 2.2.6) yields

$$\sum_{a<j\leq b} \phi(j) = \int_a^b \phi(t)dt + \left(a - \lfloor a \rfloor - \frac{1}{2}\right)\phi(a) - \frac{(-1)^M}{M!}\int_a^b P_M(t)\phi^{(M)}(t)dt \tag{2.9}$$

if we choose any $a < Y$ and $b > 2Y$, so that all derivatives $\phi^{(k)}(a), \phi^{(k)}(b)$ with $k \geq 1$ vanish and moreover $\phi(b) = 0$. Note moreover that in this setup we have

$$\phi(a) = \int_{1/2}^{1} \eta(u)du$$

and hence, if we let $a \to 0^+$ in (2.9), we get

$$\sum_{j\geq 1} \phi(j) = \int_0^{\infty} \phi(t)dt - \frac{1}{2}\int_{1/2}^{1} \eta(u)du - \frac{(-1)^M}{M!}\int_Y^{2Y} P_M(t)\phi^{(M)}(t)dt. \tag{2.10}$$

We now observe that

$$\int_0^\infty \phi(t)dt = \int_0^{2Y} \phi(t)dt = \int_0^{2Y} \int_{1/2}^{Y/t} \eta(u)du\, dt$$

$$= \int_{1/2}^1 \eta(u) \int_0^{Y/u} 1 dt\, du = \int_{1/2}^1 \frac{\eta(u)Y}{u} du = Y \int_0^\infty \frac{\eta(u)}{u} du.$$

Moreover, in light of (2.8), we see that the last integral in (2.10) is $O_{M,\eta}(Y^{1-M}) = O_{N,\eta}(Y^{-N})$. Substituting these in (2.10), we obtain

$$\sum_{j\geq 1} \phi(j) = Y \int_0^\infty \frac{\eta(u)}{u} du - \frac{1}{2} \int_0^\infty w(u)du + O_{N,\eta}(Y^{-n}).$$

This is equivalent to the desired assertion.   □

The next Proposition is an easy consequence.

Proposition 2.2.10. *We have*

$$\int_{-X}^X h(x,y)dy = 1 + O_N(Xx^{N-1}) + O_N\left(\left(\frac{X}{x}\right)^{-N}\right)$$

for any $N > 0$.

Proof. We treat separately the integrals $\int_{-X}^X h_1(x,y)dy$ and $\int_{-X}^X h_2(x,y)dy$. For the former, we recall identity (2.3) used in the proof of Proposition 2.2.7, which yields

$$h_1(x,y) = \frac{1}{x} \int_0^\infty \frac{\omega(u)}{u} du + O_N(x^{N-1}).$$

Integrating from $-X$ to X we obtain

$$\int_{-X}^X h_1(x,y)dy = \frac{2X}{x} \int_0^\infty \frac{\omega(u)}{u} du + O_N(Xx^{N-1}). \tag{2.11}$$

On the other hand, directly from the definition of h_2, we have[2]

$$\int_{-X}^X h_2(x,y)dy = 2\sum_{j\geq 1} \frac{1}{xj} \int_0^X \omega\left(\frac{y}{xj}\right) dy \tag{2.12}$$

and subtracting (2.12) from (2.11) yields

$$\int_{-X}^X h(x,y)dy = \frac{2X}{x} \int_0^\infty \frac{\omega(u)}{u} du - 2\sum_{j\geq 1} \frac{1}{xj} \int_0^X \omega\left(\frac{y}{xj}\right) dy + O_N(Xx^{N-1}),$$

or, setting $Y = X/x$ and making the variable change $y = xju$,

$$\int_{-X}^X h(x,y)dy = 2Y \int_0^\infty \frac{\omega(u)}{u} du - 2\sum_{j\geq 1} \int_0^{Y/j} \omega(u)du + O_N(Xx^{N-1}).$$

---

[2]Interchanging sum and integral is not a problem, since all summands vanish for $j > 2X/x$.

However, by Proposition 2.2.9 with $\eta = \omega$, we have

$$Y \int_0^\infty \frac{\omega(u)}{u} du - \sum_{j \geq 1} \int_0^{Y/j} \omega(u) du = \frac{1}{2} \int_0^\infty \omega(u) du + O_N(Y^{-N}) = \frac{1}{2} + O_N\left(\left(\frac{X}{x}\right)^{-N}\right)$$

since we chose ω so that $\int_\mathbb{R} \omega(x) dx = 1$. Hence we obtain

$$\int_{-X}^X h(x,y) dy = 1 + O_N\left(\left(\frac{X}{x}\right)^{-N}\right) + O_N(Xx^{N-1}),$$

which is precisely the desired statement. □

Proposition 2.2.11. *Let $n > 0$ be an integer, and assume that $x \ll \min\{1, X\}$. Then we have*

$$\int_{-X}^X y^n h(x,y) dy \ll_{N,n} X^n \left(Xx^{N-1} + \left(\frac{X}{x}\right)^{-N}\right)$$

for any $N > 0$.

Proof. If n is odd then, since the integrand is odd with respect to y, the integral vanishes, and hence the result is obvious. Therefore we may assume from now on that n is even. In that case we have

$$\int_{-X}^X y^n h(x,y) dy = 2 \int_0^X y^n h(x,y) dy$$

so it suffices to prove the desired estimate for the latter integral.

The assumption that $x \ll 1$ and $x/X \ll 1$ implies that, if the result holds for some choice of N, then it also holds for any smaller choice. Hence it suffices to prove the proposition for $N \geq n$, which we assume henceforth. (This is actually the only place where we use the assumption $x \ll \min\{1, X\}$.)

We now call on Proposition 2.2.7, where we set $K = n$, yielding for $y > 0$

$$\begin{aligned}
h(x,y) = &- \frac{(-1)^N}{N!} x^{N-1} \int_{1/2}^1 P_N\left(\frac{u}{x}\right) w^{(N)}(u) du \\
&+ \frac{(-1)^n}{n!} \frac{x^{n-1}}{y^n} \int_1^2 P_n\left(\frac{uy}{x}\right) \frac{d^n}{du^n}\left(\frac{w(u^{-1})}{u^2}\right) du,
\end{aligned}$$

whence

$$\begin{aligned}
\int_0^X y^n h(x,y) dy = &\frac{(-1)^N}{(n+1)N!} X^{n+1} x^{N-1} \int_{1/2}^1 P_N\left(\frac{u}{x}\right) w^{(N)}(u) du \\
&+ \frac{(-1)^n}{n!} x^{n-1} \int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right) \frac{d^n}{du^n}\left(\frac{w(u^{-1})}{u^2}\right) du\, dy.
\end{aligned}$$

The first summand is clearly $O_N(X^{n+1}x^{N-1})$. It suffices therefore to prove that the second summand is $O_{N,n}(x^N/X^{N-n})$, which is equivalent to

$$\int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right) \psi(u) du\, dy \ll_{N,n} \frac{x^{N-n+1}}{X^{N-n}} \tag{2.13}$$

where we set

$$\psi(u) = \frac{d^n}{du^n}\left(\frac{w(u^{-1})}{u^2}\right).$$

In order to do this we first swap the order of integration in (2.13), so that

$$\int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right)\psi(u)du\,dy = \int_1^2 \psi(u)\int_0^X P_n\left(\frac{uy}{x}\right)dy\,du \qquad (2.14)$$

and we perfrom the variable change $y = zx/u$ on the innermost integral, so that

$$\int_0^X P_n\left(\frac{uy}{x}\right) = \frac{x}{u}\int_0^{uX/x} P_n(z)dz = \frac{x}{u}\cdot\frac{1}{n+1}\left(P_{n+1}\left(\frac{uX}{x}\right) - P_{n+1}(0)\right),$$

by standard properties of the Bernoulli polynomials. Here we recall that $n \geq 2$ is even, so that $n+1 \geq 3$ is odd and hence $P_{n+1}(0) = 0$ (again by the theory of Bernoulli polynomials). We conclude by (2.14) that

$$\int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right)\psi(u)du\,dy = \int_1^2 \psi(u)\frac{x}{u(n+1)}P_{n+1}\left(\frac{uX}{x}\right)du$$
$$= \frac{x}{n+1}\int_1^2 P_{n+1}\left(\frac{uX}{x}\right)\frac{\psi(u)}{u}du.$$

We finish by repeated integration by parts: performing this $N - n$ times in the last integral above, the previous equality yields

$$\int_0^X \int_1^2 P_n\left(\frac{uy}{x}\right)\psi(u)du\,dy = \frac{x^{N-n+1}}{X^{N-n}}\cdot\frac{n!}{(N+1)!}\int_1^2 P_{N+1}\left(\frac{uX}{x}\right)\frac{\psi(u)}{u}du$$

and the straightforward estimate

$$\frac{n!}{(N+1)!}\int_1^2 P_{N+1}\left(\frac{uX}{x}\right)\frac{\psi(u)}{u}du \ll_{N,n} 1$$

implies now (2.13), and we are done. $\qquad\square$

We can now state and prove the promised delta-function behaviour of $h(x, y)$, for small x.

Lemma 2.2.12. *Let $f \in C^\infty(\mathbb{R})$ be a smooth function with compact support $supp(f) \subseteq [-B, B]$. For each $k \in \mathbb{Z}_{\geq 0}$, let B_k be a real number such that*

$$|f^{(k)}(y)| \leq B_k \text{ for all } y \in \mathbb{R}.$$

Then if $x \ll 1$ we have

$$\int_\mathbb{R} f(y)h(x,y)dy = f(0) + O_M((B_0B + B_0 + B_1 + \cdots + B_{2M+1})x^M)$$

for every $M > 0$.

Proof. Let $X = \min\{1, x^{\frac{1}{2}}\}$. According to Lemma 2.2.8, we have (for every N)

$$h(x,y) \ll_N x^{-1}\left(x^N + \left(\frac{x}{|y|}\right)^N\right).$$

If $|y| \geq X$, we have $\left(\frac{x}{|y|}\right)^N \leq \left(\frac{x}{X}\right)^N$, the latter being equal to $x^{\frac{N}{2}}$ if $x < 1$ and x^N otherwise, in view of our choice of X. It follows therefore that $\left(\frac{x}{|y|}\right)^N \ll x^{\frac{N}{2}}$, since by assumption $x \ll 1$. We obtain

$$h(x, y) \ll_N x^{-1}(x^N + x^{\frac{N}{2}}) \ll x^{\frac{N}{2}-1} \text{ for } |y| \geq X.$$

Choosing $N = 2M + 2$ we get $h(x, y) \ll x^M$ for $|y| \geq X$. It now follows that

$$\int_{|y| \geq X} f(y)h(x, y)dy \ll_M x^M \int_{|y| \geq X} f(y)dy \ll_M B_0 B x^M. \tag{2.15}$$

Now, for $|y| < X$, we use Taylor's Theorem to write

$$f(y) = \sum_{k=0}^{2M} \frac{f^{(k)}(0)}{k!} y^k + \frac{f^{(2M+1)}(c)}{(2M+1)!} y^{2M+1}$$

for some c with $|c| < X$. Setting $r(y) = \frac{f^{(2M+1)}(c)}{(2M+1)!} y^{2M+1}$, we have $r(y) \ll B_{2M+1} X^{2M+1}$. Now we have

$$\int_{|y|<X} f(y)h(x, y)dy = \int_{|y|<X} \left(\sum_{k=0}^{2M} \frac{f^{(k)}(0)}{k!} y^k + r(y) \right) h(x, y)dy$$

$$= \sum_{k=0}^{2M} \frac{f^{(k)}(0)}{k!} \int_{|y|<X} y^k h(x, y)dy + \int_{|y|<X} r(y)h(x, y)dy.$$

Using the fact that $h(x, y) \ll x^{-1}$, by Proposition 2.2.3, it follows immediately that the latter term is $O_M(B_{2M+1} x^{-1} X^{2M+2}) = O_M(B_{2M+1} x^M)$, since $X \leq x^{\frac{1}{2}}$. For the terms $k = 1, \ldots, 2M$, we use Proposition 2.2.11. The condition $x \ll \min\{1, X\}$ follows from $x \ll 1$. We then have

$$\int_{|y|<X} y^k h(x, y)dy \ll_N X^k \left(X x^{N-1} + \left(\frac{X}{x}\right)^{-N} \right) \ll_N X x^{N-1} + \left(\frac{X}{x}\right)^{-N}$$

for any N, where we used $X \leq 1$.

If $x < 1$, then $X = x^{\frac{1}{2}}$ and the above yields $\int_{|y|<X} y^k h(x, y)dy \ll_N x^{\frac{N}{2}}$. If $x \geq 1$ then $X = 1$ and the above yields $\int_{|y|<X} y^k h(x, y)dy \ll x^{N-1}$. Choosing $N = 2M$ or $N = M + 1$ as appropriate we get $\int_{|y|<X} y^k h(x, y)dy \ll x^M$. Finally we deal with the term $k = 0$ analogously, this time using Proposition 2.2.10, yielding

$$\int_{|y|<X} h(x, y)dy = 1 + O_M(x^M).$$

Putting all these estimates together, and using $|f^{(k)}(0)| \leq B_k$, we obtain

$$\int_{|y|<X} f(y)h(x, y)dy = f(0) + O_M((B_0 + B_1 + \cdots + B_{2M+1})x^M) \tag{2.16}$$

Putting (2.15) and (2.16) together gives the desired assertion. $\square$

§2.3 Counting solutions to polynomial equations

In this section we show how Lemma 2.1.1 can be used to count solutions to equations of the form $F(x) = 0$, where F is a polynomial in n variables with integer coefficients. As mentioned in the Introduction, we will do a *weighted* count, which is preferable for technical reasons even if one's goal is to compute the number of solutions in the usual sense. In this section we shall work in a quite general setup. In the next chapter we will restrict to the case of quadratic forms.

For now let $w \in C^\infty(\mathbb{R}^n)$ be a smooth compactly supported function, and let P be a positive real number. Define

$$N(F, w, P) = \sum_{\substack{x \in \mathbb{Z}^n \\ F(x) = 0}} w\left(\frac{x}{P}\right) = \sum_{x \in \mathbb{Z}^n} w\left(\frac{x}{P}\right) \delta_{F(x)}$$

as the number of solutions to $F(x) = 0$, weighted by the smooth weight whose value at x is $w(P^{-1}x)$. The main result here is the following.

Lemma 2.3.1. *For any $Q > 1$, we have*

$$N(F, w, P) = c_Q Q^{-2} \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c)$$

where

$$S_q(c) = \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, q)} \sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{aF(b) + c \cdot b}{q}\right)$$

and

$$I_q(c) = \int_{\mathbb{R}^n} w\left(\frac{x}{P}\right) h\left(\frac{q}{Q}, \frac{F(x)}{Q^2}\right) e\left(\frac{-c \cdot x}{q}\right) dx.$$

(In the Definition of $S_q(c)$, the notation $\sum\limits_{b \,(\mathrm{mod}\, q)}$ means that each component of the n-tuple b ranges over a set of class representatives $(\mathrm{mod}\, q)$. Moreover, $\cdot$ denotes the usual dot product in $\mathbb{R}^n$.)

Proof. We use Lemma 2.1.1 in the definition of $N(F, w, P)$, yielding

$$N(F, w, P) = \sum_{x \in \mathbb{Z}^n} w\left(\frac{x}{P}\right) c_Q Q^{-2} \sum_{q=1}^{\infty} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, q)} e\left(\frac{aF(x)}{q}\right) h\left(\frac{q}{Q}, \frac{F(x)}{Q^2}\right)$$

$$= c_Q Q^{-2} \sum_{q=1}^{\infty} \sideset{}{^*}\sum_{a \,(\mathrm{mod}\, q)} \sum_{x \in \mathbb{Z}^n} e\left(\frac{aF(x)}{q}\right) w\left(\frac{x}{P}\right) h\left(\frac{q}{Q}, \frac{F(x)}{Q^2}\right). \qquad (2.17)$$

Let us study the innermost sum. We split the possible choices of x into the q^n residue classes $(\mathrm{mod}\, q)$ of vectors in $\mathbb{Z}^n$. Taking into account that $F(x) \equiv F(b) \pmod{q}$ when $x \equiv b \pmod{q}$, we see that the innermost sum equals

$$\sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{aF(b)}{q}\right) \sum_{\substack{x \in \mathbb{Z}^n \\ x \equiv b \,(\mathrm{mod}\, q)}} w\left(\frac{x}{P}\right) h\left(\frac{q}{Q}, \frac{F(x)}{Q^2}\right)$$

$$= \sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{aF(b)}{q}\right) \sum_{y \in \mathbb{Z}^n} w\left(\frac{b + qy}{P}\right) h\left(\frac{q}{Q}, \frac{F(b + qy)}{Q^2}\right). \qquad (2.18)$$

The innermost sum in (2.18) can be written as $\sum_{y \in \mathbb{Z}^n} f_{q,b}(y)$ where

$$f_{q,b}(y) = w\left(\frac{b+qy}{P}\right) h\left(\frac{q}{Q}, \frac{F(b+qy)}{Q^2}\right).$$

It follows therefore from the n-dimensional Poisson summation formula that the innermost sum in (2.18) is equal to

$$\sum_{c \in \mathbb{Z}^n} \widehat{f_{q,b}}(c)$$

$$= \sum_{c \in \mathbb{Z}^n} \int_{\mathbb{R}^n} w\left(\frac{b+qy}{P}\right) h\left(\frac{q}{Q}, \frac{F(b+qy)}{Q^2}\right) e(-c \cdot y) dy$$

$$= q^{-n} \sum_{c \in \mathbb{Z}^n} e\left(\frac{c \cdot b}{q}\right) \int_{\mathbb{R}^n} w\left(\frac{x}{P}\right) h\left(\frac{q}{Q}, \frac{F(x)}{Q^2}\right) e\left(-\frac{c \cdot x}{q}\right) dx$$

$$= q^{-n} \sum_{c \in \mathbb{Z}^n} e\left(\frac{c \cdot b}{q}\right) I_q(c)$$

where the second equality follows from the change of variables $x = (y-b)/q$, and the third from the definition of $I_q(c)$. We conclude from (2.18) that the innermost sum in (2.17) is given by

$$q^{-n} \sum_{b \,(\mathrm{mod}\ q)} \sum_{c \in \mathbb{Z}^n} e\left(\frac{aF(b) + c \cdot b}{q}\right) I_q(c)$$

and hence, by (2.17), we obtain

$$N(F, w, P) = c_Q Q^{-2} \sum_{q=1}^{\infty} q^{-n} \sideset{}{^*}\sum_{a\,(\mathrm{mod}\ q)} \sum_{b\,(\mathrm{mod}\ q)} \sum_{c \in \mathbb{Z}^n} e\left(\frac{aF(b) + c \cdot b}{q}\right) I_q(c)$$

$$= c_Q Q^{-2} \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} \sideset{}{^*}\sum_{a\,(\mathrm{mod}\ q)} \sum_{b\,(\mathrm{mod}\ q)} e\left(\frac{aF(b) + c \cdot b}{q}\right) I_q(c)$$

$$= c_Q Q^{-2} \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c),$$

as desired. $\square$

3 The Case of Quadratic Forms

We shall now use Lemma 2.3.1 to count solutions in $\mathbb{Z}^n$ to $F(x) = 0$, where $F(x) = F^{(0)}(x) - m$, $F^{(0)}$ is a positive definite quadratic form with integer coefficients and $m > 1$ is an integer. For simplicity we will restrict to the case of diagonal quadratic forms, so that

$$F^{(0)}(x) = \lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$$

for some positive integers $\lambda_1, \ldots, \lambda_n$, where $n \geq 4$. Set $\lambda = (\lambda_1, \ldots, \lambda_n)$, so that

$$|\lambda| = \max_{1 \leq i \leq n} \lambda_i.$$

Moreover, define

$$\Delta = 2\lambda_1 \cdots \lambda_n$$

(the reason for the factor 2 will become clear in §3.4). Let furthermore $G(x) = F^{(0)}(x) - 1$. In our application of Lemma 2.3.1 we shall take $P = Q = \sqrt{m}$. The weight with which solutions to $F(x) = 0$ will be counted will thus be of the form $x \mapsto w(x/\sqrt{m})$, and when x is a solution to $F(x) = 0$ we have $G(x/\sqrt{m}) = 0$. Therefore the weights w we are interested in should be supported around the set $\{x \in \mathbb{R}^n : G(x) = 0\}$. Using Lemma 2.3.1 we will deduce the following result, where we abbreviate $N(F, w, \sqrt{m})$ by $N(F, w)$.

Theorem 3.0.1. *Let w be a compactly supported weight. Let $n/4 > \varepsilon > 0$, and let $K > 100n^2/\varepsilon$ be an integer. We then have*

$$N(F, w) = \sigma_\infty(F^{(0)}, w) \prod_{p \; prime} \sigma_p(F^{(0)}, m) m^{\frac{n}{2} - 1}$$
$$+ O_\varepsilon \left(\Delta^{\frac{n+3}{2}} |\lambda|^{\frac{K}{2}} |w|_K m^{\frac{n-1}{4} + \varepsilon} \right).$$

The expression for $N(F, w)$ that Lemma 2.3.1 will output involves the so-called *singular integral*, defined by

$$\sigma_\infty(F^{(0)}, w) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w(x) dx. \tag{3.1}$$

If $G(x)$ is close to 0, then $\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2$ is close to 1, and therefore one of $\lambda_i x_i^2$ must be away from 0. For technical reasons, the calculations that lead to the appearance of the singular integral in our final results are most easily performed when the index i for which this holds is fixed. We therefore decompose our weight w into a sum of weights with smaller supports with this property, and then prove our results for these small weights, from which the main results follow by additivity. This is the purpose of the next section.

§3.1 Decomposing the weight

Define the set

$$S = \left\{ x \in \mathbb{R}^n : |x_1^2 + \cdots + x_n^2 - 1| < \frac{1}{3n} \right\}$$

and for each $j \in \{1, \ldots, n\}$, define

$$S_{j,+} = S \cap \left\{ x \in \mathbb{R}^n : x_j > \frac{\sqrt{n - \frac{1}{3}}}{n} \right\} \text{ and } S_{j,-} = S \cap \left\{ x \in \mathbb{R}^n : x_j < -\frac{\sqrt{n - \frac{1}{3}}}{n} \right\}.$$

We now observe that

$$S = \bigcup_{j=1}^{n} (S_{j,+} \cup S_{j,-})$$

simply because if $x \in S$ then $x_1^2 + \cdots + x_n^2 > 1 - 1/3n$, and hence for some j we have $|x_j|^2 > (1 - 1/3n)/n$, which implies $|x_j| > \sqrt{n - 1/3}/n$. Let further

$$T = \left\{ x \in \mathbb{R}^n : |x_1^2 + \cdots + x_n^2 - 1| > \frac{1}{4n} \right\}.$$

Then $T \cup S_{1,+} \cup S_{1,-} \cup \cdots \cup S_{n,+} \cup S_{n,-}$ is a finite open cover of $\mathbb{R}^n$; we fix once and for all a smooth partition of unity $\varphi_T, \varphi_{1,+}, \varphi_{1,-} \ldots, \varphi_{n,+}, \varphi_{n,-}$ subordinate to this open cover. Now we can write

$$w = w_T + w_{1,+} + w_{1,-} + \cdots + w_{n,+} + w_{n,-}$$

where $w_T(x) = w(x) \varphi_T \left(\sqrt{\lambda_1} x_1, \ldots, \sqrt{\lambda_n} x_n \right)$, and similarly $w_{j,\pm} = w(x) \varphi_{j,\pm} \left(\sqrt{\lambda_1} x_1, \ldots, \sqrt{\lambda_n} x_n \right)$. In light of this decomposition we see that

$$N(F, w) = \sum_{j=1}^{n} N(F, w_{j,+}) + \sum_{j=1}^{n} N(F, w_{j,-}) + N(F, w_T)$$

and

$$\sigma_\infty(F^{(0)}, w) = \sum_{j=1}^{n} \sigma_\infty(G, w_{j,+}) + \sum_{j=1}^{n} \sigma_\infty(F^{(0)}, w_{j,-}) + \sigma_\infty(F^{(0)}, w_T),$$

since clearly $N(F, w)$ and $\sigma_\infty(F^{(0)}, w)$ are linear in the weight w. We also have $N(F, w_T) = 0$ and $\sigma_\infty(F^{(0)}, w_T) = 0$. For the first equality, observe that

$$N(F, w_T) = \sum_{x \in \mathbb{Z}^n} w_T \left(\frac{x}{\sqrt{m}} \right) \delta_{F(x)}$$

and when $w_T(x/\sqrt{m})$ is nonzero we have

$$\left| \frac{\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 - m}{m} \right| > \frac{1}{4n}$$

which implies that $F(x)$ (i.e. $\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 - m$) is nonzero. For the second equality, recall that

$$\sigma_\infty(F^{(0)}, w_T) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w_T(x)$$

and the integrand vanishes identically for $\varepsilon < 1/4n$.

Therefore we obtain

$$N(F, w) = \sum_{j=1}^{n} N(F, w_{j,+}) + \sum_{j=1}^{n} N(F, w_{j,-}) \tag{3.2}$$

and

$$\sigma_\infty(F^{(0)}, w) = \sum_{j=1}^{n} \sigma_\infty(F^{(0)}, w_{j,+}) + \sum_{j=1}^{n} \sigma_\infty(F^{(0)}, w_{j,-}), \tag{3.3}$$

hence in order to obtain a result of the form

$$N(F, w) = \sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} (F^{(0)}, m)\sigma_p m^{\frac{n}{2}-1} + (\text{error term})$$

it suffices to prove similar results after substitution of w by one of the $w_{j,+}$, and then to add up the obtained expressions. By symmetry it suffices to treat the weight $w_{1,+}$. However this weight has special properties that make its treatment easier. Specifically, it is G-admissible according to the Definition below.

Definition 3.1.1. A smooth weight w with compact support is called *G-admissible* if there are positive real numbers R and ρ such that the following properties hold for all $x \in \text{supp}(w)$:

(i) $|G(x)| \leq 1/2$;

(ii) $\sqrt{\lambda_1} x_1 \geq \sqrt{n - 1/3}/n$;

(iii) For any point x^* with $|x_1^* - x_1| \leq R, x_2^* = x_2, \ldots x_n^* = x_n$, we have

$$\frac{\partial G}{\partial x_1}(x^*) \geq \rho;$$

(iv) There exists exactly one x^* as in (iii) with $G(x^*) = 0$.

(Note that whether a weight is G-admissible or not can be infered from the support of the weight alone.)

As we suggested, this important property holds for the weight $w_{1,+}$. This is the content of the next Proposition.

Proposition 3.1.2. *The weight $w_{1,+}$ is G-admissible.*

Proof. The support of $w_{1,+}$ is contained in the set

$$\{x \in \mathbb{R}^n : (\sqrt{\lambda_1} x_1, \ldots, \sqrt{\lambda_n} x_n) \in S_{1,+}\},$$

For x in the set above we have

$$|G(x)| = |(\sqrt{\lambda_1} x_1)^2 + \cdots + (\sqrt{\lambda_n} x_n)^2 - 1| < \frac{1}{3n} \leq \frac{1}{2}$$

so the first condition is clearly satisfied. Condition (ii) is immediate from the Definition of $S_{1,+}$. It suffices now to prove that (iii) and (iv) hold for every x in the set above, for some choice of R and ρ. Since the properties to be proven do not change under the linear transformation

$$(x_1, \ldots, x_n) \mapsto \left(\frac{x_1}{\sqrt{\lambda_1}} \ldots, \frac{x_n}{\sqrt{\lambda_n}} \right),$$

it suffices to prove this in the case $\lambda_1 = \cdots = \lambda_n = 1$ (in which case the above set is simply $S_{1,+}$). We prove that the parameters

$$R = \sqrt{\frac{3n-1}{3n^2}} - \sqrt{\frac{2n-1}{3n^2}} \quad \text{and} \quad \rho = 2\sqrt{\frac{2n-1}{3n^2}}$$

satisfy the requirements.

For (iii), we observe that, since for every $x \in S_{1,+}$ we have by definition $x_1 > \sqrt{(3n-1)/3n^2}$, for every x_1^* with $|x_1^* - x_1| \leq R$ we have

$$x_1^* \geq \sqrt{\frac{3n-1}{3n^2}} - R = \sqrt{\frac{3n-1}{3n^2}} - \left(\sqrt{\frac{3n-1}{3n^2}} - \sqrt{\frac{2n-1}{3n^2}}\right) = \frac{\rho}{2}.$$

Since

$$\frac{\partial G}{\partial x_1}(x^*) = 2x_1^*,$$

we are done with (iii).

For the existence part of (iv), we observe that for every $x \in S_{1,+}$ we have

$$x_1^2 + \cdots + x_n^2 < 1 + \frac{1}{3n} \quad \text{and} \quad x_1 > \sqrt{\frac{3n-1}{3n^2}}$$

and hence

$$x_2^2 + \cdots + x_n^2 < 1 + \frac{1}{3n} - \frac{3n-1}{3n^2} = 1 + \left(\frac{1}{3n^2} - \frac{2}{3n}\right) < 1. \tag{3.4}$$

Therefore we may define x^* by

$$x_1^* = \sqrt{1 - x_2^2 - \cdots - x_n^2}, \ x_2^* = x_2, \ldots, x_n^* = x_n.$$

We will check that x^* satisfies property (iv). For this, we must check that

$$\left| x_1 - \sqrt{1 - x_2^2 - \cdots - x_n^2} \right| \leq R. \tag{3.5}$$

- If $x_1^2 + \cdots + x_n^2 < 1$, we note that the inequalities $x_1 > \sqrt{\frac{3n-1}{3n^2}}$ and $x_1^2 + \cdots + x_n^2 > 1 - 1/3n$ imply

$$\sqrt{1 - x_2^2 - \cdots - x_n^2} - x_1 \leq \sqrt{1 - x_2^2 - \cdots - x_n^2} - \max\left\{\sqrt{\frac{3n-1}{3n^2}}, \sqrt{1 - \frac{1}{3n} - x_2^2 - \cdots - x_n^2}\right\}$$

and writing S for $x_2^2 + \cdots + x_n^2$, this bound can be rewritten as

$$\sqrt{1 - S} - \max\left\{\sqrt{\frac{3n-1}{3n^2}}, \sqrt{1 - \frac{1}{3n} - S}\right\}.$$

Now we see two cases. If $S \leq (3n^2 - 4n + 1)/3n^2$, the max above is the second term, and hence the above is

$$\sqrt{1 - S} - \sqrt{1 - \frac{1}{3n} - S} = \frac{1}{3n\left(\sqrt{1 - S} + \sqrt{1 - \frac{1}{3n} - S}\right)}$$

which is clearly increasing as a function of S, so its maximum is attained at $S = (3n^2 - 4n + 1)/3n^2$, where it equals

$$\sqrt{\frac{4n-1}{3n^2}} - \sqrt{\frac{3n-1}{3n^2}}.$$

If, on the other hand, $S > (3n^2 - 4n + 1)/3n^2$, then the bound is

$$\sqrt{1 - S} - \sqrt{\frac{3n-1}{3n^2}}$$

which is decreasing as a function of S, so it is at most

$$\sqrt{1 - \frac{3n^2 - 4n + 1}{3n^2}} - \sqrt{\frac{3n-1}{3n^2}} = \sqrt{\frac{4n-1}{3n^2}} - \sqrt{\frac{3n-1}{3n^2}}.$$

We conclude that if $x_1^2 + \cdots + x_n^2 < 1$, then

$$\left| x_1 - \sqrt{1 - x_2^2 - \cdots - x_n^2} \right| \leq \sqrt{\frac{4n-1}{3n^2}} - \sqrt{\frac{3n-1}{3n^2}} \leq \sqrt{\frac{3n-1}{3n^2}} - \sqrt{\frac{2n-1}{2n^2}} = R$$

where the second inequality follows from the fact that the square root is concave, so we have (3.5).

- If $x_1^2 + \cdots + x_n^2 \geq 1$, then since $x_1^2 + \cdots + x_n^2 \leq 1 + 1/3n$ we have

$$\left| x_1 - \sqrt{1 - x_2^2 - \cdots - x_n^2} \right| \leq \sqrt{1 + \frac{1}{3n} - x_2^2 - \cdots - x_n^2} - \sqrt{1 - x_2^2 - \cdots - x_n^2}$$

which, writing again S for $x_2^2 + \cdots + x_n^2$, is

$$\sqrt{1 + \frac{1}{3n} - S} - \sqrt{1 - S} = \frac{1}{3n\left(\sqrt{1 + \frac{1}{3n} - S} + \sqrt{1 - S}\right)}$$

and this is increasing as a function of S; since by (3.4) we have $S < 1 + \frac{1}{3n} - \frac{3n-1}{3n^2}$, it follows that

$$\sqrt{1 + \frac{1}{3n} - S} - \sqrt{1 - S} \leq \sqrt{\frac{3n-1}{3n^2}} - \sqrt{\frac{2n-1}{3n^2}} = R$$

and we are done.

The uniqueness follows from the (already proved) property (iii), since if there were two choices of x_1^* with $|x_1 - x_1^*| \leq R$ and $G(x_1^*, \ldots, x_n) = 0$ then, by the Mean Value Theorem, the first partial derivative of G would vanish somewhere in between. $\qquad\square$

We now see that Theorem 3.0.1 follows from the following version for G-admissible weights:

Lemma 3.1.3. *Suppose the weight w is G-admissible. Then for any $\varepsilon < \frac{n}{4}$ we have*

$$N(F, w) = \sigma_\infty(F^{(0)}, w) \prod_{p \ prime} \sigma_p(F^{(0)}, m) m^{\frac{n}{2} - 1}$$

$$+ O_\varepsilon\left(\Delta^{\frac{n+3}{2}}\left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M\right) m^{\frac{n-1}{4} + \varepsilon} + |w|_{N+1} |\lambda|^{\frac{N}{2}}\right)$$

where M and N are the smallest integers such that $M > 21n^2/4\varepsilon$ and $N > 7n(n+1)/\varepsilon$, respectively.

Proof that Lemma 3.1.3 implies Theorem 3.0.1. Using equalities (3.2) and (3.3), we see that it suffices to prove that

$$N(F, w_{j,\pm}) = \sigma_\infty(F^{(0)}, w_{j,\pm}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}$$
$$+ O_\varepsilon\left(\Delta^{\frac{n+3}{2}} |\lambda|^{\frac{K}{2}} |w|_K m^{\frac{n-1}{4}+\varepsilon}\right). \tag{3.6}$$

after which the result follows from adding this for all choices of $j \in \{1, \dots, n\}$ and $\pm \in \{-, +\}$. We now use Lemma 3.1.3, which implies

$$N(F, w_{j,\pm}) = \sigma_\infty(F^{(0)}, w_{j,\pm}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}$$
$$+ O_\varepsilon\left(\Delta^{\frac{n+3}{2}} \left(\frac{|w_{j,\pm}|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w_{j,\pm}|_M\right) m^{\frac{n-1}{4}+\varepsilon} + |w_{j,\pm}|_{N+1} |\lambda|^{\frac{N}{2}}\right) \tag{3.7}$$

where M and N are the smallest integers such that $M > 21n^2/4\varepsilon$ and $N > 7n(n+1)/\varepsilon$, respectively. We now recall that

$$w_{j,\pm}(x) = w(x)\varphi_{j,\pm}(\sqrt{\lambda_1} x_1, \dots, \sqrt{\lambda_n} x_n)$$

and Leibniz' rule implies that, when $i_1 + \cdots + i_n = s$,

$$\frac{\partial^{i_1} \cdots \partial^{i_n} w_{j,\pm}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}} \ll |\lambda|^{\frac{s}{2}} |w|_s$$

(recall that the $\varphi_{j,\pm}$ are regarded as fixed). This implies

$$|w_{j,\pm}|_s \ll |\lambda|^{\frac{s}{2}} |w|_s$$

and using this in (3.7) with $s = M, N$ we arrive at

$$N(F, w_{j,\pm}) = \sigma_\infty(F^{(0)}, w_{j,\pm}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}$$
$$+ O_\varepsilon\left(\Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |\lambda|^{\frac{M}{2}} |w|_M\right) m^{\frac{n-1}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{2N+1}{2}}\right)$$

Now the definition of K obviously implies that $|\lambda|^{\frac{M}{2}} |w|_M < |\lambda|^{\frac{K}{2}} |w|_K$. Moreover, the assumption $\varepsilon < \frac{n}{4}$ implies $K > 6n$, whence $|w|_0 |\lambda|^{3n} < |\lambda|^{\frac{K}{2}} |w|_K$. We obtain

$$N(F, w_{j,\pm}) = \sigma_\infty(F^{(0)}, w_{j,\pm}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}$$
$$+ O_\varepsilon\left(\Delta^{\frac{n+3}{2}} \left(|\lambda|^{\frac{K}{2}} |w|_K\right) m^{\frac{n-1}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{2N+1}{2}}\right)$$

but the last summand is also dominated by $|\lambda|^{\frac{K}{2}} |w|_K$, so it can be safely ignored, and we obtain Theorem 3.0.1. $\qquad\square$

So for the remainder of this Chapter we only need to work with G-admissible weights. Our weights in this Chapter will then be assumed to be G-admissible from now on, unless otherwise specified. This assumption will be particularly relevant in Section §3.3.

§3.2 The integrals $I_q(c)$

In this section we will give a series of estimates for the exponential integrals $I_q(c)$ that appear in the statement of Lemma 2.3.1, which in our case ($P = Q = \sqrt{m}$) are given by

$$I_q(c) = \int_{\mathbb{R}^n} w\left(\frac{x}{\sqrt{m}}\right) h\left(\frac{q}{\sqrt{m}}, \frac{F(x)}{m}\right) e\left(\frac{-c \cdot x}{q}\right) dx.$$

An obvious change of variables yields

$$I_q(c) = m^{\frac{n}{2}} \int_{\mathbb{R}^n} w(x) h\left(\frac{q}{\sqrt{m}}, \frac{F(\sqrt{m}x)}{m}\right) e\left(\frac{-\sqrt{m}c \cdot x}{q}\right) dx$$

and since $F(\sqrt{m}x) = F^{(0)}(\sqrt{m}x) - m = m(F^{(0)}(x) - 1) = mG(x)$, we obtain

$$I_q(c) = m^{\frac{n}{2}} \int_{\mathbb{R}^n} w(x) h\left(\frac{q}{\sqrt{m}}, G(x)\right) e\left(\frac{-\sqrt{m}c \cdot x}{q}\right) dx. \tag{3.8}$$

Define $H(r, x) = rh(r, x)$. If we set

$$I(r; u) = \int_{\mathbb{R}^n} w(x) H(r, G(x)) e(-u \cdot x) dx$$

then it is clear from the definitions that

$$I_q(c) = m^{\frac{n}{2}} r^{-1} I(r; r^{-1}c) \tag{3.9}$$

where

$$r = \frac{q}{\sqrt{m}}.$$

Therefore any bound for $I(r; u)$ will translate to a bound for $I_q(c)$, under (3.9). If $r > 1$, then for $x \in \mathrm{supp}(w)$ we have $h(r, G(x)) = 0$, since we are assuming that w is G-admissible and then for such x $|G(x)| \le 1/2 < r/2$, which implies that h vanishes at $(r, G(x))$ by Lemma 2.2.1. Therefore $I(r; u) = 0$ if $r > 1$. We may hence assume without loss of generality that $r \le 1$ from now on.

Before moving on, observe that by Lemma 2.2.8 we have

$$|H(r, x)| \ll_N r^N + \min\left\{1, \left(\frac{r}{|x|}\right)^N\right\} \tag{3.10}$$

and

$$\left|\frac{\partial^j H(r, x)}{\partial x^j}\right| \ll_{j,N} r^{-j} \min\left\{1, \left(\frac{r}{|x|}\right)^N\right\}. \tag{3.11}$$

These inequalities will play a key role in the proofs of our bounds for $I(r; u)$, which we start now. We will prove three bounds, indicating after each one the corresponding bound for $I_q(c)$.

Proposition 3.2.1. *We have*

$$I(r; u) \ll \frac{|w|_0}{\sqrt{\Delta}} r.$$

Proof. By (3.10) we have

$$H(r, G(x)) \ll r^2 + \min\left\{1, \frac{r^2}{G(x)^2}\right\} \ll r + \min\left\{1, \frac{r^2}{G(x)^2}\right\}$$

and it follows then from the definition of $I(r; u)$, by estimating the exponential trivially and $w(x)$ by $|w|_0$, that

$$I(r; u) \ll |w|_0 \int_{\text{supp}(w)} |H(r, G(x))| dx$$

$$\ll |w|_0 \left(\int_{\text{supp}(w)} r dx + \int_{\text{supp}(w)} \min \left\{ 1, \frac{r^2}{G(x)^2} \right\} dx \right). \tag{3.12}$$

The first integral is $r\text{vol}(\text{supp}(w))$. Now, since w is assumed to be G-admissible, $\text{supp}(w)$ is contained in $\left\{ x : |G(x)| < \frac{1}{2} \right\}$, which has volume $O\left(\frac{1}{\sqrt{\Delta}}\right)$. Hence the first integral in (3.12) is $\ll \frac{r}{\sqrt{\Delta}}$.

The second integral can be rewritten as

$$\int_{|G(x)| \leq r} 1 dx + \int_{|G(x)| > r} \frac{r^2}{G(x)^2} dx$$

where the integrals are taken over subsets of $\text{supp}(w)$. We now observe that, for any $M > 0$, the volume of the subset of $\text{supp}(w)$ where $|G(x)| \geq M$ is $O\left(\frac{M}{\sqrt{\Delta}}\right)$. To see this, recall that we are assuming $x_1 \gg \frac{1}{\sqrt{\lambda_1}}$ on $\text{supp}(w)$ (it follows from w being G-admissible), so that $\frac{\partial G}{\partial x_1} = 2\lambda_1 x_1 \gg \sqrt{\lambda_1}$ there. From this we see that, if x and x' are both points in $\text{supp}(w)$ such that $x_i = x_i'$ for $2 \leq i \leq n$ with $|G(x)|, |G(x')| \leq M$, then, by the Mean Value Theorem,

$$|G(x) - G(x')| = |x_1 - x_1'| \cdot \left| \frac{\partial G}{\partial x_1}(\xi_1, x_2, \ldots, x_n) \right| \gg |x_1 - x_1'| \sqrt{\lambda_1}$$

for some ξ_1 between x_1 and x_1', and since $|G(x) - G(x')| \ll M$ it follows that $|x_1 - x_1'| \ll \frac{M}{\sqrt{\lambda_1}}$, i.e., any line parallel to the x_1-axis intersects the subset of $\text{supp}(w)$ where $|G(x)| \leq M$ in a region of length $\ll \frac{M}{\sqrt{\lambda_1}}$. Furthermore, any line parallel to the x_i-axis for $2 \leq i \leq n$ intersects the same set in a region of length $\ll \frac{1}{\sqrt{\lambda_i}}$, simply because $\lambda_i x_i^2 \ll 1$ in $\text{supp}(w)$. Altogether, this implies

$$\text{vol}\left(\{x \in \text{supp} w : |G(x)| \leq M\}\right) \ll \frac{M}{\sqrt{\lambda_1}} \cdot \frac{1}{\sqrt{\lambda_2}} \cdots \frac{1}{\sqrt{\lambda_n}} \ll \frac{M}{\sqrt{\Delta}}$$

as claimed.

This means that the summand $\int_{|G(x)| \leq r} 1 dx$ is $\ll \frac{r}{\sqrt{\Delta}}$. We now write

$$\int_{|G(x)| > r} \frac{r^2}{G(x)^2} dx = \sum_{k=0}^{\infty} \int_{2^{k+1} r \geq |G(x)| > 2^k r} \frac{r^2}{G(x)^2} dx$$

$$\leq \sum_{k=0}^{\infty} \int_{2^{k+1} r \geq |G(x)| > 2^k r} \frac{r^2}{(2^k r)^2} dx$$

$$= \sum_{k=0}^{\infty} \int_{2^{k+1} r \geq |G(x)| > 2^k r} \frac{1}{2^{2k}} dx$$

$$\leq \sum_{k=0}^{\infty} \int_{|G(x)| \leq 2^{k+1} r} \frac{1}{2^{2k}} dx$$

$$\ll \sum_{k=0}^{\infty} \frac{1}{2^{2k}} \frac{2^{k+1} r}{\sqrt{\Delta}} \ll \frac{r}{\sqrt{\Delta}}.$$

Thus the second integral in (3.12) is $\ll \frac{r}{\sqrt{\Delta}}$. Putting everything together in (3.12), we get

$$I(r;u) \ll |w|_0 \left(\frac{r}{\sqrt{\Delta}} + \frac{r}{\sqrt{\Delta}} \right)$$

which is equivalent to the desired assertion. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Under (3.9), we obtain the following:

Lemma 3.2.2 (First estimate for $I_q(c)$). *We have*

$$I_q(c) \ll \frac{|w|_0}{\sqrt{\Delta}} m^{\frac{n}{2}}.$$

For our next estimate we need some preparatory work. We fix once and for all a smooth function $\nu \in C^\infty(\mathbb{R})$ supported in $[-1,1]$, which is positive in $]-1,1[$ and satisfies $\nu(x) = 1$ when $|x| \leq 1/2$ (functions with this behaviour are sometimes called *bump functions* in the literature). We then have

$$I(r;u) = \int_{\mathbb{R}^n} w(x)\nu(G(x))H(r,G(x))e(-u \cdot x)dx \qquad\qquad (3.13)$$

since when $w(x) \neq 0$ we have $|G(x)| \leq 1/2$ and hence $\nu(G(x)) = 1$. Now by the Inversion Theorem for the Fourier Transform applied to the function $y \mapsto \nu(y)H(r,y)$, which is smooth and compactly supported, we have

$$\nu(y)H(r,y) = \int_{-\infty}^{\infty} p(t)e(ty)dt \qquad\qquad (3.14)$$

where

$$p(t) = \int_{-\infty}^{\infty} \nu(v)H(r,v)e(-tv)dv. \qquad\qquad (3.15)$$

Equalities (3.13) and (3.14) together imply

$$I(r;u) = \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w(x)e(tG(x) - u \cdot x)dx\, dt.$$

We now bound $p(t)$. In order to do this, we observe that, by Leibniz' rule,

$$\frac{d^N}{dv^N}(\nu(v)H(r,v)) \ll_N \sum_{k=0}^{N} \frac{d^k}{dv^k}H(r,v)$$

since ν is fixed, and hence all its derivatives are $O(1)$. However, by using (3.10) (for $k = 0$) and (3.11) (for $k \neq 0$), we see that the above is

$$\ll_N r^2 + \sum_{k=0}^{N} r^{-k} \min\left\{1, \left(\frac{r}{|v|}\right)^2\right\} \ll_N r^2 + r^{-N} \min\left\{1, \left(\frac{r}{|v|}\right)^2\right\}$$

where we used the assumption that $r \leq 1$, so that each r^{-k} is bounded above by r^{-N}. We obtain a bound

$$\frac{d^N}{dv^N}(\nu(v)H(r,v)) \ll_N r^2 + r^{-N} \min\left\{1, \left(\frac{r}{|v|}\right)^2\right\}$$

but we claim that the first summand r^2 can be removed. If $|v| > 1$ then the above derivative is 0, since $\nu(v)$ is supported in $[-1, 1]$ by construction, so we are done. If $|v| \leq 1$ then

$$r^{-N} \min \left\{ 1, \left(\frac{r}{|v|} \right)^2 \right\} \geq r^{-N} \min \left\{ 1, r^2 \right\} = r^{-N} \cdot r^2 \geq r^2$$

since $r \leq 1$. This shows that we have

$$\frac{d^N}{dv^N} (\nu(v) H(r, v)) \ll r^{-N} \min \left\{ 1, \left(\frac{r}{|v|} \right)^2 \right\}.$$

In order to get a bound for $p(t)$ from here, we integrate by parts (3.15) N times, yielding

$$p(t) = \frac{1}{t^N} \int_{-\infty}^{\infty} \frac{d^N}{dv^N} (\nu(v) H(r, v)) e(-tv) dv$$

whence

$$
\begin{aligned}
p(t) &\ll_N \frac{1}{|t|^N} \int_{-\infty}^{\infty} r^{-N} \min \left\{ 1, \left(\frac{r}{|v|} \right)^2 \right\} dv \\
&= \frac{1}{|t|^N} \left(\int_{|v|>r} r^{-N} \left(\frac{r}{|v|} \right)^2 dv + \int_{-r}^{r} r^{-N} dv \right) \\
&= \frac{1}{|t|^N} \cdot 4 r^{1-N} \\
&\ll_N r(r|t|)^{-N}.
\end{aligned}
$$

To sum up, we have proved the following:

Proposition 3.2.3. *For each $r \leq 1$ and $u \in \mathbb{R}^n$ there exists a smooth function $p \in C^\infty(\mathbb{R})$, satisfying*

$$p(t) \ll_N r(r|t|)^{-N} \tag{3.16}$$

for every $N \geq 0$, such that

$$I(r; u) = \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx\, dt. \tag{3.17}$$

The previous Proposition will be pivotal to the next bound we establish for $I(r; u)$. The technical heart of this bound will be the following.

Proposition 3.2.4. *Assume that $|t| \leq \frac{|u_i|}{16\sqrt{\lambda_i}}$ for some $i \in \{1, \ldots, n\}$, where $u = (u_1, \ldots, u_n)$. (In particular, such an i exists if $|t| \leq \frac{|u|}{16\sqrt{|\lambda|}}$.) Then we have*

$$\int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx \ll_M \frac{|w|_M \lambda_i^{\frac{M}{2}}}{\sqrt{\Delta}} |u_i|^{-M}.$$

Proof. Define $f(x) = tG(x) - u \cdot x$. Throughout the proof, x is always assumed to be in $\mathrm{supp}(w)$. First recall that, since $|G(x)| < \frac{1}{2}$, we have $\lambda_i x_i^2 < \frac{3}{2}$, and hence $|\lambda_i x_i| \leq 4\sqrt{\lambda_i}$. We note that $\frac{\partial f}{\partial x_i} = 2t\lambda_i x_i - u_i$, and hence

$$\left| \frac{\partial f}{\partial x_i} \right| \geq |u_i| - 2|t||\lambda_i x_i| \geq |u_i| - 2 \frac{|u_i|}{16\sqrt{\lambda_i}} \cdot 4\sqrt{\lambda_i} = \frac{|u_i|}{2}. \tag{3.18}$$

Also note that

$$\left|\frac{\partial^2 f}{\partial x_i^2}\right| = 2|t|\lambda_i \le 2\frac{|u_i|}{16\sqrt{\lambda_i}}\lambda_i = \frac{1}{8}\sqrt{\lambda_i}|u_i|. \tag{3.19}$$

Now define recursively a sequence of functions $\eta_0, \eta_1, \dots$ by $\eta_0 = w$ and

$$\eta_{N+1}(x) = \frac{\partial}{\partial x_i}\left(\frac{\eta_N(x)}{g(x)}\right)$$

where $g = \frac{1}{|u_i|}\left(\frac{\partial f}{\partial x_i}\right)$. From (3.18) and (3.19) we see that $g(x) \gg 1$ and $\frac{\partial g}{\partial x_i} \ll \sqrt{\lambda_i}$. The relevance of this definition comes from the following equality: if I is the integral we are trying to estimate, then

$$I = \frac{(-1)^N}{(2\pi i)^N}|u_i|^{-N}\int_{\mathbb{R}^n}\eta_N(x)e(f(x))dx. \tag{3.20}$$

In order to establish this, we use induction on N. For $N = 0$ the equality is clear. Now assume the equality holds for a given N. We note that

$$\int_{\mathbb{R}^n}\eta_N(x)e(f(x))dx = \int_{\mathbb{R}^n}\frac{\eta_N(x)}{2\pi i\frac{\partial f}{\partial x_i}}\frac{\partial}{\partial x_i}e(f(x))dx = \frac{1}{2\pi i|u_i|}\int_{\mathbb{R}^n}\frac{\eta_N(x)}{g(x)}\frac{\partial}{\partial x_i}e(f(x))dx.$$

By integration by parts with respect to x_i, we rewrite the last integral as

$$-\int_{\mathbb{R}^n}\frac{\partial}{\partial x_i}\left(\frac{\eta_N(x)}{g(x)}\right)e(f(x))dx = -\int_{\mathbb{R}^n}\eta_{N+1}(x)e(f(x))dx$$

and hence

$$\int_{\mathbb{R}^n}\eta_N(x)e(f(x))dx = \frac{-1}{2\pi i|u_i|}\int_{\mathbb{R}^n}\eta_{N+1}(x)e(f(x))dx.$$

Using the induction hypothesis (3.20), it follows that $I = \frac{(-1)^{N+1}}{(2\pi i)^{N+1}}|u_i|^{-N-1}\int_{\mathbb{R}^n}\eta_{N+1}(x)e(f(x))dx$, establishing the induction step.

We shall now estimate $\eta_N(x)$. In order to do this, we claim that

$$\eta_N = \sum_{\substack{k+l=N\\k,l\ge 0}}\frac{c_{k,l}}{g^{l+N}}\frac{\partial^k w}{\partial x_i^k}\left(\frac{\partial g}{\partial x_i}\right)^l$$

for some coefficients $c_{k,l}$ whose value will not be relevant. This again goes by induction. For $N = 0$ it follows from $\eta_0 = w$. Now assume the previous equality holds for some N. Recall that $\frac{\partial g}{\partial x_i}$ is a constant function, which is clear from the definition of g. We then have

$$\begin{aligned}
\eta_{N+1} &= \frac{\partial}{\partial x_i}\left(\sum_{\substack{k+l=N\\k,l\ge 0}}\frac{c_{k,l}}{g^{l+N+1}}\frac{\partial^k w}{\partial x_i^k}\left(\frac{\partial g}{\partial x_i}\right)^l\right)\\
&= \sum_{\substack{k+l=N\\k,l\ge 0}}\frac{\partial}{\partial x_i}\left(\frac{c_{k,l}}{g^{l+N+1}}\right)\frac{\partial^k w}{\partial x_i^k}\left(\frac{\partial g}{\partial x_i}\right)^l + \sum_{\substack{k+l=N\\k,l\ge 0}}\frac{c_{k,l}}{g^{l+N+1}}\frac{\partial^{k+1} w}{\partial x_i^{k+1}}\left(\frac{\partial g}{\partial x_i}\right)^l\\
&= \sum_{\substack{k+l=N\\k,l\ge 0}}\frac{(-l-N-1)c_{k,l}}{g^{(l+1)+(N+1)}}\frac{\partial^k w}{\partial x_i^k}\left(\frac{\partial g}{\partial x_i}\right)^{l+1} + \sum_{\substack{k+l=N\\k,l\ge 0}}\frac{c_{k,l}}{g^{l+(N+1)}}\frac{\partial^{k+1} w}{\partial x_i^{k+1}}\left(\frac{\partial g}{\partial x_i}\right)^l
\end{aligned}$$

which is of the desired form.

Since $\frac{\partial g}{\partial x_i} \ll \sqrt{\lambda_i}$ and $g(x) \gg 1$, it follows from our claim that

$$\eta_M(x) \ll_M \sum_{\substack{k+l=M \\ k,l \geq 0}} \lambda_i^{\frac{l}{2}} \frac{\partial^k w}{\partial x_i^k} \ll_M \lambda_i^{\frac{M}{2}} |w|_M$$

and, using (3.20), it follows, by estimating the exponential trivially, that

$$I \ll_M \mathrm{vol}(\mathrm{supp}(w)) |w|_M \lambda_i^{\frac{M}{2}} |u_i|^{-M} \ll_M \mathrm{vol}\left(\left\{x : |G(x)| < \frac{1}{2}\right\}\right) |w|_M \lambda_i^{\frac{M}{2}} |u_i|^{-M}$$

and since the first factor is $O\left(\frac{1}{\sqrt{\Delta}}\right)$, the proposition follows. $\qquad\square$

Corollary 3.2.5. *For any $N \geq 0$ we have*

$$I(r; u) \ll_N \frac{|w|_{N+1} |\lambda|^{\frac{N}{2}}}{\sqrt{\Delta}} r^{-N} |u|^{-N}.$$

Proof. Let $M = N + 1$. Set $T = \frac{|u|}{16\sqrt{|\lambda|}}$. We then have

$$I(r; u) = \int_{-T}^{T} p(t) \int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx\, dt + \int_{|t|>T} p(t) \int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx\, dt.$$

To estimate the first summand, I_1, we use the previous lemma: we have

$$\int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx \ll \frac{|w|_M |\lambda|^{\frac{M}{2}}}{\sqrt{\Delta}} |u|^{-M},$$

and using the bound (3.16) we have $p(t) \ll r$. The (outer) range of integration in I_1 is $O\left(\frac{|u|}{\sqrt{|\lambda|}}\right)$, and this gives

$$I_1 \ll \frac{|w|_M |\lambda|^{\frac{M-1}{2}}}{\sqrt{\Delta}} r |u|^{1-M}.$$

In order to estimate the second summand, I_2, we estimate the exponential trivially: we then have

$$\int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx \ll |w|_0 \, \mathrm{vol}(\mathrm{supp}(w))$$

and we argued before, in the proof of the previous proposition, that the second factor is $O\left(\frac{1}{\sqrt{\Delta}}\right)$, so we get

$$I_2 \ll \int_{|t|>T} |p(t)| \frac{|w|_0}{\sqrt{\Delta}} dt$$

and the bound (3.16) gives $p(t) \ll r^{1-M} |t|^{-M}$, whence

$$\int_{|t|>T} |p(t)| dt \ll r^{1-M} \int_{|t|>T} |t|^{-M} dt = O_M(r^{1-M} T^{1-M}) = O_M\left(|\lambda|^{\frac{M-1}{2}} r^{1-M} |u|^{1-M}\right).$$

Using this in our bound for I_2, and using that $|w|_0 \leq |w|_M$, it follows that

$$I_2 \ll \frac{|w|_M |\lambda|^{\frac{M-1}{2}}}{\sqrt{\Delta}} r^{1-M} |u|^{1-M}$$

and combining the estimates for I_1 and I_2 we get

$$I(r;u) \ll \frac{|w|_M |\lambda|^{\frac{M-1}{2}}}{\sqrt{\Delta}} r |u|^{1-M} + \frac{|w|_M |\lambda|^{\frac{M-1}{2}}}{\sqrt{\Delta}} r^{1-M} |u|^{1-M} \ll \frac{|w|_M |\lambda|^{\frac{M-1}{2}}}{\sqrt{\Delta}} r^{1-M} |u|^{1-M}$$

where the second inequality comes from the fact that $r \leq 1$ for all relevant values of r. This proves the corollary. $\quad\square$

As before, a bound for $I_q(c)$ follows immediately from (3.9):

Lemma 3.2.6 (Second estimate for $I_q(c)$)**.** *We have*

$$I_q(c) \ll_N \frac{|w|_{N+1} |\lambda|^{\frac{N}{2}}}{\sqrt{\Delta}} m^{\frac{n+1}{2}} q^{-1} |c|^{-N}.$$

The estimates for $I(r;u)$ given before do not suffice for our purposes. In order to get better estimates, we must split the integral $\int_{\mathbb{R}^n} w(x) e(tG(x) - u \cdot x) dx$ into integrals over smaller regions so that an idea such as the one behind Proposition 3.2.4 can be applied to some of them.

This is done as follows. Choose a smooth function defined on $\mathbb{R}$ supported on the interval $[-1, 1]$ (say, the function ν used in (3.13)). Define

$$c_0 = \int_{-\infty}^{\infty} \nu(u) du$$

and, for $x \in \mathbb{R}^n$,

$$\nu^{(n)}(x) = \prod_{i=1}^{n} \nu(x_i).$$

Now we set

$$w^\star(z, y) = c_0^{-n} \nu^{(n)}(z) w(y + \delta z)$$

where $\delta \leq 1$ is a parameter that will be specified later. The following proposition is behind the role $w^\star$ plays in the integral partitioning we mentioned above.

Proposition 3.2.7. *We have*

$$w(x) = \delta^{-n} \int_{y \in \mathbb{R}^n} w^\star \left(\frac{x - y}{\delta}, y \right) dy.$$

Proof. The right hand side above equals

$$\delta^{-n} \int_{y \in \mathbb{R}^n} c_0^{-n} \nu^{(n)} \left(\frac{x - y}{\delta} \right) w(x) dy = \delta^{-n} c_0^{-n} w(x) \int_{y \in \mathbb{R}^n} \nu^{(n)} \left(\frac{x - y}{\delta} \right) dy$$

and performing the variable change $y = x - \delta z$, we see that the integral above is

$$\delta^n \int_{z \in \mathbb{R}^n} \nu^{(n)}(z) dz = \delta^n c_0^n$$

from which the result follows. $\quad\square$

When y is clear from context we shall write $w^\star(z, y)$ simply as $w^\star(z)$. Note that $w^\star(z)$ can only be nonzero for $|z| \leq 1$. We also remark the following easy property of $w^\star$ for a fixed y, which will be used freely in what follows.

Proposition 3.2.8. *For a fixed y and any $N \geq 0$ we have*

$$|w^\star|_N \ll_N |w|_N.$$

Proof. Clear from applying Leibniz' rule to the definition of $w^\star(z)$, taking into account that $\delta \leq 1$. □

We now rewrite (3.17) as

$$I(r; u) = \delta^{-n} \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} \int_{\mathbb{R}^n} w^\star \left(\frac{x - y}{\delta}, y \right) e(tG(x) - u \cdot x) dx\, dy\, dt,$$

or, making the variable change $x = y + \delta z$ and changing the order of integration, as

$$I(r; u) = \int_{\mathbb{R}^n} \int_{-\infty}^{\infty} p(t) \int_{\mathbb{R}^n} w^\star(z) e(tG(y + \delta z) - u \cdot (y + \delta z)) dz\, dt\, dy.$$

This immediately implies

$$|I(r; u)| \leq \int_{\mathbb{R}^n} \int_{-\infty}^{\infty} |p(t)| \left| \int_{\mathbb{R}^n} w^\star(z) e(tG(y + \delta z) - u \cdot (y + \delta z)) dz \right| dt\, dy. \qquad (3.21)$$

For some pairs (y, t) it will turn out that the innermost integral above is very small, and can be estimated by a procedure similiar to the one used in the proof of Proposition 3.2.4. These pairs (y, t) are the ones that will be called "good". The formal definition is as follows, where we set $f(z) = tG(y + \delta z) - u \cdot (y + \delta z)$ (note that f depends on y).

Definition 3.2.9. Let R be a positive real number. We say that a pair (y, t) is *R-good* (or simply *good* if R is clear from context) if, with f as above, one has

$$|\nabla f(0)| \geq R \max\{|t|\delta^2, 1\}.$$

If (y, t) is not R-good, we say (y, t) is *R-bad*.

The interest of this definition comes from the following proposition.

Proposition 3.2.10. *Suppose (y, t) is R-good, where $R \geq 3|\lambda|$. We then have*

$$\int_{\mathbb{R}^n} w^\star(z) e(f(z)) dz \ll_N |w^\star|_N R^{-N} \mathrm{vol}\left(\{z : |z| \leq 1, y + \delta z \in \mathrm{supp}(w)\} \right).$$

Proof. Assume (y, t) is R-good. We first observe that $\frac{\partial f}{\partial z_i}(z) = t\delta \frac{\partial}{\partial z_i} G(y + \delta z) - \delta u_i$, and hence

$$\frac{\partial f}{\partial z_i}(z) - \frac{\partial f}{\partial z_i}(0) = t\delta \frac{\partial}{\partial z_i} G(y + \delta z) - t\delta \frac{\partial}{\partial z_i} G(y) = t\delta^2 \frac{\partial}{\partial z_i} G(z).$$

Since $\frac{\partial}{\partial z_i} G(z) = 2\lambda_i z_i$, it follows that whenever $|z| \leq 1$ (in particular, whenever $w^\star(z) \neq 0$) we have $\left| \frac{\partial f}{\partial z_i}(z) - \frac{\partial f}{\partial z_i}(0) \right| \leq 2|\lambda||t|\delta^2$. We conclude

$$\left| \frac{\partial f}{\partial z_i}(z) \right| \geq \left| \frac{\partial f}{\partial z_i}(0) \right| - \left| \frac{\partial f}{\partial z_i}(0) - \frac{\partial f}{\partial z_i}(z) \right| \geq \left| \frac{\partial f}{\partial z_i}(0) \right| - 2|\lambda||t|\delta^2.$$

Now since (y, t) is good we may choose $i \in \{1, \ldots, n\}$ such that $\left| \frac{\partial f}{\partial z_i}(0) \right| \geq R|t|\delta^2$, and since $R \geq 3|\lambda|$, we have $2|\lambda||t|\delta^2 \leq \frac{2}{3} \left| \frac{\partial f}{\partial z_i}(0) \right|$, and it follows from the previously inequality that $\left| \frac{\partial f}{\partial z_i}(z) \right| \gg \left| \frac{\partial f}{\partial z_i}(0) \right|$ whenever $w^\star(z) \neq 0$. In particular,

$$\left| \frac{\partial f}{\partial z_i}(z) \right| \gg R \max\{|t|\delta^2, 1\} \text{ whenever } w^\star(z) \neq 0.$$

We also observe that $\frac{\partial^2 f}{\partial z_i^2}(z) = 2\lambda_i t \delta^2$, whence

$$\left| \frac{\partial^2 f}{\partial z_i^2}(z) \right| \ll R \max\{|t|\delta^2, 1\}.$$

Define now $R^\star = R \max\{|t|\delta^2, 1\}$, and set $g = \frac{\left(\frac{\partial f}{\partial z_i}\right)}{R^\star}$. The previous estimates show that

$$g \gg 1 \quad \text{and} \quad \frac{\partial g}{\partial z_i} \ll 1 \quad \text{in } \operatorname{supp}(w^\star). \tag{3.22}$$

Now we proceed as in Proposition 3.2.4. Define recursively a sequence of functions $\eta_0, \eta_1, \eta_2, \ldots$ by

$$\eta_0 = w^\star \quad \text{and} \quad \eta_{N+1} = \frac{\partial}{\partial z_i}\left(\frac{\eta_N}{g}\right).$$

Let I be the integral we wish to estimate. With this definition we have, for every $N \geq 0$,

$$I = \frac{(-1)^N}{(2\pi i)^N}(R^\star)^{-N} \int_{\mathbb{R}^n} \eta_N(z) e(f(z)) dz \tag{3.23}$$

as can be seen by induction: for $N = 0$ it is the definition of I, and if this holds for some N, then

$$\int_{\mathbb{R}^n} \eta_N(z) e(f(z)) dx = \int_{\mathbb{R}^n} \frac{\eta_N(x)}{2\pi i \frac{\partial f}{\partial z_i}} \frac{\partial}{\partial z_i} e(f(z)) dz = \frac{1}{2\pi i R^\star} \int_{\mathbb{R}^n} \frac{\eta_N(z)}{g(z)} \frac{\partial}{\partial z_i} e(f(z)) dz.$$

We now integrate by parts with respect to z_i, and rewrite the last integral as

$$-\int_{\mathbb{R}^n} \frac{\partial}{\partial z_i}\left(\frac{\eta_N(z)}{g(z)}\right) e(f(z)) dz = -\int_{\mathbb{R}^n} \eta_{N+1}(z) e(f(z)) dz$$

and hence

$$\int_{\mathbb{R}^n} \eta_N(z) e(f(z)) dz = \frac{-1}{2\pi i R^\star} \int_{\mathbb{R}^n} \eta_{N+1}(z) e(f(z)) dz.$$

Using the induction hypothesis, it follows that $I = \frac{(-1)^{N+1}}{(2\pi i)^{N+1}}(R^*)^{-N-1} \int_{\mathbb{R}^n} \eta_{N+1}(z) e(f(z)) dz$, finishing the induction.

We now finish by estimating the exponential trivially in (3.23). In order to do this we need to estimate η_N; for this we claim that

$$\eta_N = \sum_{\substack{k+l=N \\ k,l \geq 0}} \frac{c_{k,l}}{g^{l+N}} \frac{\partial^k w^\star}{\partial z_i^k}\left(\frac{\partial g}{\partial z_i}\right)^l$$

for some constants $c_{k,l}$. The proof is completely analogous to the one of the corresponding claim used in the proof of Proposition 3.2.4, but we reproduce it here for the sake of completeness. For $N = 0$ there is nothing to prove. Assuming this holds for some N, we have

$$\eta_{N+1} = \frac{\partial}{\partial z_i}\left(\sum_{\substack{k+l=N \\ k,l \geq 0}} \frac{c_{k,l}}{g^{l+N+1}} \frac{\partial^k w^\star}{\partial z_i^k}\left(\frac{\partial g}{\partial z_i}\right)^l\right)$$

$$= \sum_{\substack{k+l=N \\ k,l \geq 0}} \frac{\partial}{\partial z_i}\left(\frac{c_{k,l}}{g^{l+N+1}}\right) \frac{\partial^k w^\star}{\partial z_i^k}\left(\frac{\partial g}{\partial z_i}\right)^l + \sum_{\substack{k+l=N \\ k,l \geq 0}} \frac{c_{k,l}}{g^{l+N+1}} \frac{\partial^{k+1} w^\star}{\partial z_i^{k+1}}\left(\frac{\partial g}{\partial z_i}\right)^l$$

$$= \sum_{\substack{k+l=N \\ k,l \geq 0}} \frac{(-l-N-1)c_{k,l}}{g^{(l+1)+(N+1)}} \frac{\partial^k w^\star}{\partial z_i^k}\left(\frac{\partial g}{\partial z_i}\right)^{l+1} + \sum_{\substack{k+l=N \\ k,l \geq 0}} \frac{c_{k,l}}{g^{l+(N+1)}} \frac{\partial^{k+1} w^\star}{\partial z_i^{k+1}}\left(\frac{\partial g}{\partial z_i}\right)^l$$

which has the desired form.

Since $w^\star$ is supported on $\{z : |z| \leq 1\}$, so is each η_N, and in particular the support of each η_N has volume $O(1)$. Furthermore, it follows from our last claim, together with (3.22), that

$$\eta_N \ll_N \sum_{0 \leq k \leq N} \left| \frac{\partial^k w^\star}{\partial x_i^k} \right| \leq |w^\star|_N$$

implying, together with (3.23) (and noting that only z's with $y + \delta z \in \operatorname{supp}(w)$ contribute to I, since clearly $\operatorname{supp}(\eta_N) \subseteq \operatorname{supp}(w)$), that

$$I \ll_N |w^\star|_N (R^\star)^{-N} \operatorname{vol}\left(\{z : |z| \leq 1, y + \delta z \in \operatorname{supp}(w)\}\right)$$

which, in view of $R^\star \geq R$, implies the statement of the proposition. $\qquad \square$

From the previous Proposition and (3.21) we derive that, if $R \geq 3|\lambda|$, then

$$I(r; u) \ll \iint_{(y,t) \ R\text{-good}} |p(t)| \, |w^\star|_N \, R^{-N} \int_{\substack{|z| \leq 1 \\ y + \delta z \in \operatorname{supp}(w)}} 1 dz \, dt \, dy$$

$$+ \iint_{(y,t) \ R\text{-bad}} |p(t)| \int_{\substack{|z| \leq 1 \\ y + \delta z \in \operatorname{supp}(w)}} |w^\star(z)| dz \, dt \, dy.$$

The first summand can be bounded by

$$\left(\int_{\mathbb{R}} |p(t)| \int_{\mathbb{R}^n} \int_{\substack{|z| \leq 1 \\ y + \delta z \in \operatorname{supp}(w)}} 1 dz \, dy \, dt \right) |w|_N \, R^{-N}$$

where we relaxed the condition that (y, t) is R-good and used Proposition 3.2.8. We now observe that

$$\int_{\mathbb{R}^n} \int_{\substack{|z| \leq 1 \\ y + \delta z \in \operatorname{supp}(w)}} 1 dz \, dy$$

$$= \delta^{-n} \int_{\mathbb{R}^n} \int_{\substack{|x-y| \leq \delta \\ x \in \operatorname{supp}(w)}} 1 dx \, dy \qquad \text{(by making the variable change } x = y + \delta z)$$

$$= \delta^{-n} \int_{\operatorname{supp}(w)} \int_{|x-y| \leq \delta} 1 dy \, dx \qquad \text{(by swapping the order of integration)}$$

$$= \delta^{-n} \int_{\operatorname{supp}(w)} \operatorname{vol}\left(\{y : |x - y| \leq \delta\}\right) dx$$

and since the volume above is obviously $O(\delta^n)$, it follows that

$$\int_{\mathbb{R}^n} \int_{\substack{|z| \leq 1 \\ y + \delta z \in \operatorname{supp}(w)}} 1 dz \, dy \ll \operatorname{vol}(\operatorname{supp}(w)) \ll \frac{1}{\sqrt{\Delta}}.$$

On the other hand, by using (3.16) with $N = 0$ for $|t| \leq 1/r$ and with $N = 2$ for $|t| > 1/r$, it is clear that

$$\int_{\mathbb{R}} |p(t)| dt \leq \int_{-\frac{1}{r}}^{\frac{1}{r}} r dt + \frac{1}{r} \int_{|t| > \frac{1}{r}} t^{-2} dt = 4,$$

implying that the first summand of our bound for $I(r; u)$ is

$$\ll \frac{|w|_N \, R^{-N}}{\sqrt{\Delta}}.$$

We deduce

Proposition 3.2.11. *Suppose $R \geq 3|\lambda|$. Then*

$$I(r; u) \ll_N \frac{|w|_N \, R^{-N}}{\sqrt{\Delta}} + \iint_{(y,t) \ R\text{-}bad} |p(t)| \int_{\substack{|z| \leq 1 \\ y + \delta z \in \text{supp}(w)}} |w^\star(z)| dz dt dy.$$

In order to estimate the second summand it will be convenient to fix a choice for δ. We let, from now on,

$$\delta = \frac{1}{\sqrt{|u|}}.$$

The following proposition shows some properties of R-bad pairs under this new assumption.

Proposition 3.2.12. *Assume $|u| \geq R^3$, and $R \geq 32n|\lambda|$. If (y, t) is an R-bad pair that contributes to the right hand side of Proposition 3.2.11 (i.e. if $y + \delta z \in \text{supp}(w)$ for some z with $|z| \leq 1$), then*

$$|t\nabla G(y) - u| \ll R|u|^{\frac{1}{2}}. \tag{3.24}$$

Moreover, we have $|t| \ll |u|$ and $|t| \gg \frac{1}{\sqrt{|\lambda|}}|u|$.

Proof. We begin with the first assertion. By definition, (y, t) is R-bad if $|\nabla f(0)| < R \max\{|t|\delta^2, 1\}$, where $f(z) = tG(y + \delta z) - u \cdot (y + \delta z)$. We then have

$$\nabla f(0) = \delta(t\nabla G(y) - u)$$

and hence the condition that (y, t) is bad translates (using $\delta = \frac{1}{\sqrt{|u|}}$) into

$$|t\nabla G(y) - u| \leq R|u|^{\frac{1}{2}} \max\left\{\frac{|t|}{|u|}, 1\right\}. \tag{3.25}$$

We will then be done if we can show that, under this assumption, $|t| \ll |u|$. In particular, if $|t| \leq 2\sqrt{2n}|u|$ we are done. Otherwise, the assumption implies, by looking at the first coordinate,

$$|2\lambda_1 t y_1 - u_1| \leq \frac{R|t|}{|u|^{\frac{1}{2}}}$$

and hence

$$|y_1| \leq \frac{R|t|/|u|^{\frac{1}{2}} + |u_1|}{2\lambda_1 |t|} \leq \frac{R}{2\lambda_1 |u|^{\frac{1}{2}}} + \frac{|u|}{2\lambda_1 |t|}.$$

Since by assumption $|u| \geq R^3$, we have $\frac{R}{2\lambda_1 |u|^{\frac{1}{2}}} \leq \frac{1}{2\lambda_1 R^{\frac{1}{2}}} \leq \frac{1}{4\sqrt{2n}\lambda_1}$, as we are assuming $R \geq 8n$. On the other hand, since we may assume $|t| > 2\sqrt{2n}|u|$, we have $\frac{|u|}{2\lambda_1 |t|} < \frac{1}{4\sqrt{2n}\lambda_1}$. Altogether, this implies

$$|y_1| < \frac{1}{2\sqrt{2n}\lambda_1}. \tag{3.26}$$

Note further that, since (y, t) is assumed to contribute to the right hand side of Proposition 3.2.11, y is at most δ apart from some point x in $\text{supp}(w)$. Recall that we assume $|x_1| \geq \frac{1}{\sqrt{2n}\lambda_1}$

for $x \in \mathrm{supp}(w)$. Hence $|y_1| \geq \frac{1}{\sqrt{2n\lambda_1}} - \delta = \frac{1}{\sqrt{2n\lambda_1}} - \frac{1}{|u|^{\frac{1}{2}}}$, and, since $|u| \geq R^3 \geq (8n|\lambda|)^3 \geq (8n\lambda_1)^3 \geq (2\sqrt{2n\lambda_1})^2$,

$$|y_1| \geq \frac{1}{\sqrt{2n\lambda_1}} - \frac{1}{2\sqrt{2n\lambda_1}} = \frac{1}{2\sqrt{2n\lambda_1}}. \tag{3.27}$$

Inequalities (3.26) and (3.27) contradict each other, so we are done with the first assertion.

Along the way we also proved the second assertion $|t| \ll |u|$ (we got a contradiction unless $|t| \leq 2\sqrt{2n}|u|$). Finally, we observe that (3.25) implies that, for any $i \in \{1, \ldots, n\}$, we have

$$|2\lambda_i t y_i - u_i| \leq 2\sqrt{2n}R|u|^{\frac{1}{2}}.$$

Choose i so that $|u_i| = |u|$. Dividing the above inequality by $|u|$, we have

$$\left| 2\lambda_i \frac{t}{|u|} y_i - \frac{u_i}{|u|} \right| \ll 2\sqrt{2n}R|u|^{-\frac{1}{2}} \leq \frac{2\sqrt{2n}}{R^{\frac{1}{2}}} \leq \frac{1}{2},$$

where we used $|u| \geq R^3$ and $R \geq 32n$. On the other hand, we have

$$\left| 2\lambda_i \frac{t}{|u|} y_i - \frac{u_i}{|u|} \right| \geq \left| \frac{u_i}{|u|} \right| - 2\lambda_i|y_i|\frac{|t|}{|u|} = 1 - 2\lambda_i|y_i|\frac{|t|}{|u|}$$

and combining the last two inequalities, we get

$$\frac{|t|}{|u|} \gg \frac{1}{\lambda_i y_i}.$$

We observed before that, since (y, t) is assumed to contribute to the right hand side of Proposition 3.2.11, y is at most δ apart from some point x in $\mathrm{supp}(w)$. This point x has $|x_i| \ll \frac{1}{\sqrt{\lambda_i}}$, and hence

$$|y_i| \ll \frac{1}{\sqrt{\lambda_i}} + \delta \ll \frac{1}{\sqrt{\lambda_i}}$$

since $\delta = \frac{1}{\sqrt{|u|}}$ and $|u| \gg |\lambda|$ by assumption. It follows that

$$\frac{|t|}{|u|} \gg \frac{1}{\sqrt{\lambda_i}} \geq \frac{1}{\sqrt{|\lambda|}}$$

and we are done. $\qquad\square$

Now we have everything we need in order to estimate the right hand side of Proposition 3.2.11, at least under the stronger assumptions of the previous proposition. We observe that the second summand is bounded by

$$\ll |w|_0 \, r\mathrm{vol}(\mathcal{B})$$

where $\mathcal{B}$ is the set of bad pairs (y, t) such that y is at most δ apart from a point in $\mathrm{supp}(w)$ (we used that $|p(t)| \ll r$, by (3.16)). The inequality

$$|2\lambda_i t y_i - u_i| \leq 2\sqrt{2n}R|u|^{\frac{1}{2}}$$

holds for every such pair and every $i \in \{1, \ldots, n\}$. For each fixed t, this prescribes an interval of length $O\left(\frac{R|u|^{\frac{1}{2}}}{\lambda_i|t|} \right)$ for y_i. Since $|t| \gg \frac{|u|}{\sqrt{|\lambda|}}$ by the previous Proposition, we have

$$\frac{R|u|^{\frac{1}{2}}}{\lambda_i|t|} \ll \frac{\sqrt{|\lambda|}R|u|^{-\frac{1}{2}}}{\lambda_i}$$

and hence, for $(y, t) \in \mathcal{B}$, each y_i ranges over an interval of length $O\left(\frac{\sqrt{|\lambda|}R|u|^{-\frac{1}{2}}}{\lambda_i}\right)$. Moreover, the previous proposition also implies that t ranges over an interval of length $O(|u|)$. We conclude that

$$\mathrm{vol}(\mathcal{B}) \ll |u| \cdot \prod_{i=1}^{n} \frac{\sqrt{|\lambda|}R|u|^{-\frac{1}{2}}}{\lambda_i} \ll \frac{|\lambda|^{\frac{n}{2}}}{\Delta} R^n |u|^{1-\frac{n}{2}}$$

and hence we conclude that (provided that $|u| \geq R^3$ and $R \geq 32n|\lambda|$)

$$I(r; u) \ll_N \frac{|w|_N \, R^{-N}}{\sqrt{\Delta}} + \frac{|w|_0 \, |\lambda|^{\frac{n}{2}}}{\Delta} R^n r |u|^{1-\frac{n}{2}}. \tag{3.28}$$

We are now ready to state and prove our last estimate for $I(r; u)$.

Proposition 3.2.13. *Suppose $|u| \geq 1$, let $\varepsilon \in \left(0, \frac{n}{2}\right)$ and let N be a positive integer such that $N \geq \frac{3n^2}{2\varepsilon}$. Then we have*

$$I(r; u) \ll_\varepsilon \left(\frac{|w|_0 \, |\lambda|^{\frac{3n}{2}(1-\varepsilon/n)^{-1}}}{\Delta} + \frac{|w|_N}{\sqrt{\Delta}}\right) (r^{-1}|u|)^\varepsilon r |u|^{1-\frac{n}{2}}.$$

Proof. Throughout the proof, set $C = (32n|\lambda|)^{\frac{3n}{n-\varepsilon}}$. We split the proof into two cases.

Case 1: $|u| \leq C r^{-\frac{2\varepsilon}{n}}$.
  Then we have

$$|u|^{\frac{n}{2}-1-\varepsilon} \leq |u|^{\frac{n}{2}} \leq C^{\frac{n}{2}} r^{-\varepsilon}$$

which is equivalent to

$$r \leq C^{\frac{n}{2}} (r^{-1}|u|)^\varepsilon r |u|^{1-\frac{n}{2}}.$$

By Proposition 3.2.1 we have

$$I(r; u) \ll \frac{|w|_0}{\sqrt{\Delta}} r \leq \frac{|w|_0 \, C^{\frac{n}{2}}}{\sqrt{\Delta}} (r^{-1}|u|)^\varepsilon r |u|^{1-\frac{n}{2}},$$

so we are done in this case, since $C^{\frac{n}{2}} \ll |\lambda|^{\frac{3n^2}{2(n-\varepsilon)}} = |\lambda|^{\frac{3n}{2}(1-\varepsilon/n)^{-1}}$.

Case 2: $|u| > C r^{-\frac{2\varepsilon}{n}}$.
  Let $R = 32n|\lambda|(r^{-1}|u|)^{\frac{\varepsilon}{3n}}$. We check that, with this choice of R, the conditions under which (3.28) holds are satisfied. It is clear that $R \geq 32n|\lambda|$, since $r \leq 1$ and $|u| \geq 1$. Furthermore, the condition $|u| \geq R^3$ is equivalent to $|u| \geq (32n|\lambda|)^3 (r^{-1}|u|)^{\varepsilon/n}$, which in turn is equivalent to

$$|u| \geq (32n|\lambda|)^{\frac{3n}{n-\varepsilon}} r^{-\frac{\varepsilon}{n-\varepsilon}} = C r^{-\frac{\varepsilon}{n-\varepsilon}}.$$

But this follows from the assumption of Case 2, since $r \leq 1$ and $\frac{2\varepsilon}{n} \geq \frac{\varepsilon}{n-\varepsilon}$ (the latter simplifies to $\varepsilon \leq \frac{n}{2}$).
  We now apply (3.28). In order to do this, we check that R^{-N} and R^n behave as desired:

- Our condition on N ensures that $\frac{\varepsilon N}{3n} > \frac{n}{2} - 1 - \varepsilon$ and $\frac{\varepsilon N}{3n} > 1 - \varepsilon$. We therefore have $r^{\frac{\varepsilon N}{3n}} \leq r^{1-\varepsilon}$ and $|u|^{-\frac{\varepsilon N}{3n}} \leq |u|^{\varepsilon+1-\frac{n}{2}}$. Multiplying the two yields

$$(r^{-1}|u|)^{\frac{-\varepsilon N}{3n}} \leq (r^{-1}|u|)^\varepsilon r |u|^{1-\frac{n}{2}}$$

  and since the choice of R ensures that $R^{-N} < (r^{-1}|u|)^{-\frac{\varepsilon N}{3n}}$, it follows that the first summand in (3.28) is $\ll \frac{|w|_N}{\sqrt{\Delta}} (r^{-1}|u|)^\varepsilon r |u|^{1-\frac{n}{2}}$.

- We have $R^n \ll |\lambda|^n (r^{-1}|u|)^{\frac{\varepsilon}{3}} \leq |\lambda|^n (r^{-1}|u|)^\varepsilon$. Therefore the second summand in (3.28) is $\ll \frac{|w|_0 |\lambda|^{3n/2}}{\Delta} (r^{-1}|u|)^\varepsilon r|u|^{1-\frac{n}{2}}$.

Putting the two estimates together, we obtain

$$I(r; u) \ll_\varepsilon \frac{|w|_0 |\lambda|^{\frac{3n}{2}}}{\Delta} (r^{-1}|u|)^\varepsilon r|u|^{1-\frac{n}{2}} + \frac{|w|_N}{\sqrt{\Delta}} (r^{-1}|u|)^\varepsilon r|u|^{1-\frac{n}{2}},$$

which is sufficient for the proposition. $\qquad\qquad\square$

As usual, from (3.9) we obtain the following bound:

Lemma 3.2.14 (Third estimate for $I_q(c)$). *Suppose $q \leq \sqrt{m}|c|$, and $\varepsilon \in \left(0, \frac{n}{2}\right)$. Let N be an integer such that $N \geq \frac{3n^2}{2\varepsilon}$. Then we have*

$$I_q(c) \ll_\varepsilon \left(\frac{|w|_0 |\lambda|^{\frac{3n}{2}(1-\varepsilon/n)^{-1}}}{\Delta} + \frac{|w|_N}{\sqrt{\Delta}} \right) m^{\frac{n}{2}} \left(\frac{m|c|}{q^2} \right)^\varepsilon \left(\frac{\sqrt{m}|c|}{q} \right)^{1-\frac{n}{2}}.$$

§3.3 The Singular Integral

In this section we specialize the treatment of the integrals $I_q(c)$ to the case $c = 0$, which is where the singular integral, defined for example in (3.1), comes from. This is where the assumption that our weights are G-admissible will reveal its full potential: it will play a key role in the following central technical assertion.

Proposition 3.3.1. *With $\sigma_\infty(F^{(0)}, w)$ defined as in (3.1), we have*

$$\sigma_\infty(F^{(0)}, w) = \int_{\mathbb{R}^{n-1}} \frac{w(x^*)}{\left(\frac{\partial G}{\partial x_1}(x^*) \right)} dy$$

where y runs over the projections onto the last n coordinates of vectors in $\mathrm{supp}(w)$, and x^* is defined as in Definition 3.1.1(iv) for some x that projects to y.

Proof. We prove that

$$\frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w(x) dx = \int_{\mathbb{R}^{n-1}} \frac{w(x^*)}{\left(\frac{\partial G}{\partial x_1}(x^*) \right)} dy + O_{G,w}(\varepsilon)$$

from which the result follows immediately. Note that the implied constants in the error term above are allowed to depend on G and w. This does not cause problems, since the rate of convergence of the left hand side as $\varepsilon \to 0$ will not be of interest to us.

First observe that, for any x, the condition $|G(x)| \leq \varepsilon$ implies $|G(x) - G(x^*)| \leq \varepsilon$; by the Mean Value Theorem we have

$$|G(x) - G(x^*)| = \left| \frac{\partial G}{\partial x_1}(\xi) \right| \cdot |x - x^*|$$

for some ξ in the segment connecting x and x^* and since the partial derivative above is $\geq \rho$, by the admissibility condition, it follows that $|x - x^*| \ll_{G,w} \varepsilon$. We then have (for example by the Mean Value Theorem, since the derivatives of w are bounded from above) $w(x) = w(x^*) + O_{G,w}(\varepsilon)$. We conclude that

$$\frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w(x) dx = \frac{1}{2\varepsilon} \int_{\substack{|G(x)| \leq \varepsilon \\ x \in \mathrm{supp}(w)}} w(x^*) + O_{G,w} \left(\int_{|G(x)| \leq \varepsilon} 1 dx \right). \qquad (3.29)$$

We note that, for fixed $x_2, \ldots, x_n$, the values of x_1 for which $|G(x)| \leq \varepsilon$ range over an interval of length $O_{G,w}(\varepsilon)$. Indeed, if x_1 and x_1' are two such choices, then setting $x' = (x_1', x_2, \ldots, x_n)$ we have

$$2\varepsilon \geq |G(x) - G(x')| = \left| \frac{\partial G}{\partial x_1}(\xi) \right| \cdot |x_1 - x_1'| \geq \rho |x_1 - x_1'|$$

for some ξ in the segment connecting x and x', whence $|x_1 - x_1'| \leq_{G,w} \varepsilon$. It follows that the last summand in (3.29) is $O_{G,w}(\varepsilon)$, since the other coordinates range over intervals of length $O_w(1)$. We obtain

$$\frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w(x) dx = \frac{1}{2\varepsilon} \int_{\substack{|G(x)| \leq \varepsilon \\ x \in \mathrm{supp}(w)}} w(x^*) + O_{G,w}(\varepsilon). \tag{3.30}$$

We now observe that, by Taylor's Theorem, we have

$$G(x) = (x_1 - x_1^*) \frac{\partial G}{\partial x_1}(x^*) + O_{G,w}(\varepsilon^2)$$

since the second partial derivatives of G are bounded in $\mathrm{supp}(w)$. Fix now $y = (x_2, \ldots, x_n)$ (recall that x^* only depends on y). Then the condition $|G(x_1, y)| \leq \varepsilon$ is equivalent to x_1 lying on some set I_y of measure

$$\frac{2\varepsilon}{\frac{\partial G}{\partial x_1}(x^*)} + \frac{O_{G,w}(\varepsilon^2)}{\frac{\partial G}{\partial x_1}(x^*)} = \frac{2\varepsilon}{\frac{\partial G}{\partial x_1}(x^*)} + O_{G,w}(\varepsilon^2) \tag{3.31}$$

where in the last equality we used again that the partial derivative which occurs in the denominator is $\geq \rho$. We now prove that we have, for each fixed y

$$\frac{1}{2\varepsilon} \int_{\substack{|G(x)| \leq \varepsilon \\ x \in \mathrm{supp}(w)}} w(x^*) dx_1 = \frac{w(x^*)}{\frac{\partial G}{\partial x_1}(x^*)} + O_{G,w}(\varepsilon), \tag{3.32}$$

after which the result will follow from (3.30). For this we see two cases.

<u>Case 1:</u> $(x_1, y) \in \mathrm{supp}(w)$ for every $x \in I_y$.

Then the condition that x_1 ranges over a set of measure given by (3.31) implies

$$\frac{1}{2\varepsilon} \int_{\substack{|G(x)| \leq \varepsilon \\ x \in \mathrm{supp}(w)}} w(x^*) dx_1 = \frac{1}{2\varepsilon} w(x^*) \left(\frac{2\varepsilon}{\frac{\partial G}{\partial x_1}(x^*)} + O_{G,w}(\varepsilon^2) \right)$$

which implies (3.32).

<u>Case 2:</u> There is some $x_1' \in I_y$ for which $(x_1', y) \notin \mathrm{supp}(w)$.

We have argued before that the condition $|G(x)| \leq \varepsilon$ prescribes an interval of length $O_{G,w}(\varepsilon)$ for x_1, and hence $x_1 = x_1' + O_{G,w}(\varepsilon)$. Since the first partial derivative of w is bounded from above, it follows from a straightforward application of the Mean Value Theorem that $w(x_1, y) = w(x_1', y) + O_{G,w}(\varepsilon)$. But $w(x_1', y) = 0$ since by assumption (x_1', y) lies outside $\mathrm{supp}(w)$. It follows that $w(x_1, y) = O_{G,w}(\varepsilon)$. This readily implies (again using that the values of x_1 for which $|G(x_1, y)| \leq \varepsilon$ range over an interval of length $O_{G,w}(\varepsilon)$) that

$$\frac{1}{2\varepsilon} \int_{\substack{|G(x)| \leq \varepsilon \\ x \in \mathrm{supp}(w)}} w(x^*) dx_1 \quad \text{and} \quad \frac{w(x^*)}{\frac{\partial G}{\partial x_1}(x^*)}$$

are *both* $O_{G,w}(\varepsilon)$, and then (3.32) trivially holds. $\qquad\square$

We are now ready to prove the main result of this section.

Lemma 3.3.2. *We have*

$$I_q(0) = m^{\frac{n}{2}} \left(\sigma_\infty(G, w) + O_N \left(\frac{|w|_{2N+1}}{\sqrt{\Delta}} \left(\frac{q}{\sqrt{m}} \right)^N \right) \right).$$

Proof. We use (3.8), which reduces the statement of the Lemma to

$$\int_{\mathbb{R}^n} w(x) h(r, G(x)) dx = \sigma_\infty(F^{(0)}, w) + O_N \left(\frac{|w|_{2N+1}}{\sqrt{\Delta}} r^N \right), \tag{3.33}$$

where $r = q/\sqrt{m}$. We have already seen that $h(r, G(x))$ vanishes identically on $\mathrm{supp}(w)$ if $r \geq 1$, hence we may assume $r < 1$. Now substitute $y = G(x)$ on the left hand side of (3.33). The determinant of the variable change $(x_1, x_2, \ldots, x_n) \mapsto (y, x_2, \ldots, x_n)$ is $\partial x_1 / \partial y$. Differentiating the relation $G(x_1, \ldots, x_n) = y$ with respect to y, we arrive at

$$\frac{\partial G}{\partial x_1} \cdot \frac{\partial x_1}{\partial y} = 1$$

whence this determinant is also equal to $(\partial G / \partial x_1)^{-1}$. This variable change implies that the left hand side of (3.33) equals

$$\int \frac{w(x)}{\frac{\partial G}{\partial x_1}(x)} dy \, dx_2 \cdots dx_n = \int_{\mathbb{R}} I(y) h(r, y) dy$$

where

$$I(y) = \int \frac{w(x)}{\frac{\partial G}{\partial x_1}(x)} dz;$$

in the last integral, dz stands for $dx_2 \cdots dx_n$ and $x_2, \ldots, x_n$ run over all $(n-1)$-tuples of real numbers such that $(x_1', x_2, \ldots, x_n)$ is in $\mathrm{supp}(w)$ for some x_1'; x_1 is defined via the equation $G(x_1, \ldots, x_n) = y$ (note that this equation in x_1 does not have more than one solution in $\mathrm{supp} w$, since there is at most one positive solution and $x_1 > 0$ in $\mathrm{supp}(w)$). Proposition 3.3.1 gives $I(0) = \sigma_\infty(F^{(0)}, w)$. We will apply Lemma 2.2.12 to $f(y) = I(y)$, by finding appropriate values of B and $B_0, \ldots, B_{2N+1}$.

We have

$$\frac{\partial^j}{\partial y^j} I(y) = \int \frac{\partial^j}{\partial y^j} \frac{w(x)}{2\lambda_1 x_1} dz.$$

As we said before, if $(x_2, \ldots, x_n)$ is in the range of integration then $(x_1', x_2, \ldots, x_n)$ is in $\mathrm{supp}(w)$ for some $x^\star$. This implies $|G(x_1', x_2, \ldots, x_n)| \leq \frac{1}{2}$, and thus

$$\lambda_1 (x_1')^2 + \lambda_2 x_2^2 + \cdots + \lambda_n x_n^2 \leq \frac{3}{2}$$

whence $x_j \ll \frac{1}{\sqrt{\lambda_j}}$ for $j = 2, \ldots, n$. It follows that the volume of the range of integration is $\ll \frac{1}{\sqrt{\lambda_2 \cdots \lambda_n}}$. It now suffices to bound each $\frac{\partial^j}{\partial y^j} \frac{w(x)}{2\lambda_1 x_1}$ uniformly in y. We begin by observing that, by differentiating the equation $\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 - 1 = y$ with respect to y, we get $2\lambda_1 x_1 \frac{\partial}{\partial y} x_1 = 1$. Therefore $\frac{\partial^j}{\partial y^j} \frac{w(x)}{2\lambda_1 x_1} = \frac{\partial^j}{\partial y^j} \left(w(x) \frac{\partial x_1}{\partial y} \right)$. Then Leibniz' formula yields

$$\frac{\partial^j}{\partial y^j} \frac{w(x)}{2\lambda_1 x_1} \ll \sum_{k=0}^{j} \frac{\partial^k w(x)}{\partial y^k} \frac{\partial^{j-k+1} x_1}{\partial y^{j-k+1}}. \tag{3.34}$$

The factor on the right is readily computable; by induction we see that $\frac{\partial^s x_1}{\partial y^s} = \frac{1}{c_s \lambda_1^s x_1^{2s-1}}$ for some constant c_s. In fact, this is clear for $s = 1$, and for the induction step observe that

$$\frac{\partial^{s+1} x_1}{\partial y^s} = \frac{\partial}{\partial y} \frac{1}{c_s \lambda_1^s x_1^{2s-1}} = \frac{\partial x_1}{\partial y} \frac{1}{-(2s-1)c_s \lambda_1^s x_1^{2s}} = \frac{1}{-(2s-1)c_s \lambda_1^{s+1} x_1^{2s+1}}$$

where we used again $\frac{\partial x_1}{\partial y} = 2\lambda_1 x_1$, and hence we may take $c_{s+1} = -(2s-1)c_s$. We then have $\frac{\partial^s x_1}{\partial y^s} \ll \frac{1}{\lambda_1^s x_1^{2s-1}} = \frac{x_1}{(\lambda_1 x_1^2)^s}$. But by assumption we have $\lambda_1 x_1^2 \gg 1$ (this is part of the admissibility condition), whence

$$\frac{\partial^s x_1}{\partial y^s} \ll x_1. \tag{3.35}$$

We now turn to estimates for $\frac{\partial^k w(x)}{\partial y^k}$. Observe that, as a function of y, $w(x)$ is the composite of $w(\cdot, x_2, \ldots, x_n)$ and x_1, whence $\frac{\partial^k w(x)}{\partial y^k}$ can be computed by iterated applications of the Chain Rule. Straightforward induction shows that

$$\frac{\partial^k w(x)}{\partial y^k} = \sum_{\substack{i_1 + \cdots + i_r = k \\ i_1, \ldots, i_r \geq 1}} C_{i_1, \ldots, i_k} \frac{\partial^{i_1} x_1}{\partial y^{i_1}} \cdots \frac{\partial^{i_r} x_1}{\partial y^{i_r}}$$

where $i_1, \ldots, i_r$ are positive integers, and each $C_{i_1, \ldots, i_k}$ is some linear combination of terms of the form $\frac{\partial^i w}{\partial x_1^i}(x_1, \ldots, x_n)$ for some $i \leq k$. From this description it is clear that $C_{i_1, \ldots, i_r} \ll |w|_k$, and hence

$$\frac{\partial^k w(x)}{\partial y^k} \ll |w|_k \sum_{\substack{i_1 + \cdots + i_r = k \\ i_1, \ldots, i_r \geq 1}} \frac{\partial^{i_1} x_1}{\partial y^{i_1}} \cdots \frac{\partial^{i_r} x_1}{\partial y^{i_r}}.$$

Using (3.35), we get

$$\frac{\partial^k w(x)}{\partial y^k} \ll |w|_k \sum_{\substack{i_1 + \cdots + i_r = k \\ i_1, \ldots, i_r \geq 1}} x_1^r.$$

Since $x_1 \ll \frac{1}{\sqrt{\lambda_1}} \ll 1$, each x_1^r is $\ll 1$, and it follows that

$$\frac{\partial^k w(x)}{\partial y^k} \ll |w|_k. \tag{3.36}$$

We have now everything we need in order to estimate (3.34). Using (3.35) and (3.36),

$$\frac{\partial^j}{\partial y^j} \frac{w(x)}{2\lambda_1 x_1} \ll \sum_{k=0}^{j} |w|_k x_1 \ll |w|_j x_1 \ll \frac{|w|_j}{\sqrt{\lambda_1}}.$$

This shows that we may take $B_j \ll \frac{1}{\sqrt{\lambda_2 \cdots \lambda_n}} |w|_j \frac{1}{\sqrt{\lambda_1}} \ll \frac{|w|_j}{\sqrt{\Delta}}$ for $j = 1, 2, \ldots, 2N+1$. In order to find a suitable value for B, we note that if $I(y) \neq 0$ then the equation $G(x) = y$ has at least one solution in $\text{supp} w$. This implies $|y| \leq \frac{1}{2}$, since $|G| \leq \frac{1}{2}$ on $\text{supp} w$. We can therefore take $B = \frac{1}{2}$. Now we see that

$$B_0 B + B_0 + B_1 + \cdots + B_{2N+1} \ll \sum_{j=0}^{2N+1} \frac{|w|_j}{\sqrt{\Delta}}$$

$$\ll \frac{|w|_{2N+1}}{\sqrt{\Delta}}$$

and the result follows from Lemma 2.2.12. $\square$

§**3.4** The sums $S_q(c)$

In this section we turn to the study of the exponential sums $S_q(c)$, defined by

$$S_q(c) = \sum_{a \,(\mathrm{mod}\, q)}^{*} \sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{aF(b) + c \cdot b}{q}\right).$$

Note that, as opposed to the integrals $I_q(c)$, the sums $S_q(c)$ do not depend on the weight w. We begin with the following easy statement.

Proposition 3.4.1. *If u and v are coprime integers, then we have*

$$S_{uv}(c) = S_u(\overline{v}c)S_v(\overline{u}c)$$

where $\overline{v}$ and $\overline{u}$ stand for the multiplicative inverses of v and u modulo u and v, respectively.

Proof. We note the general equality

$$\frac{\overline{u}}{v} + \frac{\overline{v}}{u} \equiv \frac{1}{uv} \pmod 1.$$

With this in mind, we write

$$S_{uv}(c) = \sum_{a \,(\mathrm{mod}\, uv)}^{*} \sum_{b \,(\mathrm{mod}\, uv)} e\left(\frac{aF(b) + c \cdot b}{uv}\right)$$

$$= \sum_{a \,(\mathrm{mod}\, uv)}^{*} \sum_{b \,(\mathrm{mod}\, uv)} e\left(\frac{\overline{v}(aF(b) + c \cdot b)}{u} + \frac{\overline{u}(aF(b) + c \cdot b)}{v}\right)$$

Now the Chinese Remainder Theorem gives us an isomorphism of rings $\mathbb{Z}/u\mathbb{Z} \times \mathbb{Z}/v\mathbb{Z} \to \mathbb{Z}/uv\mathbb{Z}$, which maps (b_1, b_2) to $u\overline{u}b_2 + v\overline{v}b_1$. Writing $b = u\overline{u}b_2 + v\overline{v}b_1$ in the sum above, we obtain

$$S_{uv}(c) = \sum_{\substack{a \,(\mathrm{mod}\, uv) b_1 \,(\mathrm{mod}\, u) \\ b_2 \,(\mathrm{mod}\, v)}}^{*} \sum e\left(\frac{\overline{v}(aF(b_1) + c \cdot v\overline{v}b_1)}{u} + \frac{\overline{u}(aF(b_2) + c \cdot u\overline{u}b_2)}{v}\right)$$

$$= \sum_{\substack{a \,(\mathrm{mod}\, uv) b_1 \,(\mathrm{mod}\, u) \\ b_2 \,(\mathrm{mod}\, v)}}^{*} \sum e\left(\frac{\overline{v}aF(b_1) + \overline{v}c \cdot b_1}{u} + \frac{\overline{u}aF(b_2) + \overline{u}c \cdot b_2}{v}\right).$$

Now for any pair of units $a_1 \in (\mathbb{Z}/u\mathbb{Z})^*$ and $a_2 \in (\mathbb{Z}/v\mathbb{Z})^*$ there exists a unique $a \in (\mathbb{Z}/uv\mathbb{Z})^*$ such that $\overline{v}a \equiv a_1 \pmod u$ and $\overline{u}a \equiv a_2 \pmod v$. Therefore the above yields

$$S_{uv}(c) = \sum_{\substack{a_1 \,(\mathrm{mod}\, u) b_1 \,(\mathrm{mod}\, u) \\ a_2 \,(\mathrm{mod}\, v) b_2 \,(\mathrm{mod}\, v)}}^{*} \sum e\left(\frac{a_1 F(b_1) + \overline{v}c \cdot b_1}{u} + \frac{a_2 F(b_2) + \overline{u}c \cdot b_2}{v}\right)$$

$$= \sum_{a_1 \,(\mathrm{mod}\, u) b_1 \,(\mathrm{mod}\, u)}^{*} \sum e\left(\frac{a_1 F(b_1) + \overline{v}c \cdot b_1}{q}\right) \sum_{a_2 \,(\mathrm{mod}\, v) b_2 \,(\mathrm{mod}\, v)}^{*} \sum e\left(\frac{a_2 F(b_2) + \overline{u}c \cdot b_2}{q}\right)$$

$$= S_u(\overline{v}c)S_v(\overline{u}c)$$

as desired. $\square$

    This proposition will essentially allow us to reduce the task of bounding $S_q(c)$ to the case in which q is a prime power. We give now our first, most naive bound.

Lemma 3.4.2. *We have*

$$S_q(c) \ll \Delta^{\frac{1}{2}} q^{\frac{n}{2}+1}.$$

Proof. We first observe that, for any $z_1, \ldots, z_k \in \mathbb{C}$, we have

$$|z_1 + \cdots + z_k|^2 \le (|z_1| + \cdots + |z_k|)^2 \le k(|z_1|^2 + \cdots + |z_k|^2),$$

where the first inequality is the triangle inequality, and the second one follows from the Cauchy-Schwarz inequality. This yields

$$|S_q(c)|^2 \le \varphi(q) \sum_{a \,(\mathrm{mod}\, q)}^{*} \left| \sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{aF(b) + c \cdot b}{q} \right) \right|^2$$

$$= \varphi(q) \sum_{\substack{a \,(\mathrm{mod}\, q) \, b_1 \,(\mathrm{mod}\, q) \\ b_2 \,(\mathrm{mod}\, q)}}^{*} e\left(\frac{a(F(b_1) - F(b_2)) + c \cdot (b_1 - b_2)}{q} \right).$$

We now set $b_1 = b + h$ and $b_2 = b$. It is clear that

$$F(b + h) - F(b) = F^{(0)}(h) + b \cdot \nabla F(h)$$

and hence

$$|S_q(c)|^2 \le \varphi(q) \sum_{\substack{a \,(\mathrm{mod}\, q) \, b \,(\mathrm{mod}\, q) \\ h \,(\mathrm{mod}\, q)}}^{*} e\left(\frac{a(F^{(0)}(h) + b \cdot \nabla F(h)) + c \cdot h}{q} \right)$$

$$= \varphi(q) \sum_{a \,(\mathrm{mod}\, q) \, h \,(\mathrm{mod}\, q)}^{*} e\left(\frac{aF^{(0)}(h) + c \cdot h}{q} \right) \sum_{b \,(\mathrm{mod}\, q)} e\left(\frac{a\nabla F(h) \cdot b}{q} \right).$$

If some entry of $\nabla F(h)$ is not divisible by q, then the innermost sum equals 0; otherwise, it equals q^n. We obtain

$$|S_q(c)|^2 \le \varphi(q) q^n \sum_{\substack{a \,(\mathrm{mod}\, q) \, h \,(\mathrm{mod}\, q) \\ q | \nabla F(h)}}^{*} e\left(\frac{aF^{(0)}(h) + c \cdot h}{q} \right)$$

$$\le \varphi(q)^2 q^n \#\{h \,(\mathrm{mod}\, q) : q \mid \nabla F(h)\}.$$

We now count vectors $h \in (\mathbb{Z}/q\mathbb{Z})^n$ such that q divides $\nabla F(h)$. We have $\nabla F(h) = (2\lambda_1 h_1, \ldots, 2\lambda_n h_n)$. The condition that $q \mid 2\lambda_j h_j$ is equivalent to

$$\frac{q}{(q, 2\lambda_j)} \mid h_j$$

and hence the number of $h_j \in \mathbb{Z}/q\mathbb{Z}$ satisfying this is $(q, 2\lambda_j)$. We obtain

$$\#\{h \,(\mathrm{mod}\, q) : q \mid \nabla F(h)\} = (q, 2\lambda_1) \cdots (q, 2\lambda_n) \le (2\lambda_1) \cdots (2\lambda_n) \ll \Delta$$

implying

$$|S_q(c)|^2 \ll \varphi(q)^2 q^n \Delta \ll \Delta q^{n+2}$$

which establishes the result.

$\square$

Our next result exploits the diagonal structure of F in order to obtain a better bound for $S_q(c)$ when q is a prime. In order to state and prove this result we need to present a definition and recall some well-known bounds.

Definition 3.4.3. Define the quadratic form H by

$$H(c) = \frac{c_1^2}{\lambda_1} + \cdots + \frac{c_n^2}{\lambda_n}.$$

Note that when p is a prime with $p \nmid \lambda_1, \ldots, \lambda_n$ and $c \in \mathbb{Z}^n$ it makes sense to evaluate $H(c)$ modulo p.

Fact 3.4.4 (Gauss Sums)**.** Let p be a prime and γ be an integer such that $p \nmid \gamma$. We then have

$$\sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{\gamma x^2}{p}\right) = \left(\frac{\gamma}{p}\right) \tau_p$$

where $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$, so that in particular $|\tau_p| = \sqrt{p}$.

Fact 3.4.5 (Kloosterman Sums)**.** Let p be a prime. For two integers α and β, define the *Kloosterman Sum*

$$K(\alpha, \beta; p) = \sum_{a \,(\mathrm{mod}\, p)}^{*} e\left(\frac{\alpha a + \beta \bar{a}}{p}\right),$$

where as usual $\bar{a}$ stands for the multiplicative inverse of a modulo p. Then if $p \nmid \alpha, \beta$ we have

$$|K(\alpha, \beta; p)| < 2\sqrt{p}.$$

Fact 3.4.6 (Salié Sums)**.** Let p be a prime. For two integers α and β, define the *Salié Sum*

$$K^{\star}(\alpha, \beta; p) = \sum_{a \,(\mathrm{mod}\, p)}^{*} \left(\frac{a}{p}\right) e\left(\frac{\alpha a + \beta \bar{a}}{p}\right).$$

Then we have

$$|K^{\star}(\alpha, \beta; p)| < 2\sqrt{p}.$$

We are now ready to embark on our next result.

Lemma 3.4.7. *Let p be a prime such that $p \nmid \Delta$. We then have*

$$S_p(c) \ll p^{\frac{n+1}{2}}$$

except when n is even and p divides m and $H(c)$. Moreover, we have the following explicit formulas for $S_p(c)$ when p divides m or $H(c)$:

- *If n is even, then*

$$S_p(c) = \begin{cases} -\left(\frac{(-1)^{\frac{n}{2}} \lambda_1 \cdots \lambda_n}{p}\right) p^{\frac{n}{2}} & \text{if } p \text{ divides one of } m, H(c) \text{ but not both} \\[2mm] \left(\frac{(-1)^{\frac{n}{2}} \lambda_1 \cdots \lambda_n}{p}\right)(p-1)p^{\frac{n}{2}} & \text{if } p \text{ divides } m \text{ and } H(c) \end{cases} ;$$

- *If n is odd, then*

$$S_p(c) = \begin{cases} \left(\frac{(-1)^{\frac{n-1}{2}} \lambda_1 \cdots \lambda_n m}{p}\right) p^{\frac{n+1}{2}} & \text{if } p \text{ divides } H(c) \\[2mm] \left(\frac{(-1)^{\frac{n-1}{2}} \lambda_1 \cdots \lambda_n H(c)}{p}\right) p^{\frac{n+1}{2}} & \text{if } p \text{ divides } m \end{cases} .$$

Proof. We have, by definition,

$$
S_p(c) = \sum_{a=1}^{p-1} \sum_{b \,(\mathrm{mod}\, p)} e\left(\frac{a(\lambda_1 b_1^2 + \cdots + \lambda_n b_n^2 - m) + c_1 b_1 + \cdots + c_n b_n}{p} \right)
$$

$$
= \sum_{a=1}^{p-1} e\left(-\frac{am}{p} \right) \sum_{b_1 \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_1 b_1^2 + c_1 b_1}{p} \right) \cdots \sum_{b_n \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_n b_n^2 + c_n b_n}{p} \right). \qquad (3.37)
$$

We can evaluate each of the inner sums by using Fact 3.4.4. We have

$$
\sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_i x^2 + c_i x}{p} \right) = \sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_i x^2 + c_i x + \overline{4a\lambda_i} c_i^2}{p} \right) e\left(\frac{-\overline{4a\lambda_i} c_i^2}{p} \right)
$$

$$
= e\left(\frac{-\overline{4a\lambda_i} c_i^2}{p} \right) \sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_i x^2 + c_i x + \overline{4a\lambda_i} c_i^2}{p} \right)
$$

$$
= e\left(\frac{-\overline{4a\lambda_i} c_i^2}{p} \right) \sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_i (x + \overline{2a\lambda_i} c_i)^2}{p} \right)
$$

$$
= e\left(\frac{-\overline{4a\lambda_i} c_i^2}{p} \right) \sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{a\lambda_i x^2}{p} \right) = \left(\frac{a\lambda_i}{p} \right) e\left(\frac{-\overline{4a\lambda_i} c_i^2}{p} \right) \tau_p.
$$

Using (3.37) we conclude that

$$
S_p(c) = \sum_{a=1}^{p-1} e\left(\frac{-am}{p} \right) \left(\frac{a^n \lambda_1 \cdots \lambda_n}{p} \right) \tau_p^n e\left(\frac{-4\overline{a}(\overline{\lambda_1} c_1^2 + \cdots + \overline{\lambda_n} c_n^2)}{p} \right)
$$

$$
= \left(\frac{\lambda_1 \cdots \lambda_n}{p} \right) \tau_p^n \sum_{a=1}^{p-1} \left(\frac{a}{p} \right)^n e\left(\frac{-am - \overline{a} \sum_{i=1}^{n} \overline{4\lambda_i} c_i^2}{p} \right)
$$

$$
= \left(\frac{\lambda_1 \cdots \lambda_n}{p} \right) \tau_p^n K_n\left(-m, -\frac{1}{4} H(c); p \right) \qquad (3.38)
$$

where $K_n = K$ if n is even and $K_n = K^\star$ if n is odd[1]. Using Fact 3.4.5 or Fact 3.4.6 according to whether n is even or odd, respectively, as well as the fact that $|\tau_p| = \sqrt{p}$, it follows immediately that, if p does not divide m nor $H(c)$, then $S_p(c) \ll p^{\frac{n+1}{2}}$.

Now, if n is even and p divides exactly one of m and $H(c)$, then

$$
K_n\left(-m, -\frac{1}{4} H(c); p \right) = \sideset{}{^*}\sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{x}{p} \right) = -1
$$

and since $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$, we have $\tau_p^n = (\tau_p^2)^{\frac{n}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{n}{2}} p^{\frac{n}{2}}$, and it follows from (3.38) that

$$
S_p(c) = \left(\frac{\lambda_1 \cdots \lambda_n}{p} \right) (-1)^{\frac{p-1}{2} \cdot \frac{n}{2}} p^{\frac{n}{2}} (-1) = -\left(\frac{(-1)^{\frac{n}{2}} \lambda_1 \cdots \lambda_n}{p} \right) p^{\frac{n}{2}}
$$

as desired. If m divides *both* m and $H(c)$, then the Kloosterman sum becomes

$$
\sideset{}{^*}\sum_{x \,(\mathrm{mod}\, p)} 1 = p - 1
$$

---

[1]There is a slight abuse of notation here. The expression $K_n\left(-m, -\frac{1}{4} H(c); p \right)$ must be interpreted as $K_n(-m, b; p)$ where b is some integer such that $b \equiv -\frac{1}{4} H(c) \pmod{p}$.

and the rest of the computation goes unchanged, so we get

$$S_p(c) = \left(\frac{(-1)^{\frac{n}{2}} \lambda_1 \cdots \lambda_n}{p} \right) (p-1) p^{\frac{n}{2}}$$

which is also what we wanted.

If n is odd, and p divides $H(c)$ but does not divide m, the Salié Sum K_n becomes

$$\sum_{a \,(\mathrm{mod}\, p)} \left(\frac{a}{p} \right) e\left(\frac{-am}{p} \right) = \sum_{a \,(\mathrm{mod}\, p)} \left(1 + \left(\frac{a}{p} \right) \right) e\left(\frac{-am}{p} \right)$$

simply because $\sum_{(\mathrm{mod}\, p)} e(-am/p) = 0$. Note that $1 + \left(\frac{a}{p} \right)$ is precisely the number of solutions in $\mathbb{Z}/p\mathbb{Z}$ to the equation $x^2 = a$. Hence

$$K_n\left(-m, -\frac{1}{4} H(c); p \right) = \sum_{a \,(\mathrm{mod}\, p)} \#\{ x \,(\mathrm{mod}\, p) : x^2 \equiv a \,(\mathrm{mod}\, p) \} e\left(\frac{-am}{p} \right)$$

$$= \sum_{x \,(\mathrm{mod}\, p)} e\left(\frac{-mx^2}{p} \right) = \left(\frac{-m}{p} \right) \tau_p$$

by Fact 3.4.4. This, together with (3.38), implies the desired formula for $S_p(c)$, in light of the equality

$$\tau_p^{n+1} = (\tau_p^2)^{\frac{n+1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{n+1}{2}} p^{\frac{n+1}{2}} = \left(\frac{-1}{p} \right)^{\frac{n+1}{2}} p^{\frac{n+1}{2}}.$$

The case when p divides $H(c)$ but does not divide m is similar: in this case the Salié Sum K_n becomes

$$\sum_{a \,(\mathrm{mod}\, p)} \left(\frac{a}{p} \right) e\left(\frac{-a\overline{4}H(c)}{p} \right) = \left(\frac{-H(c)}{p} \right) \tau_p$$

by a completely analogous computation, in which the roles of m and $\frac{1}{4} H(c)$ are reversed. Again this implies the desired formula for $S_p(c)$. Finally, if p divides *both* m and $H(c)$, the Salié Sum equals 0, so $S_p(c) = 0$, which is consistent with our result. $\qquad\square$

We now move towards estimation of the partial sums

$$\sum_{q \leq X} S_q(c),$$

which will be needed later. By Lemma 3.4.2 we immediately see that

$$\sum_{q \leq X} S_q(c) \ll \Delta^{\frac{1}{2}} \sum_{q \leq X} q^{\frac{n}{2}+1} \leq \Delta^{\frac{1}{2}} \sum_{q \leq X} X^{\frac{n}{2}+1} = \Delta^{\frac{1}{2}} X^{\frac{n}{2}+2}.$$

It turns out, however, that we can do better, by taking advantage of the multiplicative property given by Proposition 3.4.1 and the finer estimate for $S_p(c)$ when p is a prime given by Lemma 3.4.7. The general strategy will be to decompose each integer q as a product of a square-free part and a square-full[2] part. We then estimate the exponential sum arising from the square-free part using Lemma 3.4.7 and the one arising from the square-full part using Lemma 3.4.2. Since this second bound is worse, we would like some upper bounds regarding the distribution of square-full numbers, which we develop now.

---

[2] A positive integer v is called *square-full* if for every prime p dividing v, p^2 also divides v.

Proposition 3.4.8. *The number of square-full integers x satisfying $1 \le x \le N$ is $O(\sqrt{N})$.*

Proof. We first note that every square-full number can be written as $u^3 v^2$, where u and v are positive integers. Indeed, if x is square-full, write

$$x = \prod_{i=1}^{r} p_i^{2\alpha_i} \prod_{j=1}^{s} q_i^{2\beta_j + 1}$$

where the p_i's and q_j's are distinct primes. The square-full property ensures that $\beta_j \ge 1$ for each j, and therefore we can take

$$u = \prod_{j=1}^{s} q_i \quad \text{and} \quad v = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} q_j^{\beta_j - 1}.$$

Now this implies

$$
\begin{aligned}
\#\{1 \le x \le N : x \text{ square-full}\} &\le \#\{(u,v) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : u^3 v^2 \le N\} \\
&= \sum_{u=1}^{\infty} \#\{v \in \mathbb{Z}^+ : u^3 v^2 \le N\} \\
&\le \sum_{u=1}^{\infty} \sqrt{\frac{N}{u^3}} = \left(\sum_{u=1}^{\infty} \frac{1}{u^{\frac{3}{2}}} \right) \sqrt{N}.
\end{aligned}
$$

The above sum converges, and we are done. $\qquad\square$

Corollary 3.4.9. *We have*

$$\sum_{\substack{1 \le x \le N \\ x \text{ square-full}}} \frac{1}{\sqrt{x}} \ll \log(N).$$

Proof. Let k be the smallest integer such that $2^k \ge N$. For each j with $0 \le j \le k$, there are $O(\sqrt{2^j})$ square-full numbers $x \le 2^j$ by Proposition 3.4.8, and in particular there are $O(\sqrt{2^j})$ square-full numbers x with $2^{j-1} < x \le 2^j$. This implies that

$$\sum_{\substack{2^{j-1} < x \le 2^j \\ x \text{ square-full}}} \frac{1}{\sqrt{x}} \le \sum_{\substack{2^{j-1} < x \le 2^j \\ x \text{ square-full}}} \frac{1}{\sqrt{2^{j-1}}} \ll \sqrt{2^j} \cdot \frac{1}{\sqrt{2^{j-1}}} = \sqrt{2} = O(1).$$

Hence

$$\sum_{\substack{1 \le x \le N \\ x \text{ square-full}}} \frac{1}{\sqrt{x}} \le \sum_{j=0}^{k} \sum_{\substack{2^{j-1} < x \le 2^j \\ x \text{ square-full}}} \frac{1}{\sqrt{x}} \ll \sum_{j=0}^{k} 1 \ll k.$$

Since obviously $k \ll \log(N)$, we are done. $\qquad\square$

We will also need an easy statement concerning sums of gcd's.

Proposition 3.4.10. *For any positive integers N and k, we have*

$$\sum_{j=1}^{N} (j, k) \le N\tau(k)$$

where $\tau(k)$ stands for the number of divisors of k.

Proof. Each (j, k) is a divisor of k by definition, hence

$$\sum_{j=1}^{N}(j, k) = \sum_{d|k} d\#\{1 \le j \le N : (j, k) = d\}.$$

Now when $(j, k) = d$ we must have $d \mid j$, and hence the cardinality above is at most N/d. It follows that

$$\sum_{j=1}^{N}(j, k) \le \sum_{d|k} d \cdot \frac{N}{d} = N\sum_{d|k} 1 = N\tau(k).$$

$\square$

We are now ready to state and prove our estimate for the partial sums of $S_q(c)$.

Lemma 3.4.11. *We have*

$$\sum_{q \le X} |S_q(c)| \ll_\varepsilon \Delta^{\frac{n+4}{2}} X^{\frac{n+3}{2}+\varepsilon} m^\varepsilon.$$

Proof. Each positive integer q can be written uniquely in the form uv, where u and v are coprime integers, u is square-free and v is square-full. This implies, by Proposition 3.4.1, $S_q(c) = S_u(\overline{v}c)S_v(\overline{u}c)$; we estimate each factor separately.

For the latter, we simply remark that by Lemma 3.4.2 we have $S_v(\overline{u}c) \ll \Delta^{\frac{1}{2}}v^{\frac{n}{2}+1}$.

For the former, let $d = (u, \Delta)$, and write $u = dp_1 \cdots p_k$, where $p_1, \ldots, p_k$ are distinct primes. Note that $d, p_1, \ldots, p_k$ are pairwise coprime, and that by construction none of the p_j's divide Δ. Now iterated application of Proposition 3.4.1 yields

$$S_u(\overline{v}c) = S_d(rc)S_{p_1}(r_1 c) \cdots S_{p_k}(r_k c) \tag{3.39}$$

for some integers $r, r_1, \ldots, r_k$ whose value will not be relevant. By Lemma 3.4.2, we have

$$S_d(rc) \ll \Delta^{\frac{1}{2}}d^{\frac{n}{2}+1} \le \Delta^{\frac{1}{2}}\Delta^{\frac{n}{2}+1} = \Delta^{\frac{n+3}{2}} \tag{3.40}$$

since d divides Δ. Now, since each p_j does not divide Δ, we know from Lemma 3.4.7 that $S_{p_j}(r_j c) \ll p_j^{\frac{n+1}{2}}$, except potentially when n is even and p_j divides m; if that is the case, then the first exceptional case of Lemma 3.4.7 yields $S_{p_j}(r_j c) \ll p_j^{\frac{n}{2}+1}$. Therefore, in general, we have

$$S_{p_j}(r_j c) \ll p_j^{\frac{n+1}{2}}(p_j, m)^{\frac{1}{2}}$$

and taking the product over all j's we get

$$S_{p_1}(r_1 c) \cdots S_{p_k}(r_k c) \ll (p_1 \cdots p_k)^{\frac{n+1}{2}}(p_1 \cdots p_k, m) \ll u^{\frac{n+1}{2}}(u, m)^{\frac{1}{2}}. \tag{3.41}$$

The estimates (3.40) and (3.41) imply, by (3.39), that

$$S_u(\overline{v}c) \ll \Delta^{\frac{n+3}{2}}u^{\frac{n+1}{2}}(u, m)^{\frac{1}{2}}.$$

Putting together the estimates for $S_u(\overline{v}c)$ and $S_v(\overline{u}c)$ we get

$$S_q(c) \ll \Delta^{\frac{n+4}{2}}q^{\frac{n+1}{2}}v^{\frac{1}{2}}(u, m)^{\frac{1}{2}}$$

and summing over all $q \leq X$ yields

$$
\sum_{q \leq X} |S_q(c)| \ll \Delta^{\frac{n+4}{2}} \sum_{q \leq X} q^{\frac{n+1}{2}} v^{\frac{1}{2}} (u,m)^{\frac{1}{2}}
$$

$$
\leq \Delta^{\frac{n+4}{2}} X^{\frac{n+1}{2}} \sum_{\substack{uv \leq X \\ u \text{ square-free} \\ v \text{ square-full}}} v^{\frac{1}{2}} (u,m)^{\frac{1}{2}}
$$

$$
\leq \Delta^{\frac{n+4}{2}} X^{\frac{n+1}{2}} \sum_{\substack{v \leq X \\ v \text{ square-full}}} v^{\frac{1}{2}} \sum_{u \leq X/v} (u,m)^{\frac{1}{2}}. \tag{3.42}
$$

By Proposition 3.4.10, we have

$$
\sum_{u \leq X/v} (u,m)^{\frac{1}{2}} \leq \sum_{u \leq X/v} (u,m) \ll \frac{X}{v} \tau(m)
$$

and hence

$$
\sum_{\substack{v \leq X \\ v \text{ square-full}}} v^{\frac{1}{2}} \sum_{u \leq X/v} (u,m)^{\frac{1}{2}} \leq \sum_{\substack{v \leq X \\ v \text{ square-full}}} v^{\frac{1}{2}} \cdot \frac{X}{v} \tau(m)
$$

$$
= X\tau(m) \sum_{\substack{v \leq X \\ v \text{ square-full}}} \frac{1}{\sqrt{v}}
$$

$$
\ll X \log(X) \tau(m)
$$

by Corollary 3.4.9. Now (3.42) yields

$$
\sum_{q \leq X} |S_q(c)| \ll \Delta^{\frac{n+4}{2}} X^{\frac{n+3}{2}} \log(X) \tau(m).
$$

With this we are done, in light of the standard estimates $\log(X) \ll_\varepsilon X^\varepsilon$ and $\tau(m) \ll_\varepsilon m^\varepsilon$. $\qquad \square$

§3.5 The Singular Series

In this section we specialize the treatment of the sums $S_q(c)$ to the case $c = 0$. Our goal is to investigate the contribution of the summand corresponding to $c = 0$ to the expression for $N(F,w)$ given by Lemma 2.3.1; this summand is where the main term of the final result will come from. Taking into account Lemma 3.3.2, which gives an asymptotic formula for $I_q(0)$ the main term of which is constant with respect to q, it becomes natural to consider the sum

$$
\sum_{q=1}^{\infty} q^{-n} S_q(0),
$$

which we call the *singular series*.

Our first lemma describes how well the singular series can be approximated by its partial sums.

Lemma 3.5.1. *We have*

$$
\sum_{q=1}^{\infty} q^{-n} S_q(0) = \sum_{1 \leq q \leq X} q^{-n} S_q(0) + O_\varepsilon \left(\Delta^{\frac{n+4}{2}} X^{\frac{3-n}{2}+\varepsilon} m^\varepsilon \right).
$$

Moreover, the singular series converges absolutely.

Proof. We show that

$$\sum_{q>X} q^{-n}|S_q(0)| = O_\varepsilon\left(\Delta^{\frac{n+4}{2}} X^{\frac{3-n}{2}+\varepsilon} m^\varepsilon\right)$$

from which both assertions follow immediately.

For this, we define temporarily

$$S(X) = \sum_{1\le q\le X} |S_q(0)|$$

so that, for any positive integers $X < Y$, we have

$$\sum_{X<q\le Y} q^{-n}|S_q(0)| = \sum_{X<q\le Y} q^{-n}(S(q)-S(q-1))$$

$$= -(X+1)^{-n}S(X) + \sum_{X<q<Y}\left(q^{-n}-(q+1)^{-n}\right)S(q) + Y^{-n}S(Y). \quad (3.43)$$

By Lemma 3.4.11 and bounding $(X+1)^{-n}$ by X^{-n}, we have

$$(X+1)^{-n}S(X) \ll_\varepsilon X^{-n}\cdot\Delta^{\frac{n+4}{2}}X^{\frac{n+3}{2}+\varepsilon}m^\varepsilon = \Delta^{\frac{n+4}{2}}X^{\frac{3-n}{2}+\varepsilon}m^\varepsilon \quad (3.44)$$

and similarly

$$Y^{-n}S(Y) \ll_\varepsilon \Delta^{\frac{n+4}{2}}Y^{\frac{3-n}{2}+\varepsilon}m^\varepsilon \le \Delta^{\frac{n+4}{2}}X^{\frac{3-n}{2}+\varepsilon}m^\varepsilon. \quad (3.45)$$

We now observe that, by the Mean Value Theorem, we have $q^{-n}-(q+1)^{-n} \ll q^{-n-1}$. Therefore,

$$\sum_{X<q<Y}(q^{-n}-(q+1)^{-n})S(q) \ll \sum_{X<q<Y} q^{-n-1}S(q)$$

$$\ll_\varepsilon \Delta^{\frac{n+4}{2}}m^\varepsilon \sum_{X<q<Y} q^{\frac{1-n}{2}+\varepsilon} \quad \text{(by Lemma 3.4.11)}$$

$$< \Delta^{\frac{n+4}{2}}m^\varepsilon \int_X^Y t^{\frac{1-n}{2}+\varepsilon}dt$$

$$\ll \Delta^{\frac{n+4}{2}}m^\varepsilon\left(X^{\frac{3-n}{2}+\varepsilon} - Y^{\frac{3-n}{2}+\varepsilon}\right)$$

$$\le \Delta^{\frac{n+4}{2}}X^{\frac{3-n}{2}+\varepsilon}m^\varepsilon. \quad (3.46)$$

Putting together (3.44), (3.45), (3.46) we obtain, by (3.43),

$$\sum_{X<q\le Y} q^{-n}|S_q(0)| \ll_\varepsilon \Delta^{\frac{n+4}{2}}X^{\frac{3-n}{2}+\varepsilon}m^\varepsilon$$

and letting $Y\to\infty$ we obtain the wanted result. $\qquad\square$

It is in the study of the singular series that the p-adic densities σ_p which appear in our statements, for example in the statement of Theorem 3.0.1, show up. In fact the singular series turns out to be the product of these p-adic densities. In order to see this, we need the following proposition.

Proposition 3.5.2. *For any non-negative integer k, we have*

$$p^{-\nu(n-1)}\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^\nu)\} = \sum_{t=0}^{\nu} p^{-nt}S_{p^t}(0).$$

Proof. We induct on ν. For $\nu = 0$ it is clear that both sides equal 1.

Now assume that $\nu > 0$ and the above equality holds for $\nu - 1$. Given some n-tuple $b \in (\mathbb{Z}/p^\nu\mathbb{Z})^n$, we have

$$\frac{1}{p^\nu} \sum_{a \,(\mathrm{mod}\, p^\nu)} e\left(\frac{aF(b)}{p^\nu}\right) = \begin{cases} 1 & \text{if } p^\nu \mid F(b) \\ 0 & \text{if } p^\nu \nmid F(b) \end{cases}.$$

Therefore we have

$$\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^\nu)\} = \sum_{b \,(\mathrm{mod}\, p^\nu)} \frac{1}{p^\nu} \sum_{a \,(\mathrm{mod}\, p^\nu)} e\left(\frac{aF(b)}{p^\nu}\right)$$

$$= \frac{1}{p^\nu} \sum_{b \,(\mathrm{mod}\, p^\nu)} \sum_{a \,(\mathrm{mod}\, p^\nu)} e\left(\frac{aF(b)}{p^\nu}\right).$$

The double sum above is almost the definition of $S_{p^\nu}(0)$, except that now a is allowed to range over all residue classes $(\mathrm{mod}\, p^\nu)$, and not only over those that are coprime to p^ν. With this in mind, we see that

$$\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^\nu)\} = \frac{1}{p^\nu} S_{p^\nu}(0) + \frac{1}{p^\nu} \sum_{\substack{a \,(\mathrm{mod}\, p^\nu) \\ p|a}} \sum_{b \,(\mathrm{mod}\, p^\nu)} e\left(\frac{aF(b)}{p^\nu}\right)$$

$$= \frac{1}{p^\nu} S_{p^\nu}(0) + \frac{1}{p^\nu} \sum_{a' \,(\mathrm{mod}\, p^{\nu-1})} \sum_{b \,(\mathrm{mod}\, p^\nu)} e\left(\frac{a'F(b)}{p^{\nu-1}}\right)$$

where we performed the variable change $a = pa'$. The last summand only depends on b modulo $p^{\nu-1}$, and for each $b' \in (\mathbb{Z}/p^{\nu-1}\mathbb{Z})^n$ there are exactly p^n choices of $b \in (\mathbb{Z}/p^\nu\mathbb{Z})^n$ that project to b'. Therefore, we see that

$$\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^\nu)\} = \frac{1}{p^\nu} S_{p^\nu}(0) + \frac{1}{p^\nu} \sum_{a' \,(\mathrm{mod}\, p^{\nu-1})} p^n \sum_{b' \,(\mathrm{mod}\, p^{\nu-1})} e\left(\frac{a'F(b)}{p^{\nu-1}}\right)$$

$$= \frac{1}{p^\nu} S_{p^\nu}(0) + p^{n-\nu} \sum_{a' \,(\mathrm{mod}\, p^{\nu-1})} \sum_{b' \,(\mathrm{mod}\, p^{\nu-1})} e\left(\frac{a'F(b)}{p^{\nu-1}}\right).$$

But since, for $b' \in (\mathbb{Z}/p^{\nu-1}\mathbb{Z})^n$, we have

$$\frac{1}{p^{\nu-1}} \sum_{a' \,(\mathrm{mod}\, p^\nu)} e\left(\frac{a'F(b')}{p^{\nu-1}}\right) = \begin{cases} 1 & \text{if } p^{\nu-1} \mid F(b') \\ 0 & \text{if } p^{\nu-1} \nmid F(b') \end{cases}$$

it follows that

$$\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^\nu)\}$$
$$= \frac{1}{p^\nu} S_{p^\nu}(0) + p^{n-1} \#\{x \in (\mathbb{Z}/p^{\nu-1}\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^{\nu-1})\}$$

and after dividing by $p^{(n-1)\nu}$, we get

$$p^{-(n-1)\nu} \#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^\nu)\}$$
$$= p^{-n\nu} S_{p^\nu}(0) + p^{-(n-1)(\nu-1)} \#\{x \in (\mathbb{Z}/p^{\nu-1}\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^{\nu-1})\}.$$

By the induction hypothesis, we see that

$$p^{-(n-1)(\nu-1)} \#\{x \in (\mathbb{Z}/p^{\nu-1}\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\, p^{\nu-1})\} = \sum_{t=0}^{\nu-1} p^{-nt} S_{p^t}(0)$$

whence

$$p^{-(n-1)\nu}\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\,p^\nu)\}$$
$$= \sum_{t=0}^{\nu-1} p^{-nt} S_{p^t}(0) + p^{-n\nu} S_{p^\nu}(0) = \sum_{t=0}^{\nu} p^{-nt} S_{p^t}(0)$$

as desired. $\square$

Corollary 3.5.3. *For each prime p, the limit*

$$\sigma_p(F^{(0)}, m) = \lim_{\nu \to \infty} p^{-(n-1)\nu}\#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \,(\mathrm{mod}\,p^\nu)\}$$

exists, and is equal to

$$\sum_{t=0}^{\infty} p^{-nt} S_{p^t}(0). \tag{3.47}$$

Proof. By Proposition 3.5.2, it suffices to argue that the series (3.47) converges absolutely. But the partial sums of the series

$$\sum_{t=1}^{\infty} p^{-nt} |S_{p^t}(0)|$$

are bounded above by

$$\sum_{q=1}^{\infty} q^{-n} |S_q(0)|$$

which is finite by Lemma 3.5.1. $\square$

We now note that, by Proposition 3.4.1, the sums $S_q(0)$ are multiplicative in q, i.e., one has

$$S_{uv}(0) = S_u(0) S_v(0)$$

whenever u and v are coprime. This implies that the singular series decomposes into an Euler product, namely,

$$\sum_{q=1}^{\infty} q^{-n} S_q(0) = \prod_{p \text{ prime}} \left(\sum_{t=0}^{\infty} p^{-nt} S_{p^t}(0) \right)$$
$$= \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) \qquad\qquad \text{by Proposition 3.5.2.}$$

We can therefore restate Lemma 3.5.1 as follows:

Lemma 3.5.4. *We have*

$$\sum_{q=1}^{X} q^{-n} S_q(0) = \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) + O_\varepsilon\left(\Delta^{\frac{n+4}{2}} X^{\frac{3-n}{2}+\varepsilon} m^\varepsilon \right).$$

Recall that the main term of our claimed estimate for $N(F, w)$ is

$$\sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}.$$

The singular integral $\sigma_\infty(F^{(0)}, w)$ does not depend on m, but the factors $\sigma_p(F^{(0)}, m)$ do. Therefore, in order to be able to extract useful information about the asymptotic behaviour of $N(F, w)$ when $F^{(0)}$ is fixed and m varies, we would like upper and lower bounds for the product

$$\prod_{p \text{ prime}} \sigma_p(F^{(0)}, m)$$

i.e., for the singular series.

We begin with upper bounds; this will be the easy part.

Lemma 3.5.5 (Upper bounds for the singular series). *We have the following:*

(i) If $n \geq 5$, then

$$\prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) \ll \Delta^{\frac{1}{2}}.$$

(ii) If $n = 4$, then

$$\prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) \ll_\varepsilon \Delta^4 m^\varepsilon.$$

Proof. For (i), we use Lemma 3.4.2, obtaining

$$\prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) = \sum_{q=1}^{\infty} q^{-n} S_q(0) \ll \sum_{q=1}^{\infty} q^{-n} (\Delta^{\frac{1}{2}} q^{\frac{n}{2}+1}) = \Delta^{\frac{1}{2}} \sum_{q=1}^{\infty} q^{1-\frac{n}{2}}.$$

Now the assumption that $n \geq 5$ implies that $1 - \frac{n}{2} < -1$, hence the sum above converges and we are done with (i).

For (ii), just apply directly the first statement of Lemma 3.5.1, say with $X = 1$. Since $S_1(0) = 1$, this implies

$$\prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) = \sum_{q=1}^{\infty} q^{-n} S_q(0) = 1 + O_\varepsilon \left(\Delta^4 m^\varepsilon \right) \ll_\varepsilon \Delta^4 m^\varepsilon.$$

$\square$

Lower bounds are a more delicate issue, and do not hold in full generality. For an obvious example, observe that the equation

$$2(x_1^2 + \cdots + x_n^2) = m$$

has no solution when m is an odd integer, so we should not expect the number of solutions to be $\gg m^{\frac{n}{2}-1}$, as it would be if the associated singular series was bounded from below uniformly in m. The obstruction to the existence of solutions in this case is purely 2-adic: the given equation does not have solutions over the ring $\mathbb{Z}_2$ of 2-adic integers when m is odd. When this kind of p-adic obstruction does not occur, we have indeed lower bounds for the singular series. In order to prove them, we need some preparatory work. We first recall the following well-known results from local field theory, the first of which can be seen as a form of Hensel's Lemma.

Fact 3.5.6 (Strong Hensel's Lemma). Let K be a complete discretely valued field with valuation v and ring of integers $\mathcal{O}_K$ (e.g. $K = \mathbb{Q}_p$, $v = v_p$ and $\mathcal{O}_K = \mathbb{Z}_p$). Let $f \in \mathcal{O}_K[x]$ be a polynomial, and assume there is $\alpha \in \mathcal{O}_K$ such that

$$v(f(\alpha)) > 2v(f'(\alpha)).$$

Then there exists some $\beta \in \mathcal{O}_K$ such that $f(\beta) = 0$ and $v(\beta - \alpha) > v(f'(\alpha))$.

Fact 3.5.7. Let K be a local field (e.g. $\mathbb{Q}_p$). Then every quadratic form in at least five variables with coefficients in K has a non-trivial zero.

Now define, for each prime p,

$$M_p = \max\{v_p(\lambda_1), \ldots, v_p(\lambda_n)\}.$$

Proposition 3.5.8. *Let p be a prime, and assume that $n \geq 5$ and that the equation $F^{(0)}(x) = m$ has a solution in $\mathbb{Z}_p^n$. If $p \neq 2$, then the congruence*

$$F^{(0)}(x) \equiv m \pmod{p^{4M_p+1}}$$

has a solution $x \in \mathbb{Z}_p$ such that $v_p(x_i) \leq M_p$ for some $i \in \{1, \ldots, n\}$. If $p = 2$, then the congruence

$$F^{(0)}(x) \equiv m \pmod{2^{4M_2+5}}$$

has a solution $x \in \mathbb{Z}_2$ such that $v_2(x_i) \leq M_2 + 1$ for some $i \in \{1, \ldots, n\}$.

Proof. Define

$$M_p' = \begin{cases} M_p & \text{if } p \neq 2 \\ M_p + 1 & \text{if } p = 2 \end{cases}.$$

Take any $x \in \mathbb{Z}_p^n$ such that $F^{(0)}(x) = m$, which exists by assumption. If some x_i has $v_p(x_i) \leq M_p'$ we are done. Otherwise, each x_i is divisible by $p^{M_p'+1}$, and hence $F^{(0)}(x) = m$ is divisible by $p^{2M_p'+2}$.

Consider a solution $X \in \mathbb{Q}_p^n \setminus \{0\}$ to the equation $F^{(0)}(X) = 0$, which exists by Fact 3.5.7. By multiplying X by a suitable power of p we may assume without loss of generality that $X \in \mathbb{Z}_p^n \setminus p\mathbb{Z}_p^n$. Again without loss of generality, we may assume that X_1 is not divisible by p. Define a polynomial by

$$f(t) = \lambda_1 t^2 + \lambda_2 X_2^2 + \cdots + \lambda_n X_n^2 - m.$$

Since both $\lambda_1 X_1^2 + \cdots + \lambda_n X_n^2$ and m are divisible by p^{2M_p+2}, we have $p^{2M_p+2} | f(X_1)$. Moreover, we have $f'(X_1) = 2\lambda_1 X_1$, and hence, since p does not divide X_1,

$$2v_p(f'(X_1)) = 2v_p(2\lambda_1) \leq 2M_p' < 2M_p' + 2 \leq v_p(f(X_1)).$$

Now Hensel's Lemma (Fact 3.5.6) implies that there exists $X_1' \in \mathbb{Z}_p$ such that $f(X_1') = 0$, which in turn implies

$$\lambda_1 {X_1'}^2 + \lambda_2 X_2^2 + \cdots + \lambda_n X_n^2 = m \quad \text{i.e.,} \quad F^{(0)}(X_1', X_2, \ldots, X_n) = m,$$

and moreover we may take such X_1' with $v_p(X_1 - X_1') > v_p(f'(X_1)) \geq 0$, so that $p \mid X_1 - X_1'$, and, since p does not divide X_1, it follows that p does not divide X_1' either. Now $X' = (X_1', X_2, \ldots, X_n)$ satisfies $F^{(0)}(X') \equiv m \pmod{p^{4M_p'+1}}$ since we actually have $F^{(0)}(X') = m$, and since $v_p(X_1') = 0$ this solution satisfies the desired conditions. $\square$

Remark 3.5.9. The condition that $F^{(0)}(x) = m$ has a solution in $\mathbb{Z}_p^n$ was only needed to tackle the case when m is not divisible by $p^{2M_p'+1}$. So if $p^{2M_p'+1} \mid m$ this condition can be removed from the previous proposition, and from everything that follows from it.

The previous proposition is the main technical tool needed to devise the following estimate.

Proposition 3.5.10. *Let p be a prime, and assume that $n \geq 5$ and the equation $F^{(0)}(x) = m$ has a solution in $\mathbb{Z}_p^n$. If $p \neq 2$, then for every $\nu \geq 4M_p + 1$ the congruence*

$$F^{(0)}(x) \equiv m \pmod{p^\nu}$$

has at least $p^{(n-1)(\nu - 4M_p - 1)}$ solutions in $(\mathbb{Z}/p^\nu\mathbb{Z})^n$. Moreover, if $p = 2$, then for every $\nu \geq 4M_2 + 5$ the congruence

$$F^{(0)}(x) \equiv m \pmod{2^\nu}$$

has at least $p^{(n-1)(\nu - 4M_2 - 5)}$ solutions in $(\mathbb{Z}/p^\nu\mathbb{Z})^n$.

Proof. Using the notation of the previous proof, we must show that if $\nu \geq 4M_p' + 1$ then the congruence

$$F^{(0)}(x) \equiv m \pmod{p^\nu}$$

has at least $p^{(n-1)(\nu - 4M_p' - 1)}$ solutions in $(\mathbb{Z}/p^\nu\mathbb{Z})^n$.

By Proposition 3.5.8 the congruence $F^{(0)}(x) \equiv m \pmod{p^{4M_p' + 1}}$ has at least one solution in $(\mathbb{Z}/p^{4M_p' + 1}\mathbb{Z})^n$, and moreover we can find such a solution with $v_p(x_i) \leq M_p'$ for some i. Without loss of generality assume $i = 1$. Now for each $(n-1)$-tuple in $(\mathbb{Z}/p^\nu\mathbb{Z})^{n-1}$ that projects to the last $n-1$ coordinates of x under the canonical projection choose a representative $(X_2, \ldots, X_n) \in \mathbb{Z}_p^{n-1}$. In this way we get $p^{(n-1)(\nu - 4M_p' - 1)}$ distinct tuples $(X_2, \ldots, X_n) \in \mathbb{Z}_p^{n-1}$ with $X_i \equiv x_i \pmod{p^{4M_p' + 1}}$ for $i = 2, \ldots, n$. We claim that for each such tuple we can find $X_1 \in \mathbb{Z}_p$ such that $X = (X_1, \ldots, X_n)$ satisfies $F^{(0)}(X) = m$. Projecting these n-tuples onto $(\mathbb{Z}/p^\nu\mathbb{Z})^n$ we get the desired $p^{(n-1)(\nu - 4M_p' - 1)}$ solutions.

In order to find X_1, consider the polynomial

$$f(t) = \lambda_1 t^2 + \lambda_2 X_2^2 + \cdots + \lambda_n X_n^2 - m.$$

Take any $\alpha \in \mathbb{Z}_p$ that projects to x_1 in $\mathbb{Z}/p^{4M_p' + 1}\mathbb{Z}$. The condition that α projects to x_1 and X_i projects to x_i for each $i \geq 2$ implies that

$$p^{4M_p' + 1} \mid f(\alpha) \quad \text{i.e.,} \quad v_p(f(\alpha)) \geq 4M_p' + 1.$$

On the other hand, we must have $v_p(\alpha) \leq M_p'$ by assumption; moreover, the definition of M_p' implies that $v_p(2\lambda_1) \leq M_p'$. Hence we have

$$2v_p(f'(\alpha)) = 2v_p(2\lambda_1\alpha) \leq 4M_p' < v_p(f(\alpha)).$$

By Hensel's Lemma (Fact 3.5.6) there exists $X_1 \in \mathbb{Z}_p$ such that $f(X_1) = 0$, which implies precisely that $F^{(0)}(X_1, \ldots, X_n) = m$, and we are done. $\qquad\square$

Corollary 3.5.11. *For every prime $p \neq 2$ we have*

$$\sigma_p(F^{(0)}, m) \geq p^{-(n-1)(4M_p + 1)}.$$

Moreover, we also have

$$\sigma_2(F^{(0)}, m) \geq 2^{-(n-1)(4M_2 + 5)}.$$

Proof. By Proposition 3.5.10 we have, for each $\nu \geq 4M_p' + 1$,

$$p^{-(n-1)\nu} \#\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^n : F^{(0)}(x) \equiv m \pmod{p^\nu}\}$$
$$\geq p^{-(n-1)\nu} \cdot p^{(n-1)(\nu - 4M_p' - 1)} = p^{-(n-1)(4M_p' + 1)}.$$

Taking the limit as ν tends to infinity yields the desired lower bound. $\qquad\square$

We are now ready to bound the singular series from below, under appropriate conditions.

Lemma 3.5.12 (Lower bound for the singular series). *Suppose that $n \geq 5$, and that for each prime $p < (9\Delta)^{1/(n-2)}$ the equation $F^{(0)}(x) = m$ has a solution in $\mathbb{Z}_p^n$. Then we have*

$$\prod_{p \ prime} \sigma_p(F^{(0)}, m) \gg e^{-C\Delta^{1/2}} \prod_{\substack{p \ prime \\ p < (9\Delta)^{1/(n-2)}}} p^{-(n-1)(4M_p+1)}$$

for some absolute constant C. In particular,

$$\prod_{p \ prime} \sigma_p(F^{(0)}, m) \gg_\Delta 1.$$

Remark 3.5.13. Using Remark 3.5.9, one may drop the assumption on local solvability of $F^{(0)}(x) = m$ if one has

$$v_p(m) \geq 2M_p' + 1$$

for each prime $p < (9\Delta)^{1/(n-2)}$.

Proof. We write

$$\prod_{p \ prime} \sigma_p(F^{(0)}, m) = \prod_{\substack{p \ prime \\ p < (9\Delta)^{1/(n-2)}}} \sigma_p(F^{(0)}, m) \prod_{\substack{p \ prime \\ p \geq (9\Delta)^{1/(n-2)}}} \sigma_p(F^{(0)}, m)$$

and estimate each factor separately.

For the first factor we apply directly Corollary 3.5.11, yielding

$$\prod_{\substack{p \ prime \\ p < (9\Delta)^{1/(n-2)}}} \sigma_p(F^{(0)}, m) \gg \prod_{\substack{p \ prime \\ p < (9\Delta)^{1/(n-2)}}} p^{-(n-1)(4M_p+1)}. \tag{3.48}$$

For the second factor we use Corollary 3.5.3. This yields

$$\sigma_p(F^{(0)}, m) = 1 + \sum_{t=1}^{\infty} p^{-nt} S_{p^t}(0)$$

and hence

$$\begin{aligned}
|\sigma_p(F^{(0)}, m) - 1| &\leq \sum_{t=1}^{\infty} p^{-nt} |S_{p^t}(0)| \\
&\ll \sum_{t=1}^{\infty} p^{-nt} \left(\Delta^{\frac{1}{2}} p^{t\left(\frac{n}{2}+1\right)} \right) \qquad \text{by Lemma 3.4.2} \\
&= \Delta^{\frac{1}{2}} \sum_{t=1}^{\infty} p^{-\left(\frac{n}{2}-1\right)t} = \Delta^{\frac{1}{2}} \cdot \frac{1}{p^{\frac{n}{2}-1} - 1}.
\end{aligned}$$

Now observe that, if $p > (9\Delta)^{1/(n-2)}$, then $p^{\frac{n}{2}-1} > 3\Delta^{\frac{1}{2}}$, and hence $p^{\frac{n}{2}-1} - 1 > 2\Delta^{\frac{1}{2}}$, i.e.,

$$\Delta^{\frac{1}{2}} \cdot \frac{1}{p^{\frac{n}{2}-1} - 1} < \frac{1}{2}.$$

We now use the inequality $1 + x \geq e^{-2|x|}$, which is true for all $|x| \leq \frac{1}{2}$ by a routine calculus check. We have

$$\prod_{\substack{p \text{ prime} \\ p \geq (9\Delta)^{1/(n-2)}}} \sigma_p(F^{(0)}, m) \geq \prod_{\substack{p \text{ prime} \\ p \geq (9\Delta)^{1/(n-2)}}} \left(1 - \Delta^{\frac{1}{2}} \cdot \frac{1}{p^{\frac{n}{2}-1} - 1}\right)$$

$$> \exp\left(-2\Delta^{\frac{1}{2}} \sum_{\substack{p \text{ prime} \\ p \geq (9\Delta)^{1/(n-2)}}} \frac{1}{p^{\frac{n}{2}-1} - 1}\right) > e^{-C\Delta^{1/2}} \qquad (3.49)$$

if we take C greater than the sum

$$\sum_{p \text{ prime}} \frac{2}{p^{\frac{3}{2}} - 1},$$

which converges. Now multiplying together (3.48) and (3.49) yields the desired bound. $\qquad \square$

§3.6 Proof of Theorem 3.0.1

In this section we use the results previously obtained in Chapter 3 in order to prove Lemma 3.1.3, and hence Theorem 3.0.1. The following propositions lead up to this lemma.

Proposition 3.6.1. *The infinite sum*

$$\sum_{\substack{c \in \mathbb{Z}^n \\ c \neq 0}} \frac{1}{|c|^{n+1}}$$

converges.

Proof. Since there are only finitely many c's with $|c| = 1$, we can discard those when studying convergence of the sum above. For each $k \geq 0$, we observe that the number of points $c \in \mathbb{Z}^n$ with $2^k < |c| \leq 2^{k+1}$ is $(2^{k+1})^n - (2^k)^n = O(2^{nk})$. Therefore,

$$\sum_{\substack{c \in \mathbb{Z}^n \\ 2^k < |c| \leq 2^{k+1}}} \frac{1}{|c|^{n+1}} \leq \sum_{\substack{c \in \mathbb{Z}^n \\ 2^k < |c| \leq 2^{k+1}}} \frac{1}{(2^k)^{n+1}} \ll \frac{2^{nk}}{(2^k)^{n+1}} = \frac{1}{2^k}.$$

Hence we have

$$\sum_{\substack{c \in \mathbb{Z}^n \\ |c| > 1}} \frac{1}{|c|^{n+1}} = \sum_{k \geq 0} \sum_{\substack{c \in \mathbb{Z}^n \\ 2^k < |c| \leq 2^{k+1}}} \frac{1}{|c|^{n+1}} \ll \sum_{k \geq 0} \frac{1}{2^k} = 2$$

implying that the original sum converges, as desired. $\qquad \square$

Proposition 3.6.2. *Let $\varepsilon > 0$, and let $N > \left(1 + \frac{1}{2\varepsilon}\right)(n+1)$ be an integer. We then have*

$$\sum_{\substack{c \in \mathbb{Z}^n \\ |c| > m^\varepsilon}} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_N |w|_{N+1} |\lambda|^{\frac{N}{2}}.$$

Proof. We use Lemma 3.2.6 and Lemma 3.4.2, yielding

$$S_q(c) I_q(c) \ll_N |w|_{N+1} |\lambda|^{\frac{N}{2}} q^{\frac{n}{2}} m^{\frac{n+1}{2}} |c|^{-N}.$$

This implies

$$\sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_N |w|_{N+1} |\lambda|^{\frac{N}{2}} m^{\frac{n+1}{2}} |c|^{-N} \sum_{q=1}^{\infty} q^{-\frac{n}{2}} \ll |w|_{N+1} |\lambda|^{\frac{N}{2}} m^{\frac{n+1}{2}} |c|^{-N}.$$

Now the assumption that $|c| > m^{\varepsilon}$ implies that $m^{(n+1)/2} |c|^{-N} < |c|^{-(n+1)}$, since this inequality can be rewritten as $|c|^{N-(n+1)} > m^{(n+1)/2}$ and $N - (n+1) > \frac{n+1}{2\varepsilon}$ by assumption. It follows that

$$\sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_N |w|_{N+1} |\lambda|^{\frac{N}{2}} |c|^{-(n+1)}$$

and hence

$$\sum_{\substack{c \in \mathbb{Z}^n \\ |c| > m^{\varepsilon}}} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_N \sum_{\substack{c \in \mathbb{Z}^n \\ |c| > m^{\varepsilon}}} |w|_{N+1} |\lambda|^{\frac{N}{2}} |c|^{-(n+1)} = |w|_{N+1} |\lambda|^{\frac{N}{2}} \sum_{\substack{c \in \mathbb{Z}^n \\ |c| > m^{\varepsilon}}} \frac{1}{|c|^{n+1}}$$

implying the desired result, since the above sum is convergent by Proposition 3.6.1. $\qquad \square$

Proposition 3.6.3. *Let $0 < \varepsilon < \frac{1}{4}$, and let $M > \frac{3n}{2\varepsilon}$ be an integer. We then have*

$$\sum_{\substack{c \in \mathbb{Z}^n \\ m^{\varepsilon} \geq |c| > 0}} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_M \Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M \right) m^{\frac{n+3}{4} + \frac{7n\varepsilon}{2}}.$$

Proof. We use Lemma 3.2.14, with ε replaced by $n\varepsilon$. The size condition on ε implies that $(1-\varepsilon)^{-1} < 2$. Hence Lemma 3.2.14 gives, for $|c| \geq 1$,

$$I_q(c) \ll_M \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{1}{2} + \frac{n}{4} + n\varepsilon} |c|^{1 - \frac{n}{2} + n\varepsilon} q^{\frac{n}{2} - 1 - 2n\varepsilon}$$

$$\ll_M \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n}{4} + \frac{1}{2} + n\varepsilon} q^{\frac{n}{2} - 1}.$$

Now we have, for any $R > 0$,

$$\sum_{R < q \leq 2R} q^{-n} |S_q(c) I_q(c)| \ll_M \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n}{4} + \frac{1}{2} + n\varepsilon} \sum_{R < q \leq 2R} q^{-\frac{n}{2} - 1} |S_q(c)|$$

$$\ll_M R^{-\frac{n}{2} - 1} \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n}{2} + \frac{1}{2} + n\varepsilon} \sum_{q \leq 2R} |S_q(c)|$$

$$\ll_M \Delta^{\frac{n+4}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n}{4} + \frac{1}{2} + 2n\varepsilon} R^{\frac{1}{2} + n\varepsilon} \qquad (3.50)$$

where the last estimate follows from Lemma 3.4.11. We now let k be the smallest integer such that $2^k > \sqrt{m}$. Observe that for $q > \sqrt{m}$ we have $I_q(c) = 0$; this follows from (3.9) and the Observation made after (3.9) that $I(r; u) = 0$ if $r > 1$. Therefore

$$\sum_{q=1}^{\infty} q^{-n} |S_q(c) I_q(c)| = \sum_{1 \leq q \leq \sqrt{m}} q^{-n} |S_q(c) I_q(c)| \leq \sum_{j=0}^{k} \sum_{2^{j-1} < q \leq 2^j} q^{-n} |S_q(c) I_q(c)|$$

$$\ll_M \Delta^{\frac{n+4}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n}{4} + \frac{1}{2} + 2n\varepsilon} \sum_{j=0}^{k} (2^{j-1})^{\frac{1}{2} + n\varepsilon} \qquad (3.51)$$

by (3.50). We now observe that

$$\sum_{j=0}^{k} 2^{(j-1)\left(\frac{1}{2}+n\varepsilon\right)} = 2^{(k-1)\left(\frac{1}{2}+n\varepsilon\right)} \sum_{j=0}^{k} 2^{-j\left(\frac{1}{2}+n\varepsilon\right)} \leq 2^{(k-1)\left(\frac{1}{2}+n\varepsilon\right)} \sum_{j=0}^{\infty} 2^{-j/2}$$

and since the above series converges, it follows that

$$\sum_{j=0}^{k} 2^{(j-1)\left(\frac{1}{2}+n\varepsilon\right)} \ll 2^{(k-1)\left(\frac{1}{2}+n\varepsilon\right)} \leq (\sqrt{m})^{\frac{1}{2}+n\varepsilon} = m^{\frac{1}{4}+\frac{n\varepsilon}{2}}.$$

Here we used the Definition of k, which implies $2^{k-1} \leq \sqrt{m}$. Now (3.51) implies

$$\sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_M \Delta^{\frac{n+4}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n}{4}+\frac{1}{2}+2n\varepsilon} m^{\frac{1}{4}+\frac{n\varepsilon}{2}}$$

$$\ll_M \Delta^{\frac{n+4}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n+3}{4}+\frac{5n\varepsilon}{2}}.$$

We now sum this over all c's with $0 < |c| \leq m^{\varepsilon}$. The number of such c's is $O(m^{n\varepsilon})$, and we obtain

$$\sum_{\substack{c \in \mathbb{Z}^n \\ m^{\varepsilon} \geq |c| > 0}} \sum_{q=1}^{\infty} q^{-n} S_q(c) I_q(c) \ll_M \Delta^{\frac{n+4}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\Delta} + \frac{|w|_M}{\sqrt{\Delta}} \right) m^{\frac{n+3}{4}+\frac{7n\varepsilon}{2}}$$

which is precisely the desired estimate. $\square$

Proposition 3.6.4. *Let $0 < \varepsilon < \frac{n}{2} - 1$. We then have*

$$\sum_{q > m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) I_q(0) \ll_{\varepsilon} \Delta^{\frac{n+3}{2}} |w|_0 m^{\frac{n+3}{4}+\frac{n\varepsilon}{2}}.$$

Proof. We use Lemma 3.2.2, which implies, for any $R > 0$,

$$\sum_{R < q \leq 2R} q^{-n} S_q(0) I_q(0) \ll \frac{|w|_0}{\sqrt{\Delta}} m^{\frac{n}{2}} \sum_{R < q \leq 2R} q^{-n} |S_q(0)| \ll \frac{|w|_0}{\sqrt{\Delta}} m^{\frac{n}{2}} R^{-n} \sum_{q \leq 2R} |S_q(0)|.$$

We now estimate the sum above using Lemma 3.4.11, yielding

$$\sum_{R < q \leq 2R} q^{-n} S_q(0) I_q(0) \ll_{\varepsilon} \frac{|w|_0}{\sqrt{\Delta}} m^{\frac{n}{2}} R^{-n} \cdot \Delta^{\frac{n+4}{2}} R^{\frac{n+3}{2}+\varepsilon} m^{\varepsilon} = \Delta^{\frac{n+3}{2}} |w|_0 R^{\frac{3-n}{2}+\varepsilon} m^{\frac{n}{2}+\varepsilon}.$$

Using this estimate with $R = m^{\frac{1}{2}-\varepsilon} \cdot 2^k$ for $k = 0, 1, \ldots$ yields

$$\sum_{q > m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) I_q(0) \ll \Delta^{\frac{n+3}{2}} |w|_0 m^{\frac{n}{2}+\varepsilon} \sum_{k \geq 0} \left(m^{\frac{1}{2}-\varepsilon} \cdot 2^k \right)^{\frac{3-n}{2}+\varepsilon}$$

$$\ll \Delta^{\frac{n+3}{2}} |w|_0 m^{\frac{n}{2}+\varepsilon+\left(\frac{1}{2}-\varepsilon\right)\left(\frac{3-n}{2}+\varepsilon\right)} \sum_{k \geq 0} 2^{k\left(\frac{3-n}{2}+\varepsilon\right)}$$

and the size constraint on ε implies that $\frac{3-n}{2} + \varepsilon < -1$, hence the sum above is

$$\ll \sum_{k \geq 0} 2^{-k} = 2$$

implying that

$$\sum_{q>m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) I_q(0) \ll \Delta^{\frac{n+3}{2}} |w|_0 m^{\frac{n}{2}+\varepsilon+\left(\frac{1}{2}-\varepsilon\right)\left(\frac{3-n}{2}+\varepsilon\right)}.$$

Now we see that

$$\frac{n}{2} + \varepsilon + \left(\frac{1}{2} - \varepsilon\right)\left(\frac{3-n}{2} + \varepsilon\right) = \frac{n+3}{4} + \frac{n\varepsilon}{2} - \varepsilon^2 < \frac{n+3}{4} + \frac{n\varepsilon}{2}$$

establishing the desired estimate. $\square$

Proposition 3.6.5. *Let $\varepsilon > 0$, and let K be an integer such that $K \geq \frac{n}{2\varepsilon}$. Then we have*

$$\sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) I_q(0) = \sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}}$$

$$+ O_{\varepsilon,K}\left(\Delta^{\frac{n+3}{2}} |w|_0 m^{\frac{n+3}{4}+\frac{n\varepsilon}{2}} + |w|_{2K+1} \log(m)\right).$$

Moreover, the factor $\log(m)$ can be removed if $n \geq 5$.

Proof. In what follows, abbreviate $\sigma_\infty(F^{(0)}, w)$ and $\sigma_p(F^{(0)}, m)$ by σ_∞ and σ_p, respectively. We use Lemma 3.3.2, which implies for $q \leq m^{\frac{1}{2}-\varepsilon}$

$$\begin{aligned}
I_q(0) &= m^{\frac{n}{2}} \left(\sigma_\infty + O_K\left(\frac{|w|_{2K+1}}{\sqrt{\Delta}} \left(\frac{q}{m^{\frac{1}{2}}}\right)^N\right)\right) \\
&= m^{\frac{n}{2}} \left(\sigma_\infty + O_K\left(\frac{|w|_{2K+1}}{\sqrt{\Delta}} \left(m^{-\varepsilon}\right)^K\right)\right) \\
&= m^{\frac{n}{2}} \left(\sigma_\infty + O_K\left(\frac{|w|_{2K+1}}{\sqrt{\Delta}} m^{-\frac{n}{2}}\right)\right) \qquad \text{using } K\varepsilon \geq \frac{n}{2} \\
&= m^{\frac{n}{2}} \sigma_\infty + O_K\left(\frac{|w|_{2K+1}}{\sqrt{\Delta}}\right).
\end{aligned}$$

This implies

$$\sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) I_q(0) = m^{\frac{n}{2}} \sigma_\infty \sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) + O_{\varepsilon,K}\left(\frac{|w|_{2K+1}}{\sqrt{\Delta}} \sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} |S_q(0)|\right)$$

and from Lemma 3.4.2 we get

$$\sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} |S_q(0)| \ll \Delta^{\frac{1}{2}} \sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{1-\frac{n}{2}} \ll \Delta^{\frac{1}{2}} \log(m)$$

where the $\log(m)$ only needs to be present if $n = 4$, because otherwise the sum $\sum_{q \geq 1} q^{1-\frac{n}{2}}$ converges. We conclude that

$$\sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) I_q(0) = m^{\frac{n}{2}} \sigma_\infty \sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) + O_{\varepsilon,N}(|w|_{2K+1} \log(m)). \qquad (3.52)$$

It now remains to estimate the first summand above. For this we use Lemma 3.5.4, which yields

$$\begin{aligned}
\sum_{q \leq m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) &= \prod_{p \text{ prime}} \sigma_p + O_\varepsilon\left(\Delta^{\frac{n+4}{2}} m^{\left(\frac{1}{2}-\varepsilon\right)\left(\frac{3-n}{2}+\varepsilon\right)+\varepsilon}\right) \\
&= \prod_{p \text{ prime}} \sigma_p + O_\varepsilon\left(\Delta^{\frac{n+4}{2}} m^{\frac{-n+3}{4}+\frac{n\varepsilon}{2}}\right)
\end{aligned}$$

and hence

$$m^{\frac{n}{2}} \sigma_\infty \sum_{q \le m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) = \sigma_\infty \prod_{p \text{ prime}} \sigma_p m^{\frac{n}{2}} + O_\varepsilon \left(\sigma_\infty \Delta^{\frac{n+4}{2}} m^{\frac{n+3}{4}+\frac{n\varepsilon}{2}} \right).$$

We have argued before, for example in the proof of Proposition 3.2.1, that the volume of the subset of $\mathrm{supp}(w)$ where $|G(x)| \le T$ is $O\left(\frac{T}{\sqrt{\Delta}}\right)$. This implies, from the definition of the singular integral, that $\sigma_\infty \ll \frac{1}{\sqrt{\Delta}} |w|_0$. The previous equality hence implies

$$m^{\frac{n}{2}} \sigma_\infty \sum_{q \le m^{\frac{1}{2}-\varepsilon}} q^{-n} S_q(0) = \sigma_\infty \prod_{p \text{ prime}} \sigma_p m^{\frac{n}{2}} + O_\varepsilon \left(\Delta^{\frac{n+3}{2}} |w|_0 m^{\frac{n+3}{4}+\frac{n\varepsilon}{2}} \right)$$

and together with 3.52 this implies the result. $\qquad \square$

We are now ready to complete the proof of Lemma 3.1.3.

Proof of Lemma 3.1.3. Use Propositions 3.6.2 and 3.6.3 with ε replaced by $2\varepsilon/7n$, and Propositions 3.6.4 and 3.6.5 with ε replaced by $2\varepsilon/n$. Adding up the estimates obtained in each of these Propositions, we arrive at

$$\sum_{c \in \mathbb{Z}^n} \sum_{q=1}^\infty q^{-n} S_q(c) I_q(c) = \sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}}$$
$$+ O_\varepsilon \left(\Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M \right) m^{\frac{n+3}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{N}{2}} + |w|_{2K+1} \log(m) \right),$$

where N, M and K are respectively the smallest integers exceeding $7n(n+1)/2\varepsilon$, $21n^2/4\varepsilon$ and $n^2/4\varepsilon$, respectively. Since $M > 2K+1$, we have

$$|w|_{2K+1} \log(m) \ll_\varepsilon |w|_M m^{\frac{n+3}{4}+\varepsilon}$$

and hence the last summand can be removed. We are left with

$$\sum_{c \in \mathbb{Z}^n} \sum_{q=1}^\infty q^{-n} S_q(c) I_q(c) = \sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}}$$
$$+ O_\varepsilon \left(\Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M \right) m^{\frac{n+3}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{N}{2}} \right).$$

We now use Lemma 2.3.1 with $P = Q = \sqrt{m}$; recall that then $C_Q = 1 + O(m^{-n})$ by Lemma 2.1.1. This yields

$$N(F, w) = m^{-1}(1 + O(m^{-n})) \sum_{c \in \mathbb{Z}^n} \sum_{q=1}^\infty q^{-n} S_q(c) I_q(c)$$
$$= \sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}$$
$$+ O_\varepsilon \left(\Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M \right) m^{\frac{n-1}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{N}{2}} \right)$$
$$+ O_\varepsilon \left(\sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{1-\frac{n}{2}} \right)$$
$$+ O_\varepsilon \left(\Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M \right) m^{\frac{-3n-1}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{N}{2}} m^{-n-1} \right).$$

The terms in the last line are obviously bounded by the terms two lines above, so these can be ignored. Moreover, it follows from Lemma 3.5.5, together with the estimate $\sigma_\infty \ll \frac{|w|_0}{\sqrt{\Delta}}$ shown in the proof of Proposition 3.6.5, that

$$\sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{1-\frac{n}{2}} \ll \Delta^{\frac{7}{2}} |w|_0$$

and, on the other hand, since $\varepsilon < \frac{n}{4}$ by assumption, we have

$$\frac{N}{2} > \frac{7n^2}{4 \cdot \frac{n}{4}} = 7n > \frac{7n}{2}$$

whence

$$|w|_{N+1} |\lambda|^{\frac{N}{2}} \geq |w|_0 |\lambda|^{\frac{7n}{2}} \gg \Delta^{\frac{7}{2}} |w|_0.$$

Hence the summand

$$\sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{1-\frac{n}{2}}$$

can also be ignored, since it is bounded by the summand on the line before. We therefore obtain

$$N(F, w) = \sigma_\infty(F^{(0)}, w) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1}$$

$$+ O_\varepsilon \left(\Delta^{\frac{n+3}{2}} \left(\frac{|w|_0 |\lambda|^{3n}}{\sqrt{\Delta}} + |w|_M \right) m^{\frac{n-1}{4}+\varepsilon} + |w|_{N+1} |\lambda|^{\frac{N}{2}} \right)$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad\square$

§3.7 Proof of Theorem 1.0.3

We now prove Theorem 1.0.3. For that we use again the function ν defined after Lemma 3.2.2. Define a smooth, compactly supported weight w by

$$w(x) = \nu(G(x)).$$

Now we observe that, by definition, we have

$$N(F, w) = \sum_{\substack{x \in \mathbb{Z}_n \\ F(x)=0}} w\left(\frac{x}{\sqrt{m}}\right),$$

but when $F(x) = 0$ we have $F^{(0)}(x) = m$, whence $F^{(0)}(x/\sqrt{m}) = 1$ and $G(x/\sqrt{m}) = 0$, implying $w(x/\sqrt{m}) = 1$. Therefore,

$$N(F, w) = \#\{x \in \mathbb{Z}^n : F^{(0)}(x) = m\}.$$

On the other hand, we recall that

$$\sigma_\infty(F^{(0)}, w) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} w(x) dx$$

but when $\epsilon \leq \frac{1}{2}$ we have $w(x) = \nu(G(x)) = 1$ whenever $|G(x)| \leq \varepsilon$. It follows that

$$\sigma_\infty(F^{(0)}, w) = \lim_{\varepsilon \to 0} \frac{1}{2\varepsilon} \int_{|G(x)| \leq \varepsilon} 1 dx = \sigma_\infty(F^{(0)}).$$

It follows therefore from Theorem 3.0.1 that

$$
\begin{aligned}
&\#\{x \in \mathbb{Z}^n : F^{(0)}(x) = m\} \\
&= \sigma_\infty(F^{(0)}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1} + O_\varepsilon\left(\Delta^{\frac{n+3}{2}} |\lambda|^{\frac{K}{2}} |w|_K m^{\frac{n-1}{4}+\varepsilon}\right)
\end{aligned}
\tag{3.53}
$$

where K is the smallest integer such that $K > 100n^2/\varepsilon$.

It remains to estimate $|w|_K$. For that, we observe that, by a straightforward induction, there exist constants $c_{a_1, b_1, \ldots, a_n, b_n}$ indexed by $2n$-tuples of non-negative integers such that

$$
\frac{\partial^{i_1 + \cdots + i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}} w(x) = \sum_{\substack{a_1 + 2b_1 = i_1 \\ \cdots \\ a_n + 2b_n = i_n}} c_{a_1, b_1, \ldots, a_n, b_n} \nu^{(a_1 + b_1 + \cdots + a_n + b_n)}(G(x)) \prod_{i=1}^n \left(\frac{\partial G}{\partial x_i}\right)^{a_i} \left(\frac{\partial^2 G}{\partial x_i^2}\right)^{b_i}
$$

for every non-negative integers $i_1, \ldots, i_n$. For $x \in \operatorname{supp}(w)$, we must have $|G(x)| < 1$, implying

$$
\lambda_1 x_1^2 + \cdots + \lambda_n x_n^2 < 2
$$

and hence $x_i \ll \frac{1}{\sqrt{\lambda_i}}$. Since $\frac{\partial G}{\partial x_i} = 2\lambda_i x_i$, it follows that $\frac{\partial G}{\partial x_i} \ll \lambda_i$. Also observe that $\frac{\partial^2 G}{\partial x_i^2} = 2\lambda_i$. It follows that

$$
\frac{\partial^{i_1 + \cdots + i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}} w(x) \ll \sum_{\substack{a_1 + 2b_1 = i_1 \\ \cdots \\ a_n + 2b_n = i_n}} \prod_{k=1}^n \lambda_k^{\frac{a_k}{2}} \lambda_k^{b_k} = \sum_{\substack{a_1 + 2b_1 = i_1 \\ \cdots \\ a_n + 2b_n = i_n}} \prod_{k=1}^n \lambda_k^{\frac{i_k}{2}} \ll \prod_{k=1}^n \lambda_k^{\frac{i_k}{2}} \leq |\lambda|^{\frac{i_1 + \cdots + i_n}{2}}.
$$

This implies that

$$
|w|_K \ll |\lambda|^{\frac{K}{2}}
$$

and using this estimate on (3.53), we obtain

$$
\begin{aligned}
&\#\{x \in \mathbb{Z}^n : F^{(0)}(x) = m\} \\
&= \sigma_\infty(F^{(0)}) \prod_{p \text{ prime}} \sigma_p(F^{(0)}, m) m^{\frac{n}{2}-1} + O_\varepsilon\left(\Delta^{\frac{n+3}{2}} |\lambda|^K m^{\frac{n-1}{4}+\varepsilon}\right).
\end{aligned}
$$

Since obviously $K < 1 + 100n^2/\varepsilon$, Theorem 1.0.3 follows.

Bibliography

[1] D.R. Heath-Brown, *A New Form of the Circle Method, and its Application to Quadratic Forms*, J. Reine. Angew. Math. **481** (1996), 149-206.

[2] W. Duke, J. Friedlander and H. Iwaniec, *Bounds for automorphic L-functions*, Invent. Math, **122** (1993), 1-8.

[3] H. Iwaniec, *Topics in Classical Automorphic Forms*, Graduate Studies in Mathematics, 17 (American Mathematical Society, 1997)

[4] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, 67 (American Mathematical Society, 2005)

[5] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, 53 (Colloquium Publications, 2004)