The values of a quadratic form at square-free points

R. C. Baker

§1 Introduction

Let $f(\boldsymbol{x}) = f(x_1, \dots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j \quad (a_{ij} = a_{ji} \in \mathbb{Z})$ be a nonsingular quadratic form, $n \geq 3$. Let $M = [a_{ij}]$, $D = \det M$. We are interested in the distribution of square-free solutions $\boldsymbol{x}$ in $\mathbb{Z}^n$ of

$$f(\boldsymbol{x}) = m \tag{1.1}$$

for a given m. More precisely, let

$$\pi_{\boldsymbol{x}} = x_1 \dots x_n.$$

Define

$$\mu(\boldsymbol{x}) = 0 \ \text{ if } \ \pi_{\boldsymbol{x}} = 0, \ \mu(\boldsymbol{x}) = \mu(|x_1|) \dots \mu(|x_n|) \ \text{ if } \ \pi_{\boldsymbol{x}} \neq 0. \tag{1.2}$$

A *square-free* solution of (1.1) is a solution having $\mu(\boldsymbol{x}) \neq 0$. We assume, without loss of generality, that $m \geq 0$.

Until now, this question has only been investigated for positive-definite f. In this case, let $R(m)$ denote the total number of square-free solutions of (1.1). Estermann [8] gave an asymptotic formula for $R(m)$ in the case $f(\boldsymbol{x}) = x_1^2 + \cdots + x_n^2$, $n \geq 5$. Later, Podsypanin [13] extended this to all positive-definite forms f with $n \geq 4$. (For the literature from [8] to [13], see [13].) In the present paper, f may be indefinite, and $m = 0$ in some results.

We note two obvious necessary conditions for a nonempty set of square-free solutions of (1.1).

(A) *The equation* (1.1) *has a real solution* $\boldsymbol{x} \neq \mathbf{0}$.

(B) *The congruence*

$$f(\boldsymbol{x}) \equiv m \pmod{(2D)^5} \tag{1.3}$$

has a solution $\boldsymbol{x}$ *with*

$$p^2 \nmid x_1, \ldots, p^2 \nmid x_n \text{ for each prime } p \mid 2D. \tag{1.4}$$

We always assume that condition A is satisfied. Condition B appears in Theorem 5.

Podsypanin uses a modified version of Kloosterman's refinement [11] of the Hardy-Littlewood circle method. In the present paper, we use the new form of the circle method due to Heath-Brown [9], and we also deduce one result (Theorem 4) from the work of Duke [6]. Heath-Brown obtains asymptotic formulae for the weighted sum

$$N(F, w) = \sum_{F(\boldsymbol{x})=0} w\left(\frac{\boldsymbol{x}}{P}\right),$$

where we write

$$F = f - m.$$

His results cover $n \geq 4$, m arbitrary, and $n = 3$, $m = 0$. The weight function w is assumed in [9] to be infinitely differentiable, with compact support not containing $\mathbf{0}$. The corresponding object of study here is

$$R(F, w) = \sum_{F(\boldsymbol{x})=0} \mu^2(\boldsymbol{x}) w\left(\frac{\boldsymbol{x}}{P}\right).$$

where $\boldsymbol{x}$ runs over the solutions of (1.1) in $\mathbb{Z}^n$. For simplicity, we restrict w a little further, assuming that $w \geq 0$, that $w(\boldsymbol{x}) > 0$ for some real solution $\boldsymbol{x} \neq \mathbf{0}$ of (1.1), and that $w(\boldsymbol{x}) = 0$ whenever $\pi_{\boldsymbol{x}} = 0$.

As in [9], we write

$$G = f - 1 \text{ if } m \neq 0; \qquad G = f \text{ if } m = 0.$$

The singular integral for both $N(F, w)$ and $R(F, w)$ is

$$\sigma_\infty(G, w) = \lim_{\beta \to 0+} \frac{1}{2\beta} \int_{|G(\boldsymbol{x})| \leq \beta} w(\boldsymbol{x}) d\boldsymbol{x}.$$

The limit exists and is positive ([9, Theorem 3]). For $n = 3$, we shall also need

$$\sigma_\infty(G) = \lim_{\beta\to 0+} \frac{1}{2\beta} \int_{|G(\boldsymbol{x})|\le\beta} d\boldsymbol{x}.$$

Turning to the singular series, this naturally has a different form for $N(F, w)$ and $R(F, w)$. Let

$$M(p^\nu) = \#\{\boldsymbol{x} \pmod{p^\nu} : F(\boldsymbol{x}) \equiv 0 \pmod{p^\nu}\},$$

for a prime power p^ν. For $\nu \ge 2$, let

$$M'(p^\nu) = \#\{\boldsymbol{x} \pmod{p^\nu} : F(\boldsymbol{x}) \equiv 0 \pmod{p^\nu}, p^2 \nmid x_1, \ldots, p^2 \nmid x_n\}. \tag{1.5}$$

The relevant 'densities' in [9], [5], [6] are the numbers

$$\sigma_p = \lim_{\nu\to\infty} \frac{M(p^\nu)}{p^{\nu(n-1)}},$$

whereas in the present paper we are concerned with the densities

$$\rho_p = \lim_{\nu\to\infty} \frac{M'(p^\nu)}{p^{\nu(n-1)}}. \tag{1.6}$$

Both limits σ_p and ρ_p exist, and we shall see that $\rho_p > 0$ for each p when condition B is satisfied.

For $N(F, w)$, the singular series is

$$\sigma(F) = \prod_p \sigma_p$$

if $n \ge 5$ or $n = 4$, $m \ne 0$. For $n = 4$, $m = 0$, D a non-square, the singular series is

$$\sigma^*(F) = \prod_p \left(1 - \frac{\chi(p)}{p}\right) \sigma_p.$$

Here the character χ is the Jacobi symbol $\left(\frac{D}{\cdot}\right)$. For $n = 3$, f positive-definite, the singular series is

$$\sigma^*(F) = \prod_p \left(1 - \frac{\chi^*(p)}{p}\right) \sigma_p.$$

Here $\chi^*(\cdot) = \left(-\frac{Dm}{\cdot}\right)$.

For $R(F, w)$, the singular series is

$$\rho(F) = \prod_p \rho_p$$

if $n \geq 5$ or $n = 4$, $m \neq 0$;

$$\rho^*(F) = \prod_p \left(1 - \frac{\chi(p)}{p}\right) \rho_p$$

for $n = 4$, $m = 0$. For $n = 3$, f positive-definite, the singular series for $R(m)$ is

$$\rho^*(F) = \prod_p \left(1 - \frac{\chi^*(p)}{p}\right) \rho_p.$$

Convergence of the infinite products is covered in §5.

We state Heath-Brown's and Duke's results alongside those obtained for $R(F, w)$, $R(m)$. We make the convention that $P \to \infty$ if we have $m = 0$, while if $m > 0$, we let m tend to infinity and take $P = m^{1/2}$.

For $n \geq 4$, $m \neq 0$, we have [9]

$$N(F, w) = \sigma_\infty(G, w)\sigma(F)m^{n/2-1} + O(m^{(n-1)/4+\epsilon}).$$

Our convention for implied constants whose dependence is not given explicitly is that they may depend on f, w and ϵ. As usual, ϵ denotes any sufficiently small positive number. We also introduce a small positive constant $\gamma = \gamma(n)$.

Theorem 1 *Let $n \geq 4$, $m \neq 0$. Then*

$$R(F, w) = \sigma_\infty(G, w)\rho(F)m^{n/2-1} + O(m^{(n-\gamma)/2-1}).$$

Now let $n \geq 5$, $m = 0$. Then [9]

$$N(F, w) = \sigma_\infty(F, w)\sigma(F)P^{n-2} + O(P^{(n-1+\delta)/2+\epsilon}),$$

where $\delta = 0$ for n odd, $\delta = 1$ for n even.

Theorem 2 *Let $n \geq 5$, $m = 0$. Then*

$$R(F, w) = \sigma_\infty(F, w)\rho(F)P^{n-2} + O(P^{n-2-\gamma}).$$

Suppose that $n = 4$, $m = 0$ and D is a non-square. Then [9]

$$N(F, w) = \sigma_\infty(F, w)L(1, \chi)\sigma^*(F)P^2 + O(P^{3/2+\epsilon}).$$

Theorem 3 *Let $n = 4$, $m = 0$ and suppose that D is not a square. Then*

$$R(F, w) = \sigma_\infty(F, w)L(1, \chi)\rho^*(F)P^2 + O(P^{2-\gamma}).$$

For $n = 3$, f positive-definite, let

$$r(f, m) = \#\{\boldsymbol{x} \in \mathbb{Z}^3 : f(\boldsymbol{x}) = m\}.$$

Duke [5] shows that, for m square-free,

$$r(f, m) = \sigma_\infty(G)L(1, \chi^*)\sigma^*(F)m^{1/2} + O(m^{1/2-1/28+\epsilon}).$$

(This is certainly not how he expresses the result, but see the introduction to §7 below.)

Theorem 4 *Let $n = 3$, let f be positive-definite and m square-free. Then*

$$R(m) = \sigma_\infty(G)L(1, \chi^*)\rho^*(F)m^{1/2} + O(m^{(1-\gamma)/2}).$$

By imposing condition B, we get a dominant main term in our theorems.

Theorem 5 *Suppose that condition B holds. Then in Theorems 1–4,*

$$1 \ll \rho(F) \le \sigma(F) \ll 1 \quad (n \ge 5), \tag{1.7}$$

$$m^{-\epsilon} \ll \rho(F) \le \sigma(F) \ll m^\epsilon \quad (n = 4, m \ne 0), \tag{1.8}$$

$$0 < \rho^*(F) \le \sigma^*(F) \quad (n = 4), \tag{1.9}$$

$$m^{-\epsilon} \ll \rho^*(F) \le \sigma^*(F) \ll m^\epsilon \quad (n = 3). \tag{1.10}$$

The plan of the paper is as follows. In §2 we prove an auxiliary bound for 'special' solutions of (1.1). In §3, we describe Heath-Brown's underlying method and record some of his results for weighted exponential integrals.

$$I_{q,F,w}(\boldsymbol{c}) = I_q(\boldsymbol{c}) = \int_{\mathbb{R}^n} w(\boldsymbol{x})h\left(\frac{q}{P}, \frac{F(\boldsymbol{x})}{P^2}\right) e_q(-\boldsymbol{c}\cdot\boldsymbol{x})d\boldsymbol{x}, \tag{1.11}$$

and exponential sums

$$S_{q,F}(\boldsymbol{c}) = S_q(\boldsymbol{c}) = \sum_{a=1}^{q}{}^{*} \sum_{\boldsymbol{b} \pmod q} e_q(aF(\boldsymbol{b}) + \boldsymbol{c}\cdot\boldsymbol{b}). \tag{1.12}$$

The function $h(x, y)$ will be described in §3. We write $\boldsymbol{c}\cdot\boldsymbol{x}$ for inner product in $\mathbb{R}^n$, and $e(\theta) = e^{2\pi i\theta}$, $e_q(z) = e\left(\frac{z}{q}\right)$. The sum $\sum_{a=1}^{q}{}^{*}$ is restricted by $(a, q) = 1$.

In §4, we begin the proofs of Theorems 1–3. It becomes obvious that we need results for the function $F_{\boldsymbol{d}}(\boldsymbol{x}) := F(d_1^2 x_1, \ldots, d_n^2 x_n)$ when $\boldsymbol{d}$ has positive coordinates, $\mu(\boldsymbol{d}) \neq 0$. The corresponding weight function is $w_{\boldsymbol{d}}(\boldsymbol{x}) := w(d_1^2 x_1, \ldots, d_n^2 x_n)$, and we must give counterparts of Heath-Brown's results for

$$I_q(\boldsymbol{d}, \boldsymbol{c}) := I_{q,F_{\boldsymbol{d}},w_{\boldsymbol{d}}}(\boldsymbol{c}),\ S_q(\boldsymbol{d}, \boldsymbol{c}) := S_{q,F_{\boldsymbol{d}}}(\boldsymbol{c}). \tag{1.13}$$

In §5, we construct $\rho(F)$, $\rho^*(F)$ from the $S_q(\boldsymbol{d}, \boldsymbol{c})$, and prove essential results about the singular series, including Theorem 5. In §6, we complete the proofs of Theorems 1–3. In §7, we introduce some basic notions from Siegel [14]. We then give the relatively straightforward deduction of Theorem 4 from a result of Duke [6].

I would like to thank the referee for detecting a number of errors and infelicities in the previous version of the paper.

§2 A subset of solutions of (1.1)

Proposition 1 *Suppose either that $n \geq 4$, or that $n = 3$ and f is positive-definite. Let $1 \leq h \leq P$ and fix i, $1 \leq i \leq n$. The equation* (1.1) *has $O(P^{n-2+\epsilon}h^{-1})$ solutions $\boldsymbol{x}$ in $\mathbb{Z}^n$ for which*

$$|\boldsymbol{x}| := \max_j |x_j| \leq P, \quad x_i \neq 0, \quad x_i \equiv 0 \pmod h. \tag{2.1}$$

It is noteworthy that the proposition does not extend to $n = 3$, f indefinite. For $1 \leq h \leq P$, the equation

$$x_1^2 - x_2^2 + x_3^2 = h^2$$

has more than P solutions (x_1, x_1, h) satisfying (2.1).

Lemma 1 *Let A, k be nonzero integers. Let $P > 1$. The number of solutions $(x, y) \in \mathbb{Z}^2$ of*

$$x^2 + Ay^2 = k \quad , \quad |(x, y)| \le P \tag{2.2}$$

is at most $C(A, \epsilon)P^\epsilon$.

In the proof, implied constants depend at most on A, ϵ. We write $d(\ell)$ for the divisor function, and $\omega(\ell)$ for the number of distinct prime divisors of ℓ.

Proof. A preliminary transformation $A = A'u^2$, $y' = uy$ enables us to assume that A is square-free. A simple divisor argument permits us to restrict attention to coprime x, y.

If $A = -1$, then $x - y$ and $x + y$ are divisors of k. Clearly there are $O(P^\epsilon)$ possibilities for x, y.

Now assume that $A \neq -1$. The quadratic form $x_1^2 + Ax_2^2$ has discriminant $d = -4A$. Note that d is not a square, since if $-A$ is at least 2 and square-free, then $-4A$ is not a square.

Consider a solution of (2.2) with coprime x, y. By Theorem 2.1 of Landau [12], the integers r, s and ℓ may be chosen in exactly one way so that

(i) $xs - yr = 1$;

(ii) $\ell^2 \equiv d \pmod{4k}$, $\quad 0 \le \ell < 2k$;

(iii) we have

$$x_1^2 + Ax_2^2 = ky_1^2 + \ell y_1 y_2 + my_2^2$$

with $m = (\ell^2 - d)/4k$, under the change of variables

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x & r \\ y & s \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

There are $O(P^\epsilon)$ possibilities for ℓ as x, y vary. To see this, factor $4k$ into prime powers,

$$4k = p_1^{m_1} \dots p_r^{m_r}.$$

The congruence

$$\ell^2 \equiv d \pmod{p_j^{m_j}} \tag{2.3}$$

yields

$$\ell = p_j^h \ell', \quad p_j \nmid \ell', \quad p_j^{\min(2h, m_j)} \mid d.$$

If $m_j \le 2h$, then $p_j^{m_j} | \, d$ and (2.3) has at most d solutions. Otherwise,

$$\ell'^2 \equiv d p_j^{-2h} \pmod{p_j^{m_j - 2h}}.$$

For each h, there are at most 4 possibilities for $\ell' \pmod{p_j^{m_j-2h}}$ ([12], Theorem 87). Hence there are most $4p_j^h$ possibilities for $\ell \pmod{p_j^{m_j}}$; overall, there are at most

$$4 \sum_{p_j^{2h} | \, d} p_j^h \le 8d$$

such ℓ. Since $k = O(P^2)$, we conclude that there are at most

$$(8d)^{\omega(4k)} = O(P^\epsilon)$$

possibilities for $\ell \pmod{k}$, giving the desired result since $0 \le \ell < 2k$.

It now suffices to show that once ℓ is fixed, satisfying (ii), there are $O(\log P)$ coprime x, y satisfying (i), (iii). We may restrict attention to x, y with

$$x > 0, \ y > 0.$$

Take a fixed coprime pair $x_0 \ge 0$, $y_0 \ge 0$ (which we may assume exists) with the property that $x_1^2 + Ax_2^2$ goes into $ky_1^2 + \ell y_1 y_2 + my_2^2$ under the change of variables with matrix $\begin{bmatrix} x_0 & r_0 \\ y_0 & s_0 \end{bmatrix}$. By following the argument on pp. 184–5 of [11], we arrive at the representation

$$x = \frac{t}{2}\, x_0 - Au\, y_0 \quad , \quad y = ux_0 + \frac{ty_0}{2},$$

for some integers t and u satisfying Pell's equation

$$t^2 - du^2 = 4. \tag{2.4}$$

Since there are $O(1)$ possible t, u if $d < 0$, we now suppose that $d > 0$. Theorem 111 of [12] provides an integer pair $g_1 > 0$, $g_2 > 0$ such that the formula

$$\frac{t + u\sqrt{d}}{2} = \pm \left(\frac{g_1 + g_2\sqrt{d}}{2} \right)^r (r \in \mathbb{Z})$$

yields all solutions of (2.4). Moreover,

$$2x + \sqrt{d}\, y = (2x_0 + \sqrt{d}\, y_0) \left(\frac{g_1 + g_2\sqrt{d}}{2} \right)^r,$$

by the argument on p. 186 of [12]. This implies

$$1 \ll \left(\frac{g_1 + g_2\sqrt{d}}{2} \right)^r \ll P.$$

There are $O(\log P)$ possible r, and the lemma follows.

Proof of Proposition 1. Suppose for example that $i = 1$. We first show that there is a nonsingular linear change of variables with rational coefficients (briefly, a *change of variables*),

$$\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \to \boldsymbol{z} = (x_1, z_1, \ldots, z_{n-1})$$

such that

$$\boldsymbol{z} \in \mathbb{Z}^n \quad \text{whenever} \quad \boldsymbol{x} \in \mathbb{Z}^n, \tag{2.5}$$

$$kf(x_1, \ldots, x_n) = cx_1^2 + x_1 \sum_{2<j<n} b_j z_j + z_1^2 + A_2 z_2^2 + A_3 z_3^2 + \cdots + A_{n-1} z_{n-1}^2, \tag{2.6}$$

$$k, c, b_j, A_j \text{ are integers, } k \neq 0, \text{ and } A_2 \neq 0. \tag{2.7}$$

Let B be the matrix obtained from M by deleting the first row and column. The rank r of B satisfies $n - 2 \le r \le n - 1$. In fact, $r = 2$ in the case $n = 3$, f positive-definite. For then r is the rank of the positive-definite binary form $f(0, x_2, x_3)$. By a standard result ([3, p. 392]), a change of variables $(x_2, \ldots, x_n) \to (y_1, \ldots, y_{n-1})$ gives

$$f(0, x_2, \ldots, x_n) = c_1 y_1^2 + \cdots + c_r y_r^2,$$

with $c_1 \ldots c_r \neq 0$. Now

$$\begin{aligned} f(x_1, \ldots, x_n) &= a_{11}x_1^2 + 2x_1(a_{12}x_2 + \cdots + a_{1n}x_n) + c_1 y_1^2 + \cdots + c_r y_r^2 \\ &= a_{11}x_1^2 + x_1(d_1 y_1 + \cdots + d_{n-1}y_{n-1}) + c_1 y_1^2 + \cdots + c_r y_r^2 \end{aligned}$$

for certain rationals $d_1, \dots, d_{n-1}$. For a suitable positive integer q, the further change of variables

$$w_j = q\left(y_j + \frac{b_j x_1}{2c_j}\right) \ (j = 1, 2), \qquad w_j = q y_j \quad (j > 2)$$

produces a change of variables $(x_1, \dots, x_n) \to (x_1, w_1, \dots, w_{n-1})$ with the property (2.5), such that

$$f(x_1, \dots, x_n) = g x_1^2 + x_1 \sum_{2<j<n} h_j w_j + u_1 w_1^2 + u_2 w_2^2 + \cdots + u_r w_r^2 \tag{2.8}$$

with $u_1 u_2 \neq 0$. We multiply f by a nonzero integer k to produce (i) integer coefficients $gk, h_1 k, \dots, h_{n-1} k, u_1 k, \dots, u_r k$; (ii) $u_1 k = s^2$ for some positive integer s. A final change of variables

$$z_1 = s w_1 \quad , \quad z_j = w_j \quad (j > 1)$$

does not disturb the property (2.5), and yields (2.6), (2.7).

It now suffices to show that the equation

$$c x_1^2 + x_1 \sum_{2<j<n} b_j z_j + z_1^2 + A_2 z_2^2 + \cdots + A_{n-1} z_{n-1}^2 = km \tag{2.9}$$

has $O(P^{n-2+\epsilon} h^{-1})$ solutions with

$$|(x_1, z_1, \dots, z_{n-1})| \ll P, \ x_1 \neq 0, \ h \mid x_1.$$

If $n = 3$, then x_1 determines z_1 and z_2 to within $O(P^\epsilon)$ possibilities. This follows from Lemma 1 if $c x_1^2 < km$, and from the positive-definiteness of f (which implies $A_2 > 0$) otherwise.

If $n \geq 4$, considerations of rank imply that either $b_3 \neq 0$ or $A_3 \neq 0$. We can give a satisfactory bound for the solutions not satisfying

$$c x_1^2 + x_1 \sum_{2<j<n} b_j z_j + A_3 z_3^2 + \cdots + A_{n-1} z_{n-1}^2 = km \tag{2.10}$$

using Lemma 1. For the remaining solutions, z_3 is determined via (2.10) to within 2 possibilities once z_j $(3 < j < n)$ and x_1 are given. Thus there are $O(P^{n-3} h^{-1})$ possible $z_3, \dots, z_{n-1}, x_1$. Since $z_1^2 + D z_2^2 = 0$, there are $O(P)$ possible z_1, z_2. This completes the proof.

§3 Heath-Brown's form of the circle method

Heath-Brown begins with a formula due essentially to Duke, Friedlander and Iwaniec [7]. Let

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

Let $\omega(x)$ be a suitable non-negative smooth function with support in $\left(\frac{1}{2}, 1\right)$. For $x > 0$, y real, let

$$h(x, y) = \sum_j \frac{1}{xj} \left(\omega(xj) - \omega(|y|/xj)\right).$$

Then for any $Q > 1$, we have

$$\delta_n = c_Q Q^{-2} \sum_{q=1}^{\infty} \sideset{}{^*}\sum_{a=1}^{q} e_q(an) h\left(\frac{q}{Q}, \frac{n}{Q^2}\right). \tag{3.1}$$

The constant c_Q satisfies

$$c_Q = 1 + O_N(Q^{-N}) \tag{3.2}$$

for any $N > 0$. Moreover, $h(x, y)$ is nonzero only for $x \leq \max(1, 2\,|y|)$. See [9], Theorem 1.

Now let $F = f - m$. We may write

$$N(F, w) = \sum_{\boldsymbol{x} \in \mathbb{Z}^n} w\left(\frac{\boldsymbol{x}}{P}\right) \delta_{F(\boldsymbol{x})}. \tag{3.3}$$

Heath-Brown uses (3.1) and the Poisson summation formula to rewrite the right-hand side of (3.3). In the present context, one chooses $Q = P$, and the result is

$$N(F, w) = c_P P^{-2} \sum_{\boldsymbol{c} \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(\boldsymbol{c}) I_q(\boldsymbol{c}) \tag{3.4}$$

([9, Theorem 2]).

We now quote some of the key lemmas of [9].

Lemma 2 ([9, Lemma 13]). *Let $N \geq 1$. For $q < P$,*

$$I_q(\mathbf{0}) = P^n\{\sigma_\infty(G, w) + O_{f,w,N}((q/P)^N)\}.$$

Lemma 3 ([9, Lemma 16]). *We have*

$$\frac{\partial}{\partial q^j} I_q(\mathbf{0}) \ll P^n q^{-j} \quad (j = 0, 1).$$

Lemma 4 ([9, Lemma 19]). *Let $N \geq 1$. For $\boldsymbol{c} \neq \mathbf{0}$,*

$$I_q(\boldsymbol{c}) \ll_{f,w,N} P^{n+1} q^{-1} |\boldsymbol{c}|^{-N}.$$

Lemma 5 ([9, Lemma 22]). *For $\boldsymbol{c} \neq \mathbf{0}$,*

$$I_q(\boldsymbol{c}) \ll P^n \left(\frac{P^2|\boldsymbol{c}|}{q^2}\right)^{\epsilon} \left(\frac{P|\boldsymbol{c}|}{q}\right)^{1-n/2}.$$

In the case $m = 0$, the same bound applies to $q \frac{\partial}{\partial q} I_q(\boldsymbol{c})$.

In the following lemma, F may be any polynomial in $\mathbb{Z}[X_1, \ldots, X_n]$.

Lemma 6 ([9, Lemma 23]). *If $(u, v) = 1$, then*

$$S_{uv}(\boldsymbol{c}) = S_u(\bar{v}\boldsymbol{c}) S_v(\bar{u}\boldsymbol{c}), \tag{3.5}$$

where $u\bar{u} \equiv 1 \pmod{v}$, $v\bar{v} \equiv 1 \pmod{u}$.

Lemma 7 *We have*

$$|S_q(\boldsymbol{c})|^2 \leq q^{n+2} \sum_{\substack{\boldsymbol{u} \pmod{q} \\ q \,|\, \boldsymbol{\nabla} F(\boldsymbol{u})}} 1 \tag{3.6}$$

where

$$\boldsymbol{\nabla} F(\boldsymbol{x}) = \left(\frac{\partial F}{\partial x_1}, \ldots, \frac{\partial F}{\partial x_n}\right).$$

(We use the abbreviation $q \,|\, \boldsymbol{a}$, or $\boldsymbol{a} \equiv \mathbf{0} \pmod{q}$, for $q \,| a_j$ $(1 \leq j \leq n)$.)

The inequality (3.6) is proved just before Lemma 25 in [9].

When referring to a specific point $\boldsymbol{y}$, we abuse notation slightly by writing $\frac{\partial F}{\partial y_i}$ for the value of the i-th component of $\boldsymbol{\nabla} F$ at $\boldsymbol{y}$.

We denote by $M^{-1}(\boldsymbol{x})$ the quadratic form whose matrix is M^{-1}. When $p \nmid 2D$, we may think of $M^{-1}(\boldsymbol{x})$ as being defined modulo p.

Lemma 8 ([9, Lemma 26]). *Let $p \nmid 2D$. We have*

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

except when n is even and p divides both m and $M^{-1}(\boldsymbol{c})$. When n is even, we have

$$S_p(\boldsymbol{c}) = -\left(\frac{(-1)^{n/2}D}{p}\right)p^{n/2} \tag{3.7}$$

if p divides exactly one of m, $M^{-1}(\boldsymbol{c})$, and

$$S_p(\boldsymbol{c}) = (p-1)\left(\frac{(-1)^{n/2}D}{p}\right)p^{n/2} \tag{3.8}$$

if p divides both m and $M^{-1}(\boldsymbol{c})$.

When n is odd, we have

$$S_p(\boldsymbol{c}) = \left(\frac{(-1)^{(n-1)/2}Dm}{p}\right)p^{(n+1)/2} \tag{3.9}$$

if $p \mid M^{-1}(\boldsymbol{c})$, and

$$S_p(\boldsymbol{c}) = \left(\frac{(-1)^{(n-1)/2}DM^{-1}(\boldsymbol{c})}{p}\right)p^{(n+1)/2} \tag{3.10}$$

if $p \mid m$.

§4 First steps of the proofs of Theorems 1–3

We add some further notations to those already adopted. We reserve the symbols $\boldsymbol{d} = (d_1, \dots, d_n)$, $\boldsymbol{t}$ for square-free points with positive coordinates. We write

$$\boldsymbol{d} \mid q \ \text{ if } \ d_j \mid q \quad (1 \le j \le n),$$

and

$$p^\nu \parallel \boldsymbol{a} \ \text{ if } \ p^\nu \mid \boldsymbol{a} \quad , \quad p^{\nu+1} \nmid a_j \ \text{ for some } j.$$

In the proof of Lemma 10, (a, b, c) denotes the g.c.d. of a, b, c.

With this notation, we have

$$R(F,w) = \sum_{\substack{\boldsymbol{y} \\ F(\boldsymbol{y})=0}} \sum_{\substack{\boldsymbol{d} \\ d_i^2 \mid y_i}} \mu(\boldsymbol{d}) w\left(\frac{\boldsymbol{y}}{P}\right).$$

Writing $\boldsymbol{y} = (d_1^2 x_1, \ldots, d_n^2 x_n)$ and interchanging summations,

$$R(F,w) = \sum_{\boldsymbol{d}} \mu(\boldsymbol{d}) \sum_{\substack{\boldsymbol{x} \\ F_{\boldsymbol{d}}(\boldsymbol{x})=0}} w_{\boldsymbol{d}}\left(\frac{\boldsymbol{x}}{P}\right). \tag{4.1}$$

The outer sum is actually finite, since

$$w_{\boldsymbol{d}}\left(\frac{\boldsymbol{x}}{P}\right) = 0 \quad \text{unless} \quad |\boldsymbol{d}| \ll P^{1/2}.$$

We now rewrite (4.1) in the form

$$R(F,w) = \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \mu(\boldsymbol{d}) \sum_{\substack{\boldsymbol{x} \\ F_{\boldsymbol{d}}(\boldsymbol{x})=0}} w_{\boldsymbol{d}}\left(\frac{\boldsymbol{x}}{P}\right) + \sum_{j=1}^{n} S_j \tag{4.2}$$

with 'small' $S_1, \ldots, S_n$. For any $\boldsymbol{d}$ with $\pi_{\boldsymbol{d}} > P^{2n\gamma}$, we write $j_{\boldsymbol{d}}$ for the least integer j with $d_j > P^{2\gamma}$. Now let

$$S_j = \sum_{d_j > P^{2\gamma}} S_j(d_j)$$

where

$$S_j(d_j) = \sum_{\substack{d_1,\ldots,d_{j-1},d_{j+1},\ldots,d_n \\ \pi_{\boldsymbol{d}} > P^{2n\gamma} \\ j_{\boldsymbol{d}}=j}} \mu(\boldsymbol{d}) \sum_{F_{\boldsymbol{d}}(\boldsymbol{x})=0} w_{\boldsymbol{d}}\left(\frac{\boldsymbol{x}}{P}\right).$$

We treat each S_j in the same way. Taking $j=1$, we collect terms for which $(d_2^2 x_2, \ldots, d_n^2 x_n)$ takes a fixed value $(y_2, \ldots, y_n)$. For a given value of d_1,

$$S_1(d_1) \ll P^{\epsilon} \sum_{\substack{x_1, y_2, \ldots, y_n \\ (4.3)}} 1,$$

where the last summation extends over values with

$$x_1 \ne 0, \quad F(d_1^2 x_1, y_2, \ldots, y_n) = 0, \ |(d_1^2 x_1, y_2, \ldots, y_n)| \ll P. \tag{4.3}$$

An application of Proposition 1 yields

$$S_1 \ll \sum_{d_1 > P^{2\gamma}} \frac{P^{n-2+\epsilon}}{d_1^2}. \tag{4.4}$$

We conclude that

$$\sum_{j=1}^{n} S_j \ll P^{n-2-\gamma}. \tag{4.5}$$

We now combine (4.2), (4.5) with an application of (3.4) for every pair $F = F_{\boldsymbol{d}}$, $w = w_{\boldsymbol{d}}$ with $\pi_{\boldsymbol{d}} \le P^{2n\gamma}$. This yields

(4.6)

$$R(F, w) = c_P P^{-2} \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \mu(\boldsymbol{d}) \sum_{\boldsymbol{c}} \sum_{q=1}^{\infty} q^{-n} S_q(\boldsymbol{d}, \boldsymbol{c}) I_q(\boldsymbol{d}, \boldsymbol{c}) + O(P^{n-2-\gamma}).$$

We must now bring dependence on $\boldsymbol{d}$ into the arguments of [9]. This is easy for $I_q(\boldsymbol{d}, \boldsymbol{c})$. We have

$$I_q(\boldsymbol{d}, \boldsymbol{c}) = \int_{\mathbb{R}^n} w\left(\frac{d_1^2 x_1}{P}, \ldots, \frac{d_n^2 x_n}{P}\right) h\left(\frac{q}{P}, \frac{F(d_1^2 x_1, \ldots, d_n^2 x_n)}{P^2}\right) e_q(-\boldsymbol{c} \cdot \boldsymbol{x}) d\boldsymbol{x}.$$

We obtain

$$I_q(\boldsymbol{d}, \boldsymbol{c}) = \frac{1}{\pi_{\boldsymbol{d}}^2} I_q\left(\frac{c_1}{d_1^2}, \ldots, \frac{c_n}{d_n^2}\right) \tag{4.7}$$

on substituting $(y_1, \ldots, y_n) = (d_1^2 x_1, \ldots, d_n^2 x_n)$.

From (4.7) and Lemmas 2–5,

$$I_q(\boldsymbol{d}, \boldsymbol{0}) = \frac{P^n}{\pi_{\boldsymbol{d}}^2} \left\{ \sigma_\infty(G, w) + O_{f,w,N}\left(\left(\frac{q}{P}\right)^N\right) \right\} \tag{4.8}$$

for $q < P$,

$$\frac{\partial}{\partial q^j} I_q(\boldsymbol{d}, \boldsymbol{0}) \ll \frac{P^n}{\pi_{\boldsymbol{d}}^2} q^{-j} \quad (j = 0, 1), \tag{4.9}$$

$$I_q(\boldsymbol{d}, \boldsymbol{c}) \ll_{f,w,N} \pi_{\boldsymbol{d}}^{2N} P^{n+1} q^{-1} |\boldsymbol{c}|^{-N} \quad (\boldsymbol{c} \ne \boldsymbol{0}), \tag{4.10}$$

$$I_q(\boldsymbol{d}, \boldsymbol{c}) \ll P^n \left(\frac{P^2 |\boldsymbol{c}|}{q^2}\right)^{\epsilon} \pi_{\boldsymbol{d}}^n \left(\frac{P |\boldsymbol{c}|}{q}\right)^{1-n/2} \quad (\boldsymbol{c} \ne \boldsymbol{0}) \tag{4.11}$$

and

$$q\,\frac{\partial}{\partial q}\,I_q(\boldsymbol{d},\boldsymbol{c}) \ll P^n\left(\frac{P^2|\boldsymbol{c}|}{q^2}\right)^{\epsilon}\pi_{\boldsymbol{d}}^n\left(\frac{P|\boldsymbol{c}|}{q}\right)^{1-n/2} \qquad (\boldsymbol{c}\neq\boldsymbol{0}, m=0). \tag{4.12}$$

(Since we do not aim for a particularly good value of γ, we are not economical with powers of $\pi_{\boldsymbol{d}}$.)

We now turn to $S_q(\boldsymbol{d},\boldsymbol{c})$. We adapt the arguments of [9], §11.

Lemma 9 *We have*

$$S_q(\boldsymbol{d},\boldsymbol{c}) \ll q^{1+n/2}(d_1^2,q)\dots(d_n^2,q).$$

Proof. This is an application of Lemma 7. We note that

$$\nabla F_{\boldsymbol{d}}(\boldsymbol{u}) = 2(d_1^2L_1(\boldsymbol{u}^{(\boldsymbol{d})}),\dots,d_n^2L_n(\boldsymbol{u}^{(\boldsymbol{d})}))$$

where

$$L_j(\boldsymbol{x}) = \sum_{j=1}^n a_{ij}x_j \quad , \ \boldsymbol{u}^{(\boldsymbol{d})} = (d_1^2u_1,\dots,d_n^2u_n).$$

Let $\boldsymbol{u}$ be a solution of

$$\boldsymbol{\nabla} F_{\boldsymbol{d}}(\boldsymbol{u}) \equiv \boldsymbol{0} \pmod{q}. \tag{4.13}$$

There are $O((d_1^2,q)\dots(d_n^2,q))$ possibilities for $\boldsymbol{v}$, where

$$\boldsymbol{v} = (L_1(\boldsymbol{u}^{(\boldsymbol{d})}),\dots,L_n(\boldsymbol{u}^{(\boldsymbol{d})})). \tag{4.14}$$

For a fixed $\boldsymbol{v}$, multiply the equation (between column vectors)

$$M\boldsymbol{u}^{(\boldsymbol{d})} = \boldsymbol{v}$$

by the adjoint of M. This gives

$$D\boldsymbol{u}^{(\boldsymbol{d})} = (\operatorname{adj} M)\boldsymbol{v}.$$

It follows that there are $O(1)$ possible $\boldsymbol{u}^{(\boldsymbol{d})}$ associated with $\boldsymbol{v}$ in (4.14), and there are accordingly $O((d_1^2,q)\dots(d_n^2,q))$ possibilities for $\boldsymbol{u}$ associated with $\boldsymbol{v}$. Hence (4.13) has $O((d_1^2,q)^2\dots(d_n^2,q)^2)$ solutions $\boldsymbol{u}$ (mod q). An application of (3.6) completes the proof.

Lemma 10 *For $X > 1$, we have*

$$\sum_{q \le X} |S_q(\boldsymbol{d}, \boldsymbol{c})| \ll \pi_{\boldsymbol{d}}^2 X^{(3+n)/2+\epsilon}(m + |\boldsymbol{c}| + 1)^\epsilon \tag{4.15}$$

except when n is even and $m = M^{-1}(\boldsymbol{c}) = 0$, in which case we have

$$\sum_{q \le X} |S_q(\boldsymbol{d}, \boldsymbol{c})| \ll \pi_{\boldsymbol{d}}^2 X^{(4+n)/2}. \tag{4.16}$$

Proof. We write $q = uv$ where

$$u = \prod_{\substack{p \,\|\, q \\ p \nmid \pi_{\boldsymbol{d}}}} p \qquad , v = \prod_{\substack{p^\nu \| q \\ p \,|\, \pi_{\boldsymbol{d}}}} p^\nu \prod_{\substack{p^\nu \,\|\, q \\ \nu \ge 2 \\ p \nmid \pi_{\boldsymbol{d}}}} p^\nu .$$

Thus $(u, v) = 1$. Lemmas 6 and 9 yield

$$S_v(\boldsymbol{d}, \boldsymbol{c}) \ll v^{1+n/2}(d_1^2, v) \dots (d_n^2, v) \, |S_{\boldsymbol{u}}(\boldsymbol{d}, \bar{v}\boldsymbol{c})|. \tag{4.17}$$

Moreover,

$$S_u(\boldsymbol{d}, \bar{v}\boldsymbol{c}) \ll C^{\omega(u)} u^{(n+1)/2}(u, m, M^{-1}(\boldsymbol{c}))^\lambda \tag{4.18}$$

from Lemma 8, where C is a constant and

$$\lambda = \begin{cases} \frac{1}{2} & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd.} \end{cases}$$

Combining (4.17), (4.18),

$$S_q(\boldsymbol{d}, \boldsymbol{c}) \ll \pi_{\boldsymbol{d}}^2 v^{1+n/2} u^{(n+1)/2+\epsilon}(u, m, M^{-1}(\boldsymbol{c}))^\lambda .$$

As pointed out on p. 193 of [9],

$$\sum_{u \le U} (u, k) \le U d(k)$$

for any integer $k \neq 0$. The relevant value of k is $O(m + |\boldsymbol{c}|^2)$. Thus, unless n is even and $m = M^{-1}(\boldsymbol{c}) = 0$,

$$\sum_{q \le X} |S_q(\boldsymbol{d}, \boldsymbol{c})| \ll \pi_{\boldsymbol{d}}^2 X^{(1+n)/2+\epsilon} \sum_{v \le X} v^{1/2} \sum_{u \le X/v} u^\epsilon (u, m, M^{-1}(\boldsymbol{c}))$$

$$\ll \pi_{\boldsymbol{d}}^2 X^{(3+n)/2+2\epsilon}(m + |\boldsymbol{c}| + 1)^\epsilon \sum_{v \le X} v^{-1/2}$$

where v runs over numbers av', $a|\pi_{\boldsymbol{d}}$, v' square-full. It is easy to see that

$$\sum_{v\le X} v^{-1/2} \ll X^{\epsilon},$$

and (4.15) follows. As for (4.16), this is an immediate consequence of Lemma 9.

We now focus on the case treated in Theorem 3 and suppose that $M^{-1}(\boldsymbol{c}) = 0$. The series

$$\zeta(s,\boldsymbol{d},\boldsymbol{c}) := \sum_{q=1}^{\infty} q^{-s} S_q(\boldsymbol{d},\boldsymbol{c})$$

converges absolutely for Re $s := \sigma > 4$, and

$$\zeta(s,\boldsymbol{d},\boldsymbol{c}) = \prod_p \sum_{\nu=0}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{c})$$

[9, pp. 193–195]. We see from [9, p. 195] that the individual factors satisfy

$$(4.19)\qquad (1-\chi(p)p^{3-s})\left(1+\sum_{\nu=1}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{c})\right) = 1 + O(p^{-1-\epsilon})\ (p\nmid \pi_{\boldsymbol{d}})$$

in the larger half-plane $\sigma \ge \frac{7}{2}+\epsilon$. Here of course we use

$$\left(\frac{D\pi_{\boldsymbol{d}}^4}{p}\right) = \left(\frac{D}{p}\right) = \chi(p).$$

We need a corresponding bound for divisors p of $\pi_{\boldsymbol{d}}$. For $\sigma \ge \frac{7}{2}+\epsilon$, Lemma 9 yields

$$\begin{aligned}(1-\chi(p)p^{3-s})&\left(1+\sum_{\nu\ge1} p^{-s\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{c})\right)\\ &\ll 1+\sum_{\nu\ge 1} p^{-(1/2+\epsilon)\nu}(d_1^2,p^\nu)\dots(d_4^2,p^\nu)\\ &\ll (d_1^2,p^2)\dots(d_4^2,p^2),\end{aligned}$$

giving

$$(4.20)\qquad \prod_{p\,|\,\pi_{\boldsymbol{d}}} \max\left(1, \left|(1-\chi(p)p^{3-s})\left(1+\sum_{\nu=1}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{c})\right)\right|\right) \ll \pi_{\boldsymbol{d}}^{2+\epsilon}.$$

Combining this with (4.19), we obtain a $\boldsymbol{d}$-dependent version of a portion of [9], Lemma 29.

Lemma 11 *Make the hypotheses of Theorem 3 and suppose that* $M^{-1}(\boldsymbol{c}) = 0$. *Then* $\zeta(s, \boldsymbol{d}, \boldsymbol{c})$ *has an analytic continuation to the region* $\sigma > \frac{7}{2}$, *and*

$$\zeta(s, \boldsymbol{d}, \boldsymbol{c}) = L(s-3, \chi)\nu(s, \boldsymbol{d}, \boldsymbol{s}),$$

with

$$\nu(s, \boldsymbol{d}, \boldsymbol{c}) = \prod_p (1 - \chi(p)p^{3-s}) \left(1 + \sum_{\nu=1}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{c})\right)$$
$$\ll \pi_{\boldsymbol{d}}^{2+\epsilon} \quad \left(\sigma \geq \frac{7}{2} + \epsilon\right).$$

For $n = 3$, f positive-definite, m square-free, we write

$$\zeta(s, \boldsymbol{d}) = \sum_{q=1}^{\infty} q^{-s} S_q(\boldsymbol{d}, \boldsymbol{0}) \quad (\sigma > 3).$$

Lemma 12 *Make the hypothesis of Theorem 4. The Dirichlet series* $\zeta(s, \boldsymbol{d})$ *converges absolutely for* $\sigma > 3$, *and*

$$\zeta(s, \boldsymbol{d}) = \prod_p \sum_{\nu=0}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0}).$$

We have

$$\sum_{\nu=0}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0}) = 1 + \chi^*(p)p^{2-s} + O(p^{-1-\epsilon}) \tag{4.21}$$

for $p \nmid 2D\pi_{\boldsymbol{d}}$, $\sigma \geq \frac{5}{2} + \epsilon$.

The function $\zeta(s, \boldsymbol{d})$ *has an analytic continuation to* $\sigma > 5/2$, *and*

$$\zeta(s, \boldsymbol{d}) = L(s-2, \chi^*)\nu(s, \boldsymbol{d}),$$

with

$$\nu(s, \boldsymbol{d}) = \prod_p (1 - \chi^*(p)p^{2-s}) \left(1 + \sum_{\nu=1}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0})\right)$$
$$\ll \pi_{\boldsymbol{d}}^{2+\epsilon} \quad \left(\sigma \geq \frac{5}{2} + \epsilon\right).$$

Proof. From (3.9),

$$S_p(\boldsymbol{d},\mathbf{0}) = \chi^*(p)p^2 \quad (p \nmid 2D\pi_{\boldsymbol{d}}).$$

We can deduce the value of $S_{p^\nu}(\boldsymbol{d},\mathbf{0})$ for $\nu \geq 2$ from Hilfssatze 12, 13 and 16 of Siegel [14], if we recall the formula

$$\frac{M(p^N)}{p^{N(n-1)}} = \sum_{\nu=0}^{N} p^{-n\nu} S_{p^\nu}(\mathbf{0})$$

(compare (5.12) below). We obtain

$$S_{p^\nu}(\boldsymbol{d},\mathbf{0}) = 0 \quad (\nu \geq 2,\ p \nmid 2D\pi_{\boldsymbol{d}}, p \nmid m), \tag{4.22}$$

(whether or not m is square-free). If $p \,\|\, m$, $p \nmid 2D\pi_{\boldsymbol{d}}$, then

$$S_{p^\nu}(\boldsymbol{d},\mathbf{0}) = \begin{cases} -p^4 & (\nu = 2) \\ 0 & (\nu \geq 3). \end{cases} \tag{4.23}$$

Alternatively, (4.22), (4.23) can be deduced from [9], Lemma 24.

We conclude that (4.21) holds for $p \nmid 2D\pi_{\boldsymbol{d}}$, $\sigma \geq 5/2 + \epsilon$. Consequently,

$$\prod_{p \nmid 2D\pi_{\boldsymbol{d}}} \max\left(1, \left|\left(1 - \chi^*(p)p^{2-s}\right)\left(1 + \sum_{\nu=1}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d},\mathbf{0})\right)\right|\right) \ll 1 \quad \left(\sigma \geq \frac{5}{2} + \epsilon\right). \tag{4.24}$$

On the other hand, by a variant of the argument leading to (4.20),

$$\prod_{p \mid 2D\pi_{\boldsymbol{d}}} \max\left(1, \left|(1 - \chi^*(p)p^{2-s})\left(1 + \sum_{\nu=1}^{\infty} p^{-s\nu} S_{p^\nu}(\boldsymbol{d},\mathbf{0})\right)\right|\right) \ll \pi_{\boldsymbol{d}}^{2+\epsilon} \quad \left(\sigma \geq \frac{5}{2} + \epsilon\right). \tag{4.25}$$

The lemma follows at once from (4.24), (4.25).

We shall make several applications of a 'Perron formula.'

Lemma 13 *Let K, b, c be positive constants and λ a real constant, $\lambda + c > 1 + b$. Let $a_1, a_2, \ldots$ be complex numbers,*

$$|a_\ell| \leq K\ell^b.$$

Define

$$h(s) = \sum_{\ell=1}^{\infty} \frac{a_\ell}{\ell^s} \qquad (\sigma > 1 + b).$$

Let $x > 1$, $T > 1$, $x - 1/2 \in \mathbb{Z}$. Then

$$\sum_{\ell \leq x} \frac{a_\ell}{\ell^\lambda} - \frac{1}{2\pi i} \int_{c-iT}^{c+iT} h(s+\lambda) \, \frac{x^s}{s} \, ds = O\left(\frac{Kx^c}{T}\right). \tag{4.26}$$

Implied constants in Lemma 13 and its proof depend only on $\lambda + c - b$.

Proof. By the proof of Lemma 3.12 of [15], the left-hand side of (4.26) is

$$\ll \frac{x^c}{T} \sum_{\ell=1}^{\infty} \frac{|a_\ell|}{\ell^{\lambda+c} |\log \frac{x}{\ell}|} \ll \frac{Kx^c}{T} S,$$

where

$$S = \sum_{\ell=1}^{\infty} \frac{1}{\ell^{\lambda+c-b} |\log \frac{x}{\ell}|}.$$

Separating S into contributions from $\ell \notin \left(\frac{x}{2}, 2x\right)$, $\ell \in \left(\frac{x}{2}, 2x\right)$ as in [15], we obtain

$$\begin{aligned} S &\ll \sum_{\ell=1}^{\infty} \frac{1}{\ell^{\lambda+c-b}} + x^{-\lambda-c+b} \sum_{1 \leq |r| < 2x} \frac{x}{|r|} \\ &\ll 1 + x^{1+b-\lambda-c} \log x \ll 1. \end{aligned}$$

The lemma follows at once.

Lemma 14 *Make the hypothesis of Theorem 3. For $X > 1$, we have*

$$\sum_{q \leq X} S_q(\boldsymbol{d}, \boldsymbol{c}) = O(\pi_{\boldsymbol{d}}^{2+\epsilon} X^{7/2+\epsilon}), \tag{4.27}$$

and

$$\sum_{q\le X} q^{-4} S_q(\boldsymbol{d},\boldsymbol{0}) = \zeta(4,\boldsymbol{d},\boldsymbol{0}) + O(\pi_{\boldsymbol{d}}^{2+\epsilon} X^{-1/2+\epsilon}). \tag{4.28}$$

In particular,

$$\sum_{q=1}^{\infty} q^{-4} S_q(\boldsymbol{d},\boldsymbol{0}) = \zeta(4,\boldsymbol{d},\boldsymbol{0}).$$

Proof. For (4.27), we apply Lemma 13 with $a_\ell = S_\ell(\boldsymbol{d},\boldsymbol{c})$, $b = 3$, $\lambda = 0$, $x = [X] + 1/2$, $T = x^{10}$. According to Lemma 9, we may take $K \ll \pi_{\boldsymbol{d}}^2$. Now

$$\sum_{q\le X} S_q(\boldsymbol{d},\boldsymbol{c}) = \frac{1}{2\pi i}\int_{5-iT}^{5+iT} \zeta(s,\boldsymbol{d},\boldsymbol{c})\,\frac{x^s}{s}\,ds + O(\pi_{\boldsymbol{d}}^2 X^{-1}).$$

We move the line of integration back to

$$\operatorname{Re} s = \frac{7}{2} + \epsilon.$$

On the segments $\left[\frac{7}{2}+\epsilon, 5\right] \pm iT$, we have

$$L(s-3,\chi) \ll T^{1/2},$$

while

$$\frac{\nu(s,\boldsymbol{d},\boldsymbol{c})x^s}{s} \ll \pi_{\boldsymbol{d}}^{2+\epsilon} T^{-1/2}$$

from Lemma 11. Thus these segments contribute $O(\pi_{\boldsymbol{d}}^{2+\epsilon})$. Moreover,

$$\int_{-T}^{T} \left|\zeta\left(\frac{7}{2}+\epsilon+it,\,\boldsymbol{d},\,\boldsymbol{c}\right)\right| \frac{dt}{1+|t|} \ll \pi_{\boldsymbol{d}}^{2+\epsilon}\log T$$

from the mean value estimate

$$\int_0^U |L(\sigma+it,\chi)|^2 dt \ll_{D,\sigma} U \quad \left(\frac{1}{2} < \sigma < 1\right).$$

Hence the segment $\left[\frac{7}{2}+\epsilon-iT,\ \frac{7}{2}+\epsilon+iT\right]$ contributes $O\left(\pi_{\boldsymbol{d}}^{2+\epsilon} X^{\frac{7}{2}+2\epsilon}\right)$, proving (4.27).

Turning to (4.28), we choose a_ℓ, b, x, T as before, but now $\lambda = 4$, $c = 1$. This leads to

$$\sum_{q \le X} \frac{S_q(\boldsymbol{d}, \mathbf{0})}{q^4} = \frac{1}{2\pi i} \int_{1-iT}^{1+iT} \zeta(4+s, \boldsymbol{d}, \mathbf{0}) \frac{x^s}{s}\, ds + O(\pi_{\boldsymbol{d}}^2 X^{-1}).$$

We move the line of integration back to $\sigma = -\frac{1}{2}+\epsilon$. We estimate the integrals along segments much as before, but now there is a contribution $\zeta(4, \boldsymbol{d}, \mathbf{0})$ from the pole at 0, and the outcome is (4.28).

Lemma 15 *Under the hypotheses of Theorem 4, we have*

$$\sum_{q \le X} q^{-3} S_q(\boldsymbol{d}, \mathbf{0}) = \zeta(3, \boldsymbol{d}) + O(\pi_{\boldsymbol{d}}^{2+\epsilon} X^{-1/2+\epsilon}). \tag{4.29}$$

for $X > 1$, and in particular

$$\sum_{q=1}^{\infty} q^{-3} S_q(\boldsymbol{d}, \mathbf{0}) = \zeta(3, \boldsymbol{d}).$$

Proof. We apply Lemma 13 with $a_\ell = S_\ell(\boldsymbol{d}, \mathbf{0})$, $b = \frac{5}{2}$, $\lambda = 3$, $c = 1$, $x = [X] + 1/2$, $T = x^{10}$, $K \ll \pi_{\boldsymbol{d}}^2$. This gives

$$\sum_{q \le X} q^{-3} S_q(\boldsymbol{d}, \mathbf{0}) = \frac{1}{2\pi i} \int_{1-iT}^{1+iT} \zeta(3+s, \boldsymbol{d}) \frac{x^s}{s}\, ds + O\left(\frac{\pi_{\boldsymbol{d}}^2}{X}\right).$$

We move the line of integration back to $\sigma = -\frac{1}{2} + \epsilon$. The proof is completed in the same way as the proof of (4.28), using Lemma 12 in place of Lemma 11.

§5 The singular series

The next three lemmas are valid for a general F in $\mathbb{Z}[X_1, \ldots, X_n]$. Similar results can be found in Baker and Brüdern [2], but some blemishes there have been removed. We define $M'(p^N)$, ρ_p and $S_q(\boldsymbol{d}, \mathbf{0})$ via (1.5), (1.6), (1.12) and (1.13). Let

$$B_q(s) = \sum_{\boldsymbol{d} \mid q} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^s} S_q(\boldsymbol{d}, \mathbf{0}).$$

Lemma 16 *Let* $q \geq 1$, $\operatorname{Re} s > 1$. *The multiple series*

$$\sum_{\boldsymbol{t}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} S_q(\boldsymbol{t}, \boldsymbol{0}) \tag{5.1}$$

converges absolutely with sum

$$B_q(s)\zeta(s)^{-n} \prod_{p\,|\,q} (1 - p^{-s})^{-n}. \tag{5.2}$$

Proof. We rewrite the sum in (5.1) as

$$\sum_{\substack{\boldsymbol{t}' \\ (\pi_{\boldsymbol{t}'}, q) = 1}} \frac{\mu(\boldsymbol{t}')}{\pi_{\boldsymbol{t}'}^s} \sum_{\boldsymbol{d}\,|\,q} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^s} S_q(\boldsymbol{d}, \boldsymbol{0}) = \sum_{\substack{\boldsymbol{t}' \\ (\pi_{\boldsymbol{t}'}, q) = 1}} \frac{\mu(\boldsymbol{t}')}{\pi_{\boldsymbol{t}'}^s} B_q(s) \tag{5.3}$$

on expressing t_j uniquely as $t_j = d_j t_j'$, $d_j \,|\, q$, $(t_j', q) = 1$ and observing that $S_q(\boldsymbol{t}, \boldsymbol{0}) = S_q(\boldsymbol{d}, \boldsymbol{0})$. The proof is now completed by observing that in (5.3),

$$\begin{aligned} \sum_{\substack{\boldsymbol{t}' \\ (\pi_{\boldsymbol{t}'}, q) = 1}} \frac{\mu(\boldsymbol{t}')}{\pi_{\boldsymbol{t}'}^s} &= \prod_{p \nmid q} (1 - p^{-s})^n \\ &= \zeta(s)^{-n} \prod_{p\,|\,q} (1 - p^{-s})^{-n}. \end{aligned}$$

A variant of this argument yields, for $\sigma > 1$,

$$\sum_{\boldsymbol{t}} \frac{1}{\pi_{\boldsymbol{t}}^\sigma} |S_q(\boldsymbol{t}, \boldsymbol{0})| \ll_\sigma \sum_{\boldsymbol{d}\,|\,q} \frac{1}{\pi_{\boldsymbol{d}}^\sigma} |S_q(\boldsymbol{d}, \boldsymbol{0})|. \tag{5.4}$$

Lemma 17 $B_q(s)$ *is multiplicative in* q.

Proof. For $(q, q') = 1$, we have

$$B_{qq'}(s) = \sum_{\boldsymbol{d}\,|\,q,\, \boldsymbol{d}'\,|\,q'} \frac{\mu(\boldsymbol{d})\mu(\boldsymbol{d}')}{\pi_{\boldsymbol{d}}^s \pi_{\boldsymbol{d}'}^s} S_{qq'}(\boldsymbol{d}'', \boldsymbol{0})$$

(where $d_j'' = d_j d_j'$)

$$\begin{aligned} &= \sum_{\boldsymbol{d}\,|\,q,\, \boldsymbol{d}'\,|\,q'} \frac{\mu(\boldsymbol{d})\mu(\boldsymbol{d}')}{\pi_{\boldsymbol{d}}^s \pi_{\boldsymbol{d}'}^s} S_q(\boldsymbol{d}, \boldsymbol{0}) S_q(\boldsymbol{d}', \boldsymbol{0}) \\ &= B_q(s) B_{q'}(s). \end{aligned}$$

In the second equality, we use Lemma 6:

$$S_{qq'}(\boldsymbol{d}'', \boldsymbol{0}) = S_q(\boldsymbol{d}'', \boldsymbol{0}) S_{q'}(\boldsymbol{d}'', \boldsymbol{0}) = S_q(\boldsymbol{d}, \boldsymbol{0}) S_{q'}(\boldsymbol{d}', \boldsymbol{0}).$$

Lemma 18 *Suppose that* $\sigma \geq 1 + \epsilon$ *and*

$$T := \sum_{q=1}^{\infty} \frac{1}{q^n} \sum_{\boldsymbol{d} \mid q} \frac{|S_q(\boldsymbol{d}, \boldsymbol{0})|}{\pi_{\boldsymbol{d}}^{\sigma}} < \infty. \tag{5.5}$$

The multiple series

$$\mathfrak{S}(s) = \sum_{\boldsymbol{t}, q} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^{s} q^n} S_q(\boldsymbol{t}, \boldsymbol{0}) \tag{5.6}$$

converges absolutely, with $|\mathfrak{S}(s)| \ll T$ *and*

$$\mathfrak{S}(s) = \zeta(s)^{-n} \prod_p \left(1 + (1 - p^{-s})^{-n} \sum_{\nu \geq 1} p^{-n\nu} B_{p^\nu}(s)\right). \tag{5.7}$$

For $s = 2$*, we have the further expression*

$$\mathfrak{S}(2) = \prod_p \rho_p. \tag{5.8}$$

Proof. We appeal to (5.4) and (5.5) to obtain

$$\sum_{\boldsymbol{t}, q} \frac{1}{\pi_{\boldsymbol{t}}^{\sigma} q^n} |S_q(\boldsymbol{t}, \boldsymbol{0})| \ll \sum_{q=1}^{\infty} \frac{1}{q^n} \sum_{\boldsymbol{d} \mid q} \frac{|S_q(\boldsymbol{d}, \boldsymbol{0})|}{\pi_{\boldsymbol{d}}^{\sigma}} = T,$$

proving the absolute convergence and $|\mathfrak{S}(s)| \ll T$. Now Lemma 16 gives

$$\begin{aligned} \mathfrak{S}(s) &= \sum_{q=1}^{\infty} \frac{1}{q^n} \sum_{\boldsymbol{t}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^{s}} S_q(\boldsymbol{t}, \boldsymbol{0}) \\ &= \zeta(s)^{-n} \sum_{q=1}^{\infty} \frac{1}{q^n} B_q(s) \prod_{p \mid q} (1 - p^{-s})^{-n}. \end{aligned}$$

Given the absolute convergence in (5.5), a standard result on multiplicative functions now yields (5.7).

In order to deduce (5.8), it suffices to show that, for $N \geq 2$,

$$1 + (1 - p^{-2})^{-n} \sum_{\nu=1}^{N} p^{-n\nu} B_{p^\nu}(2) = (1 - p^{-2})^{-n} \frac{M'(p^N)}{p^{N(n-1)}}. \tag{5.9}$$

For later use, we note that the identity (5.9) does not depend on (5.5). Moreover, for the limit relation

$$1 + (1 - p^{-2})^{-n} \sum_{\nu=1}^{\infty} p^{-n\nu} B_{p^\nu}(2) = (1 - p^{-2})^{-n} \rho_p,$$

we need only assume that

$$\sum_{\nu=1}^{\infty} p^{-n\nu} \sum_{\boldsymbol{d} \mid p} \pi_{\boldsymbol{d}}^{-2} \,|\, S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0})| < \infty \quad \textit{for all } p. \tag{5.10}$$

By the inclusion-exclusion principle,

$$M'(p^N) = \sum_{\boldsymbol{d} \mid p} \mu(\boldsymbol{d}) M(\boldsymbol{d}, p^N),$$

where

$$M(\boldsymbol{d}, p^N) = \#\{\boldsymbol{x} \pmod{p^N} : d_j^2 \,|\, x_j \quad (j = 1, \ldots, n), \\ F(\boldsymbol{x}) \equiv 0 \pmod{p}\}.$$

We may write

$$M(\boldsymbol{d}, p^N) = \frac{1}{\pi_{\boldsymbol{d}}^2 p^N} \sum_{b=1}^{p^N} \sum_{\boldsymbol{x} \pmod{p^N}} e\left(\frac{bF_{\boldsymbol{d}}(\boldsymbol{x})}{p^N}\right). \tag{5.11}$$

because, in the sum (5.11), $(d_1^2 x_1, \ldots, d_n^2 x_n)$ runs $\pi_{\boldsymbol{d}}^2$ times over the vectors $\boldsymbol{y}$ with $d_j^2 \,|\, y_j$ $(j = 1, \ldots, n)$. Now

$$(5.12)\qquad \sum_{b=1}^{p^N} \sum_{\boldsymbol{x}\ (\mathrm{mod}\ p^N)} e\left(\frac{bF_{\boldsymbol{d}}(\boldsymbol{x})}{p^N}\right)$$

$$= \sum_{\nu=0}^{N} \sideset{}{^*}\sum_{a=1}^{p^\nu} \sum_{\boldsymbol{x}\ (\mathrm{mod}\ p^N)} e\left(\frac{ap^{N-\nu}F_{\boldsymbol{d}}(\boldsymbol{x})}{p^N}\right)$$

$$= \sum_{\nu=0}^{N} \sideset{}{^*}\sum_{a=1}^{p^\nu} (p^{N-\nu})^n \sum_{\boldsymbol{x}\ (\mathrm{mod}\ p^\nu)} e\left(\frac{aF_{\boldsymbol{d}}(\boldsymbol{x})}{p^\nu}\right).$$

Using (5.11), (5.12), our expression for $M'(p^N)$ becomes

$$M'(p^N) = \sum_{\boldsymbol{d}\,|\,p} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} p^{N(n-1)} \sum_{\nu=0}^{N} p^{-n\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0})$$

$$= p^{N(n-1)} \left\{ \sum_{\boldsymbol{d}\,|\,p} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} + \sum_{\boldsymbol{d}\,|\,p} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} \sum_{\nu=1}^{N} p^{-n\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0}) \right\}$$

$$= p^{N(n-1)} \left\{ \left(1 - \frac{1}{p^2}\right)^n + \sum_{\nu=1}^{N} p^{-n\nu} B_{p^\nu}(2) \right\}.$$

This proves (5.9), and the lemma follows.

We now revert to the special case $F = f - m$ of §§1–4.

Lemma 19 *Let* $\sigma \geq \frac{7}{4} + \epsilon$. *Then for* $n \geq 4$,

$$(5.13)\qquad \sum_{\nu \geq 2} p^{-n\nu} \sum_{\boldsymbol{d}\,|\,p} \pi_{\boldsymbol{d}}^{-\sigma} |S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0})| \ll p^{-1-\epsilon},$$

$$(5.14)\qquad p^{-n} \sum_{\substack{\boldsymbol{d}\,|\,p \\ \boldsymbol{d} \neq (1,\ldots,1)}} \pi_{\boldsymbol{d}}^{-\sigma} |S_p(\boldsymbol{d}, \boldsymbol{0})| \ll p^{-7/4}.$$

For $n \geq 5$, *or* $n = 4$, $p \nmid m$,

$$(5.15)\qquad 1 + (1 - p^{-s})^{-n} \sum_{\nu \geq 1} p^{-n\nu} B_{p^\nu}(s) = 1 + O(p^{-1-\epsilon}).$$

For $n=4$, $p \,|\, m$,

$$1 + (1-p^{-s})^{-4} \sum_{\nu \geq 1} p^{-4\nu} B_{p^\nu}(s) = 1 + O(p^{-1}) \tag{5.16}$$

and

$$\left(1 - \frac{\chi(p)}{p}\right)\left(1 + (1-p^{-s})^{-4} \sum_{\nu \geq 1} p^{-4\nu} B_{p^\nu}(s)\right) = 1 + O(p^{-1-\epsilon}). \tag{5.17}$$

Proof. For $\boldsymbol{d} \,|\, p$, Lemma 9 in conjunction with a trivial bound yields

$$p^{-n\nu} |S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0})| \ll \min(p^\nu, p^{2n - \nu\left(\frac{n}{2}-1\right)}).$$

Thus for $p \,|\, 2D$,

$$\sum_{\nu \geq 1} p^{-n\nu} \sum_{\boldsymbol{d} \,|\, p} \pi_{\boldsymbol{d}}^{-\sigma} |S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0})| \ll 1. \tag{5.18}$$

This implies (5.13)–(5.17).

Now suppose that $p \nmid 2D$. Then for $\nu \geq 2$,

$$\pi_{\boldsymbol{d}}^{-\sigma} p^{-n\nu} S_{p^\nu}(\boldsymbol{d}, \boldsymbol{0}) \ll \pi_{\boldsymbol{d}}^{-\sigma+2} p^{-\nu\left(\frac{n}{2}-1\right)} \tag{5.19}$$

(Lemma 9)

$$\ll \pi_{\boldsymbol{d}}^{1/4-\epsilon} p^{-\nu\left(\frac{n}{2}-1\right)}$$

$$\ll p^{n/4 - \nu\left(\frac{n}{2}-1\right) - \epsilon} \ll p^{-\nu/2-\epsilon},$$

and (5.13) follows.

We now consider $\nu = 1$. If $\boldsymbol{d} \,|\, p$ and $\pi_{\boldsymbol{d}} \geq p^2$, then trivially

$$\pi_{\boldsymbol{d}}^{-\sigma} p^{-n} S_p(\boldsymbol{d}, \boldsymbol{0}) \ll \pi_{\boldsymbol{d}}^{-7/4} p \ll p^{-5/2}.$$

If $\pi_{\boldsymbol{d}} = p$, then

$$\pi_{\boldsymbol{d}}^{-\sigma} p^{-n} S_p(\boldsymbol{d}, \boldsymbol{0}) \ll \pi_{\boldsymbol{d}}^{-\sigma} p^{-\frac{n}{2}+2} \ll p^{-7/4}$$

by Lemma 9. This proves (5.14).

Turning to (5.15)–(5.17), we need only consider the contribution to $p^{-n}B_p(s)$ from $p^{-n}S_p(\mathbf{0})$. For $n \geq 5$,

$$p^{-n}S_p(\mathbf{0}) \ll p^{1-n/2} \ll p^{-3/2} \tag{5.20}$$

from Lemma 9. For $n = 4$, $p \nmid m$, Lemma 8 gives

$$p^{-4}S_p(\mathbf{0}) \ll p^{-3/2}. \tag{5.21}$$

Combining (5.13), (5.14), (5.20), (5.21), we obtain (5.15). For $n = 4$, $p \,|\, m$, we use (3.8), obtaining

$$1 + (1-p^{-s})^{-4} \sum_{\nu=1}^{\infty} p^{-n\nu} B_{p^\nu}(s) = 1 + \frac{\chi(p)}{p} + O(p^{-1-\epsilon}),$$

which yields (5.16), (5.17) at once.

Lemma 20 *Let $\sigma \geq \frac{11}{6} + \epsilon$. Under the hypotheses of Theorem 4, we have*

$$\sum_{\nu \geq 2} p^{-3\nu} \sum_{\boldsymbol{d} \,|\, p} \pi_{\boldsymbol{d}}^{-\sigma} |S_{p^\nu}(\boldsymbol{d}, \mathbf{0})| \ll p^{-1-\epsilon}, \tag{5.22}$$

$$p^{-3} \sum_{\substack{\boldsymbol{d} \,|\, p \\ \boldsymbol{d} \neq (1,1,1)}} \pi_{\boldsymbol{d}}^{-\sigma} |S_p(\boldsymbol{d}, \mathbf{0})| \ll p^{-5/3}. \tag{5.23}$$

Moreover,

$$1 + (1-p^{-s})^{-3} \sum_{\nu \geq 1} p^{-3\nu} B_{p^\nu}(s) = 1 + O(p^{-1}) \tag{5.24}$$

and

$$\left(1 - \frac{\chi^*(p)}{p}\right)\left(1 + (1-p^{-s})^{-3} \sum_{\nu \geq 1} p^{-3\nu} B_{p^\nu}(s)\right) = 1 + O(p^{-1-\epsilon}). \tag{5.25}$$

Proof. As in the preceding proof, we may suppose that $p \nmid 2D$. For $\nu \geq 3$, the first estimate in (5.19) yields

$$\begin{aligned} \pi_{\boldsymbol{d}}^{-\sigma} p^{-3\nu} S_{p^\nu}(\boldsymbol{d}, \mathbf{0}) &\ll \pi_{\boldsymbol{d}}^{1/6-\epsilon} p^{-\nu/2} \\ &\ll p^{1/2-\epsilon-\nu/2}, \end{aligned}$$

so that

$$\sum_{\nu\ge 3} p^{-3\nu} \sum_{\boldsymbol{d}\,|\,p} \pi_{\boldsymbol{d}}^{-\sigma} |S_{p^\nu}(\boldsymbol{d},\boldsymbol{0})| \ll p^{-1-\epsilon}.$$

For $\nu = 1, 2$ and $\pi_{\boldsymbol{d}} \ge p^2$, a trivial bound yields

$$\pi_{\boldsymbol{d}}^{-\sigma} p^{-3\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{0}) \ll p^{-11/3+\nu} \ll p^{-5/3}.$$

Next we show that

$$\pi_{\boldsymbol{d}}^{-\sigma} p^{-3\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{0}) \ll p^{-11/6} \tag{5.26}$$

when $\nu = 1$ or 2 and $\pi_{\boldsymbol{d}} = p$. Let D_j be the minor obtained by deleting row j and column j from $\det[a_{ij}]$. We have $D_1 D_2 D_3 \ne 0$, since f is positive-definite. In proving (5.26), we may suppose that

$$p \nmid D_1 D_2 D_3.$$

Now suppose, for example, $\boldsymbol{d} = (p, 1, 1)$. Since

$$f^*(x_2, x_3) := f(0, x_2, x_3)$$

is nonsingular $\pmod p$,

$$S_{p^\nu}(\boldsymbol{d},\boldsymbol{0}) = p^\nu S_{p^\nu, f^*}(\boldsymbol{0}) \ll p^\nu p^{\nu(2/2+1)}$$

(Lemma 9) and

$$\pi_{\boldsymbol{d}}^{-\sigma} p^{-3\nu} S_{p^\nu}(\boldsymbol{d},\boldsymbol{0}) \ll p^{-\sigma} \ll p^{-11/6}.$$

Recalling (4.22), (4.23), we can deal with the case $\nu = 2$, $\pi_{\boldsymbol{d}} = 1$. This completes the proof of (5.22), (5.23). As in the preceding proof, but using (3.9) in place of (3.8), (5.24) and (5.25) follow.

Lemma 21 *For $n \ge 5$ or $n = 4$, $m \ne 0$, the condition* (5.5) *holds for $\sigma > \frac{7}{4}$. The product*

$$\rho(F) = \prod_p \rho_p$$

converges, and for $X > 1$ we have

$$\sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}} \le X}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^2} \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t},\boldsymbol{0})}{q^n} = \rho(F) + O\left((1+m)^\epsilon X^{-\frac{1}{4}+\epsilon}\right). \tag{5.27}$$

Proof. By (5.15), (5.16),

(5.28)
$$\sum_{q=1}^{\infty} \frac{1}{q^n} \sum_{\boldsymbol{d}\,|\,q} \frac{|S_q(\boldsymbol{d},\boldsymbol{0})|}{\pi_{\boldsymbol{d}}^{\sigma}} = \prod_p \left(1 + \sum_{\nu\geq 1} p^{-n\nu} \sum_{\boldsymbol{d}\,|\,p} \frac{1}{\pi_{\boldsymbol{d}}^{\sigma}} |S_{p^\nu}(\boldsymbol{d},\boldsymbol{0})|\right)$$
$$\ll \begin{cases} 1 & \text{if } n \geq 5 \\ \prod_{p\,|\,m} (1+O(p^{-1})) \ll m^{\epsilon} & \text{if } n=4,\ m\neq 0. \end{cases}$$

This shows that (5.5) holds. From Lemma 18, the series $\mathfrak{S}(s)$ converges absolutely for $\sigma > 7/4$, and (giving a wasteful estimate for $n \geq 5$)

$$\mathfrak{S}(s) \ll (1+m)^{\epsilon} \qquad \left(\sigma \geq \frac{7}{4} + \epsilon\right). \tag{5.29}$$

To obtain (5.27), we apply Lemma 13, with

$$a_\ell = \sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}}=\ell}} \mu(\boldsymbol{t}) \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t},\boldsymbol{0})}{q^n}. \tag{5.30}$$

It follows from Lemma 10 that

$$a_\ell \ll (m+1)^{\epsilon} \sum_{\pi_{\boldsymbol{t}}=\ell} \pi_{\boldsymbol{t}}^2 \ll (m+1)^{\epsilon} \ell^{2+\epsilon}. \tag{5.31}$$

In Lemma 13, take $\lambda = 2$, $b = 2+\epsilon$, $K \ll (m+1)^{\epsilon}$, $c = 2$, $x = [X] + 1/2$, $T = X^3$. We conclude that

$$\sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}}\leq X}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^2} \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t},\boldsymbol{0})}{q^n} = \sum_{\ell \leq X} \frac{a_\ell}{\ell^2}$$
$$= \frac{1}{2\pi i} \int_{2-iT}^{2+iT} \mathfrak{S}(2+s) \frac{x^s}{s}\, ds + O((m+1)^{\epsilon} X^{-1}).$$

We move the line of integration back to

$$\operatorname{Re} s = -\frac{1}{4} + \epsilon.$$

The contribution from the pole at 0 is

$$\mathfrak{S}(2) = \rho(F),$$

from (5.8). Taking (5.29) into account, the contribution from the horizontal segments is $O((1+m)^{\epsilon}X^{-1})$. The vertical segment $\left[-\frac{1}{4}+\epsilon-iT, -\frac{1}{4}+\epsilon+iT\right]$ contributes

$$O((1+m)^{\epsilon}X^{-1/4+2\epsilon})$$

from (5.29) and the estimate

$$\int_{-T}^{T} \frac{1}{1+|t|}\, dt \ll \log T \ll \log x.$$

This establishes (5.27) and completes the proof.

In order to treat the remaining cases together, we write $\chi_3 = \chi^*$, $\chi_4 = \chi$, $\theta_3 = 11/6$, $\theta_4 = 7/4$, $\zeta_3(s,d) = \zeta(s,\boldsymbol{d})$, $\zeta_4(s,\boldsymbol{d}) = \zeta(s,\boldsymbol{d},\boldsymbol{0})$.

Lemma 22 *Under the hypotheses of either Theorem 3 or 4, the series*

$$\sum_{\boldsymbol{t}} \frac{1}{\pi_{\boldsymbol{t}}^{\sigma}} \left| \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t},\boldsymbol{0})}{q^n} \right|$$

converges for $\sigma > 3$. *Moreover, the function*

$$g(n,s) = \sum_{\boldsymbol{t}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^{\sigma}} \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t},\boldsymbol{0})}{q^n} \quad (\sigma > 3)$$

has an analytic continuation to $\sigma > \theta_n$ *given by*

(5.32)

$$g(n,s) = \zeta(s)^{-n} L(1,\chi_n) \prod_p \left(1 - \frac{\chi_n(p)}{p}\right) \left(1 + (1-p^{-s})^{-n} \sum_{\nu \geq 1} p^{-n\nu} B_{p^{\nu}}(s)\right).$$

We have

(5.33) $$g(n,s) \ll 1 \quad (\sigma \geq \theta_n + \epsilon).$$

Proof. For $\ell \geq 1$, let

$$a_\ell = \sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}} = \ell}} \mu(\boldsymbol{t}) \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t}, \boldsymbol{0})}{q^n}.$$

It follows from Lemmas 14, 15 that

$$a_\ell \ll \sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}} = \ell}} \left| \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t}, \boldsymbol{0})}{q^n} \right| \ll \ell^{2+\epsilon}. \tag{5.34}$$

Hence $g(n, s)$ may be written

$$g(n, s) = \sum_{\ell=1}^{\infty} \frac{a_\ell}{\ell^s},$$

and this series converges absolutely for $\sigma > 3$.

Let

$$g^*(n, s) = \zeta(s)^{-n} L(1, \chi_n) \prod_p \left(1 - \frac{\chi_n(p)}{p}\right) \left(1 + (1 - p^{-s})^{-n} \sum_{\nu \geq 1} p^{-n\nu} B_{p^\nu}(s)\right).$$

It is clear from (5.17), (5.25) that $g^*(n, s)$ is holomorphic in the region $\sigma > \theta_n$, and

$$g^*(n, s) \ll 1 \qquad (\sigma \geq \theta_n + \epsilon).$$

It remains to show that $g(n, s) = g^*(n, s)$ for any given s with $\sigma > 3 + \epsilon$. We shall obtain this equation in the form

$$g(n, s) = \lim_{N \to \infty} g_N(n, s). \tag{5.35}$$

Here

$$g_N(n, s) = \zeta(s)^{-n} k_N(n) \prod_{p \leq N} \left(1 - \frac{\chi_n(p)}{p}\right) \left(1 + (1 - p^{-s})^{-n} \sum_{\nu=1}^{\infty} p^{-n\nu} B_{p^\nu}(s)\right),$$

with

$$k_N(n) = \prod_{p \leq N} \left(1 - \frac{\chi_n(p)}{p}\right)^{-1}.$$

As a first step, we show that

$$g_N(n,s) = \sum_{\boldsymbol{t}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} \sum_{q \in V_N} q^{-n} S_q(\boldsymbol{t}, \boldsymbol{0}), \tag{5.36}$$

where

$$V_N = \{q \geq 1 \ : \ p \,|\, q \Rightarrow p \leq N\}.$$

We have

$$\sum_{q \in V_N} q^{-n} \, |S_q(\boldsymbol{t}, \boldsymbol{0})| = \prod_{p \leq N} \left(1 + \sum_{\nu \geq 1} p^{-n\nu} |S_{p^\nu}(\boldsymbol{t}, \boldsymbol{0})|\right) \tag{5.37}$$
$$\ll_{f,N} \pi_{\boldsymbol{t}}^2.$$

The last estimate is a consequence of Lemma 9. Since $\sigma > 3$, the right-hand side of (5.36) may be rewritten as

$$\sum_{q \in V_N} q^{-n} \sum_{\boldsymbol{t}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} S_q(\boldsymbol{t}, \boldsymbol{0})$$
$$= \zeta(s)^{-n} \sum_{q \in V_N} q^{-n} B_q(s) \prod_{p \,|\, q} (1 - p^{-s})^{-n}$$

(by Lemma 16)

$$= \zeta(s)^{-n} \prod_{p \leq N} \left(1 + (1 - p^{-s})^{-n} \sum_{\nu \geq 1} p^{-n\nu} B_{p^\nu}(s)\right)$$

(by Lemma 17 and (5.13), (5.22))

$$= g_N(n,s).$$

Let $d\tau$ be the counting measure on

$$\Omega = \{\boldsymbol{t} \in \mathbb{Z}^n : t_i > 0 \ (i = 1, \ldots, n), \ \mu(\boldsymbol{t}) \neq 0\}.$$

We may now rewrite the desired conclusion (5.35) in the form

$$\int_\Omega \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} \sum_{q \geq 1} q^{-n} S_q(\boldsymbol{t}, \boldsymbol{0}) d\tau(\boldsymbol{t}) \tag{5.38}$$
$$= \lim_{N \to \infty} \int_\Omega \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} \sum_{q \in V_N} q^{-n} S_q(\boldsymbol{t}, \boldsymbol{0}) d\tau(\boldsymbol{t}).$$

We use the Lebesgue dominated convergence to prove (5.38). To establish pointwise convergence of the integrand to the desired limit, we begin with the identity

(5.39)

$$\frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} \sum_{q \in V_N} q^{-n} S_q(\boldsymbol{t}, \mathbf{0}) = \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^s} k_N(n) \prod_{p \le N} \left(1 - \frac{\chi_n(p)}{p}\right)\left(1 + \sum_{\nu \ge 1} p^{-n\nu} S_{p^\nu}(\boldsymbol{t}, \mathbf{0})\right).$$

Now $k_N(n) \to L(1, \chi_n)$ as $N \to \infty$, while

$$\lim_{N \to \infty} \prod_{p \le N} \left(1 - \frac{\chi_n(p)}{p}\right) \left(1 + \sum_{\nu \ge 1} p^{-n\nu} S_{p^\nu}(\boldsymbol{t}, \mathbf{0})\right)$$

$$= \prod_{p} \left(1 - \frac{\chi_n(p)}{p}\right) \left(1 + \sum_{\nu \ge 1} p^{-n\nu} S_{p^\nu}(\boldsymbol{t}, \mathbf{0})\right)$$

$$= L(1, \chi_n)^{-1} \zeta_n(n, \boldsymbol{t})$$

(Lemmas 11, 12)

$$= L(1, \chi_n)^{-1} \sum_{q=1}^{\infty} q^{-n} S_q(\boldsymbol{t}, \mathbf{0})$$

(Lemmas 14, 15). Pointwise convergence follows at once.

Moreover, the right-hand side of (5.39) is

$$\ll \pi_{\boldsymbol{t}}^{-\sigma+2+\epsilon}$$

uniformly in $\boldsymbol{t}$. Here the factor $k_N(n)$ is bounded independently of $\boldsymbol{t}$, so the assertion follows from (4.19) and (4.20) ($n = 4$), and from (4.24) and (4.25) ($n = 3$). Since

$$\int_{\Omega} \pi_{\boldsymbol{t}}^{-\sigma+2+\epsilon} d\tau(\boldsymbol{t}) < \infty.$$

this establishes dominated convergence and proves the lemma.

Lemma 23 *Under the hypotheses of Lemma 22, we have*

$$\sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}} \le X}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^2} \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t}, \mathbf{0})}{q^n} = L(1, \chi_n)\rho^*(F) + O(X^{\theta_n - 2 + \epsilon})$$

for $X > 1$.

Proof. We apply Lemma 13 with

$$a_\ell = \sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}} = \ell}} \mu(\boldsymbol{t}) \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t}, \boldsymbol{0})}{q^n}.$$

Recalling (5.34), we may take

$$\lambda = 2,\ b = 2 + \epsilon,\ c = 2,\ x = [X] + 1/2,\ T = X^3.$$

With $g(n, s)$ as in Lemma 22, this produces

$$\sum_{\substack{\boldsymbol{t} \\ \pi_{\boldsymbol{t}} \le X}} \frac{\mu(\boldsymbol{t})}{\pi_{\boldsymbol{t}}^2} \sum_{q=1}^{\infty} \frac{S_q(\boldsymbol{t}, \boldsymbol{0})}{q^n} = \int_{2-iT}^{2+iT} g(n, s+2) \frac{x^s}{s} \, ds + O(X^{-1}).$$

We now move the line of integration back to $\sigma = \theta_n - 2 + \epsilon$. By (5.33), the horizontal integrals and the integral over $[\theta_n - 2 + \epsilon - iT,\ \theta_n - 2 + \epsilon + iT]$ are $O(X^{-1})$ and $O(X^{\theta_n - 2 + \epsilon})$ respectively. We use (5.32) to write the contribution from the pole at 0 as

$$g(n, 2) = \zeta(2)^{-n} L(1, \chi_n) \prod_p \left(1 - \frac{\chi_n(p)}{p}\right)\left(1 + (1 - p^{-s})^{-n} \sum_{\nu \ge 1} p^{-n\nu} B_{p^\nu}(2)\right).$$

Since the condition (5.10) is satisfied, we may rewrite this as

$$g(n, 2) = \zeta(2)^{-n} L(1, \chi_n) \prod_p \left(1 - \frac{\chi_n(p)}{p}\right) (1 - p^{-2})^{-n} \rho_p,$$

as pointed out after (5.9). Combining the factors $\zeta(2)^{-n}$, $\prod_p (1 - p^{-2})^{-n}$, we complete the proof.

So far, we have not touched on positivity of the ρ_p. We require a version of Hensel's lemma.

Lemma 24 *Let p be a prime and ℓ, α positive integers. Let $F \in \mathbb{Z}[X_1, \dots, X_n]$. Suppose that there is an integer vector $\boldsymbol{y}$ having*

$$p^{\ell - 1} \parallel \boldsymbol{\nabla} F(\boldsymbol{y})$$

and

$$F(\boldsymbol{y}) \equiv 0 \pmod{p^\alpha}.$$

Suppose either that $\ell = 1$*,* $\alpha \geq 1$ *or that* $\ell \geq 2$*,* $\alpha = 2\ell - 1$*. Then for* $\nu \geq 0$*, there are at least* $p^{(n-1)\nu}$ *solutions* $\boldsymbol{x}$ $\pmod{p^{\alpha+\nu}}$ *of*

$$F(\boldsymbol{x}) \equiv 0 \pmod{p^{\alpha+\nu}}$$

for which $\boldsymbol{x} \equiv \boldsymbol{y} \pmod{p^\alpha}$*.*

Proof. The case $\ell \geq 2$ follows immediately from the proof of [4], Lemma 42, although Davenport is concerned with a cubic form F. The case $\ell = 1$ is similar but simpler.

Lemma 25 *Let* $f(\boldsymbol{X})$ *be a nonsingular quadratic form in* $F_p[X_1, \ldots, X_n]$*, where* $F_p = \mathbb{Z}/p\mathbb{Z}$*,* $n \geq 3$*,* $p \geq 3$*. Let* $m \in F_p$*. There is a solution* $\boldsymbol{x}$ *in* F_p^n *of*

$$f(\boldsymbol{x}) = m \tag{5.40}$$

such that either

(i) for some i*, we have* $x_i \frac{\partial f}{\partial x_i} \neq 0$*; or*

(ii) $\boldsymbol{\nabla} f(\boldsymbol{x})$ *has at least two nonzero components.*

Proof. It is shown in [1], §2 that for $n \geq 4$, alternative (ii) always holds. The argument employed there works (with obvious modifications) for $n = 3$, $p \geq 5$. Thus we may assume that $n = p = 3$. Let us suppose that no $\boldsymbol{x}$ with (5.40) satisfies (i) or (ii).

The number of solutions of (5.40) is

$$9 + \left(-\frac{Dm}{3}\right) 3$$

from Lemma 8. Let

$$V_i = \left\{ \boldsymbol{x} \in F_p^3 : \frac{\partial f}{\partial x_j} = 0 \quad \text{for } j \neq i \right\}.$$

Since (ii) fails, each solution of (5.40) is in some V_i. Obviously V_i is a one-dimensional subspace and

$$V_1 \cup V_2 \cup V_3 = \{\boldsymbol{0}\} \cup (V_1 - \{\boldsymbol{0}\}) \cup (V_2 - \{\boldsymbol{0}\}) \cup (V_3 - \{\boldsymbol{0}\})$$

has ≤ 7 points. Thus $m \neq 0$.

Clearly V_3 must contain a solution $\boldsymbol{x}$ of (5.40). (If not, the number of solutions is ≤ 5.) For this $\boldsymbol{x}$, $\frac{\partial f}{\partial x_3} \neq 0$. Hence $x_3 = 0$,

$$\frac{\partial f}{\partial x_1} = \frac{\partial f}{\partial x_2} = 0.$$

That is,

$$a_{11}x_1 + a_{12}x_2 = a_{21}x_1 + a_{22}x_2 = 0. \tag{5.41}$$

Since $(x_1, x_2) \neq \mathbf{0}$,

$$a_{11}a_{22} = a_{12}a_{21} = a_{12}^2.$$

In particular, $\{a_{11}, a_{22}\}$ cannot be $\{1, 2\}$. Replacing f, m by $2f, 2m$ if necessary, we conclude that

$$a_{11}, a_{22} \text{ are 0 or 1.}$$

Suppose $a_{11} = a_{22} = 1$. From (5.41) and $\boldsymbol{x} \neq \mathbf{0}$, we infer that $a_{12} \neq 0$, $x_1 \neq 0$, $x_2 \neq 0$. Now

$$f(\boldsymbol{x}) = x_1^2 + x_2^2 + 2a_{12}x_1x_2 = 1 + 1 - 2x_1^2 = 0.$$

This is absurd. Hence $a_{11}a_{22} = a_{12}^2 = 0$. Similarly $a_{11}a_{33} = a_{13}^2 = a_{22}a_{33} = a_{23}^2 = 0$. This contradicts $\det[a_{ij}] \neq 0$, and the lemma is proved.

Proof of Theorem 5. We first show that

$$\rho_p > 0 \quad \text{for all } p. \tag{5.42}$$

For $p \nmid 2D$, we adapt the argument of [1]. By Lemma 25, there is an integer vector $\boldsymbol{y}$,

$$F(\boldsymbol{y}) \equiv 0 \pmod{p}$$

such that either $y_i \frac{\partial F}{\partial y_i} \not\equiv 0 \pmod{p}$ for some i, or two components of $\boldsymbol{\nabla} F(\boldsymbol{y})$ are nonzero $\pmod{p}$. In the former case, we employ Lemma 24 with $n = 1$, $\ell = 1$, $\alpha = 1$. Say $y_1 \frac{\partial F}{\partial y_1} \neq 0$. We select integers $x_2, \ldots, x_n$, $x_j \equiv y_j \pmod{p}$, $x_j \not\equiv 0 \pmod{p^2}$. There is an integer x_1 with $x_1 \equiv y_1 \pmod{p}$, $F(\boldsymbol{x}) \equiv 0 \pmod{p^2}$. We have

$$F(\boldsymbol{x}) \equiv 0 \pmod{p^2}, \quad p^2 \nmid x_1, \ldots, p^2 \nmid x_n. \tag{5.43}$$

In the latter case, suppose for example that

$$\boldsymbol{\nabla} F(\boldsymbol{y}) = (e_1, \dots, e_n), \quad p \nmid e_1 e_2.$$

We take $\boldsymbol{x}$ of the form $\boldsymbol{x} = \boldsymbol{y} + p\boldsymbol{z}$, so that

$$\begin{aligned} F(\boldsymbol{x}) &\equiv F(\boldsymbol{y}) + p\boldsymbol{e} \cdot \boldsymbol{z} \pmod{p^2} \\ &\equiv bp + p\boldsymbol{e} \cdot \boldsymbol{z} \pmod{p^2}, \end{aligned}$$

where $F(\boldsymbol{y}) = bp$. The conditions (5.43) reduce in this case to

$$\boldsymbol{e} \cdot \boldsymbol{z} \equiv -b \pmod{p} \tag{5.44}$$

together with n conditions

$$y_j + pz_j \not\equiv 0 \pmod{p^2}. \tag{5.45 (j)}$$

We choose z_j to satisfy (5.45)(j) for $j \geq 3$. Now (5.44) reduces to (say)

$$e_1 z_1 + e_2 z_2 \equiv c \pmod{p}. \tag{5.46}$$

There are $\geq p-1$ choices of z_2 with (5.45)(2). Each defines a value of z_1 with (5.46), and at least one of these z_1's must satisfy (5.45)(1). Again, we can satisfy (5.43).

Another application of Lemma 24, with $\ell = 1$, $\alpha = 2$, shows that there are $\geq p^{(n-1)\nu}$ solutions $\boldsymbol{w} \pmod{p^{\nu+2}}$ of

$$F(\boldsymbol{w}) \equiv 0 \pmod{p^{\nu+2}}, \quad \boldsymbol{w} \equiv \boldsymbol{x} \pmod{p^2}.$$

Thus

$$\rho_p \geq \lim_{\nu \to \infty} \frac{p^{(n-1)\nu}}{p^{(n-1)(\nu+2)}} = p^{-2n-2}.$$

Now suppose that $p^\theta \,\|\, 2D$ with $\theta \geq 1$. Since $5\theta \geq 3 + 2\theta$, condition B provides a solution of

$$F(\boldsymbol{y}) \equiv 0 \pmod{p^{3+2\theta}}, \quad p^2 \nmid y_i \quad (i = 1, \dots, n).$$

Define ℓ by

$$p^{\ell-1} \,\|\, \boldsymbol{\nabla} F(\boldsymbol{y}). \tag{5.47}$$

We claim that

$$2\ell - 1 \le 3 + 2\theta. \tag{5.48}$$

Once we have (5.48), we may apply Lemma 24 to obtain $M'(p^{2\ell-1+\nu}) \ge p^{(n-1)\nu}$, and (as above) $\rho_p > 0$.

From (5.47), as in the proof of Lemma 9,

$$2D\boldsymbol{y} \equiv (\operatorname{adj} M)2M\boldsymbol{y} \equiv \boldsymbol{0} \pmod{p^{\ell-1}}.$$

Since $p^2 \nmid y_1$, we have

$$2D \equiv 0 \pmod{p^{\ell-2}},$$

and $\ell - 2 \le \theta$, which yields (5.48). Now (5.42) follows.

Suppose that $n \ge 5$. From (5.15) and its proof,

$$\rho_p = 1 + O(p^{-1-\epsilon}),\ \sigma_p = 1 + O(p^{-1-\epsilon}).$$

Combining these estimates for sufficiently large p with (5.42) yields (1.7).

For $n = 4$, $m \ne 0$, the argument of the previous paragraph gives

$$1 \ll \prod_{p \nmid m} \rho_p \le \prod_{p \nmid m} \sigma_p \ll 1,$$

while

$$m^{-\epsilon} \ll \prod_{p \,|\, m} \rho_p \le \prod_{p \,|\, m} \sigma_p \ll m^{\epsilon},$$

by combining (5.42) with (5.16) and the corresponding (simpler) estimate for σ_p. These bounds combine to give (1.8). Finally, we obtain (1.9) and (1.10) by using (5.42) and the corresponding estimate for σ_p in conjunction with (5.17) and (5.25).

§6 Completion of the proofs of Theorems 1–3

The theorems will follow from (3.2) and (4.6) if we show that

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \mu(\boldsymbol{d}) \sum_{\boldsymbol{c} \in \mathbb{Z}^n} \sum_{q=1}^{\infty} q^{-n} S_q(\boldsymbol{d}, \boldsymbol{c}) I_q(\boldsymbol{d}, \boldsymbol{c}) \tag{6.1}$$

$$= \sigma_\infty(G, w)\lambda P^n + O(P^{n-\gamma}),$$

where $\lambda = \rho(F)$ ($n \geq 5$ or $n = 4$, $m \neq 0$), $\lambda = L(1, \chi)\rho^*(F)$ ($n = 4, m = 0$).

We recall that $h(x, y) = 0$ for $x > \max(1, 2|y|)$. It follows readily that

$$I_q(\boldsymbol{d}, \boldsymbol{c}) = 0 \textit{ unless } \ q \ll P,$$

and we may restrict summation over q in (6.1) to $q \ll P$.

It is convenient to write $\delta = 1$ if n is even and $m = 0$, and $\delta = 0$ otherwise. We record the useful bound

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \leq P^{2n\gamma}}} \pi_{\boldsymbol{d}}^k \sum_{R < q \leq 2R} q^{-n} |S_q(\boldsymbol{d}, \boldsymbol{c})| \ll (1 + |\boldsymbol{c}|)^{\epsilon} P^{2n(k+4)\gamma} R^{(3+\delta-n)/2+\epsilon}, \tag{6.2}$$

where k is a non-negative constant and $R > 1$. The bound (6.2) is an immediate consequence of Lemma 10.

Let $\eta = 12n^2\gamma$. Consider first the contribution to the sum in (6.1) from

$$|\boldsymbol{c}| > P^{\eta}.$$

Fix an integer $K > 2$ with $\left(\frac{K}{2} - 2\right)\eta > n + 1$. Now (4.10) gives

$$I_q(\boldsymbol{d}, \boldsymbol{c}) \ll \pi_{\boldsymbol{d}}^{2Kn} P^{n+1} q^{-1} |\boldsymbol{c}|^{-Kn}.$$

Combining this with (6.2),

$$\begin{aligned} &\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \leq P^{2n\gamma}}} \sum_{q \ll P} \sum_{|\boldsymbol{c}| > P^{\eta}} q^{-n} |S_q(\boldsymbol{d}, \boldsymbol{c}) I_q(\boldsymbol{d}, \boldsymbol{c})| \\ &\qquad \ll P^{2n(2Kn+4)\gamma+n+1+\epsilon} \sum_{|\boldsymbol{c}| > P^{\eta}} |c_1|^{-K+\epsilon} \cdots |c_n|^{-K+\epsilon} \\ &\qquad \ll P^{6n^2K\gamma+n+1-(K-1-\epsilon)\eta} \\ &\qquad \ll P^{-\left(\frac{K}{2}-2\right)\eta+n+1} \ll 1. \end{aligned} \tag{6.3}$$

Now consider $\boldsymbol{c}$ with $0 < |\boldsymbol{c}| \leq P^{\eta}$. Here (4.11) gives, for $q \ll P$,

$$I_q(\boldsymbol{d}, \boldsymbol{c}) \ll \pi_{\boldsymbol{d}}^n P^{\frac{n}{2}+1+\epsilon} q^{\frac{n}{2}-1}.$$

In conjunction with (6.2), this yields

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \sum_{q \ll P} \sum_{0<|\boldsymbol{c}|\le P^{\eta}} q^{-n}|S_q(\boldsymbol{d},\boldsymbol{c})I_q(\boldsymbol{d},\boldsymbol{c})| \ll P^{15n^3\gamma+(n+3+\delta)/2} \ll P^{n-\gamma}, \tag{6.4}$$

except in the case $n=4$, $m=0$, to which we return below.

For $\boldsymbol{c}=\boldsymbol{0}$, we first treat those q with

$$P^{1-\epsilon} < q \ll P.$$

Here (4.9) gives

$$I_q(\boldsymbol{d},\boldsymbol{0}) \ll P^n.$$

Again using (6.2),

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \sum_{P^{1-\epsilon}<q\ll P} q^{-n}|S_q(\boldsymbol{d},\boldsymbol{0})I_q(\boldsymbol{d},\boldsymbol{0})| \ll P^{9n\gamma+(n+3+\delta)/2} \ll P^{n-\gamma}, \tag{6.5}$$

except when $n=4$, $m=0$.

The terms with $\boldsymbol{c}=\boldsymbol{0}$, $q \le P^{1-\epsilon}$ provide the main term, with an acceptable error. We first use (4.8), with a suitable $N=N(\epsilon)$, in conjunction with (6.2) to obtain

$$\begin{aligned} \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \mu(\boldsymbol{d}) \sum_{q\le P^{1-\epsilon}} q^{-n}S_q(\boldsymbol{d},\boldsymbol{0})I_q(\boldsymbol{d},\boldsymbol{0}) &= P^n\sigma_\infty(G,w) \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} \sum_{q\le P^{1-\epsilon}} q^{-n}S_q(\boldsymbol{d},\boldsymbol{0}) + O(1) \\ &= P^n\sigma_\infty(G,w) \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} \sum_{q=1}^{\infty} q^{-n}S_q(\boldsymbol{d},\boldsymbol{0}) \\ &\quad + O(P^{(n+3+\delta)/2+9n\gamma}). \end{aligned} \tag{6.6}$$

Leaving aside the case $n = 4$, $m = 0$, the last error term is $O(P^{n-\gamma})$, and Lemma 21 now gives

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \mu(\boldsymbol{d}) \sum_{q \le P^{1-\epsilon}} q^{-n} S_q(\boldsymbol{d}, \boldsymbol{0}) I_q(\boldsymbol{d}, \boldsymbol{0}) \tag{6.7}$$

$$= P^n \sigma_\infty(G, w) \rho(F) + O(P^{n-\gamma}).$$

We may now complete the proof of (6.1) for $n \ge 5$ and $n = 4$, $m \ne 0$ by combining (6.3), (6.4), (6.5) and (6.7).

We now adapt the argument to prove (6.1) for $n = 4$, $m = 0$. Because of (6.3), we may restrict attention to $|\boldsymbol{c}| \le P^\eta$. Suppose first that $\boldsymbol{c} \ne \boldsymbol{0}$. From (4.11), (4.12) and a partial summation,

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{2n\gamma}}} \mu(\boldsymbol{d}) \sum_{R < q \le 2R} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{c}) I_q(\boldsymbol{d}, \boldsymbol{c})$$

$$\ll P^{3+\epsilon} R \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \pi_{\boldsymbol{d}}^4 \max_{R < R' \le 2R} \left| \sum_{R < q \le R'} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{c}) \right|.$$

The last expression is

$$\ll P^{3+\epsilon} R \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \pi_{\boldsymbol{d}}^{6+\epsilon} R^{-1/2+\epsilon}$$

by Lemma 14. Hence

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \mu(\boldsymbol{d}) \sum_{0 < |\boldsymbol{c}| < P^\eta} \sum_{q \ll P} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{c}) I_q(\boldsymbol{d}, \boldsymbol{c}) \tag{6.8}$$

$$\ll P^{7/2+900\gamma} \ll P^{4-\gamma}.$$

For $\boldsymbol{c} = \boldsymbol{0}$, we use partial summation again. By (4.9), in conjunction with

Lemma 14,

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \sum_{R < q \le 2R} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{0}) I_q(\boldsymbol{d}, \boldsymbol{0})$$

$$\ll P^4 \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \pi_{\boldsymbol{d}}^{-2} \max_{R < R' \le 2R} \left| \sum_{R < q \le R'} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{0}) \right|$$

$$\ll P^{4+\epsilon} \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} R^{-1/2+\epsilon}.$$

This gives

$$\sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \sum_{P^{1-\epsilon} < q \ll P} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{0}) I_q(\boldsymbol{d}, \boldsymbol{0}) \ll P^{7/2+10\gamma} \ll P^{4-\gamma}. \tag{6.9}$$

We are left with $\boldsymbol{c} = \boldsymbol{0}$, $q \le P^{1-\epsilon}$. By the first step in (6.6), these terms contribute

$$P^4 \sigma_\infty(G, w) \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} \sum_{q \le P^{1-\epsilon}} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{0}) + O(1)$$

$$= P^4 \sigma_\infty(G, w) \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} \sum_{q=1}^{\infty} q^{-4} S_q(\boldsymbol{d}, \boldsymbol{0})$$

$$+ O\left(P^4 \sigma_\infty(G, w) \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} P^{-\frac{1}{2}+\epsilon} \right)$$

(from Lemma 14)

$$= P^4 \sigma_\infty(G, w) L(1, \chi) \rho^*(F) + O(P^{4-2\gamma+\epsilon}).$$

For the last step, we apply Lemma 23. We combine this estimate with (6.3), (6.8), and (6.9) to complete the proof of (6.1).

The techniques of the present paper do not appear to be strong enough to attack the cases $n = 4$, $m = 0$, D a square and $n = 3$, $m = 0$. (In both cases, the main term in Heath-Brown's approximation to $N(F, w)$ is of order $P^{n-2} \log P$.) The difficulties will become apparent to the reader on an examination of §13 of [9].

§7 Proof of Theorem 4

We recall some notions from Siegel [14]. The *genus* of a positive-definite quadratic form $q(x_1, x_2, x_3)$ consists of those positive-definite forms that are equivalent to q under invertible variable changes over the p-adic integers, for all p. The genus $\boldsymbol{G}$ splits into finitely many $\mathbb{Z}$-equivalence classes. Here the $\mathbb{Z}$-equivalence class $\{q\}$ consists of forms obtained from q by invertible integral change of variables. A sum $\sum\limits_{\{q\}}$ will run over all classes in $\boldsymbol{G}$.

Let ω_q be the number of invertible integral changes of variable that take q onto itself and write

$$M(\boldsymbol{G}) = \sum_{\{q\}} \omega_q^{-1}.$$

The average number of representations of an integer m by forms in $\boldsymbol{G}$ is

$$r(m, \boldsymbol{G}) = M(\boldsymbol{G})^{-1} \sum_{\{q\}} \omega_q^{-1} r(q, m).$$

Siegel's fundamental theorem [14] states (in our particular case) that

$$r(m, \boldsymbol{G}) = \lambda \prod_p \sigma_p,$$

where σ_p is the density defined in §1 above (with $f = q$), and the positive number λ is prescribed as follows. To a neighborhood V of m in $\mathbb{R}$ corresponds an open set

$$V' = \{\boldsymbol{x} \in \mathbb{R}^3 : q(\boldsymbol{x}) \in V\}.$$

As V shrinks to m,

$$\lambda = \lim \frac{v_3(V')}{v_1(V)}$$

(v_k = volume in $\mathbb{R}^k$). The values of σ_p, λ do not depend on the choice of q in $\boldsymbol{G}$. Let $q = f$. Clearly, in the terminology of §1 above,

$$\lambda = \lim_{\beta \to 0} \frac{1}{2\beta} \int_{|f(\boldsymbol{x}) - m| \leq \beta} d\boldsymbol{x} = m^{1/2} \sigma_\infty(G).$$

From the first paragraph of the proof of Lemma 12,

$$\sigma_p = 1 + \frac{\chi^*(p)}{p} \quad \text{if } p \nmid 2Dm,$$

so that we may rewrite Siegel's theorem in the form

$$r(m, \boldsymbol{G}) = \sigma_\infty(G) m^{1/2} L(1, \chi^*) \prod_p \left(1 - \frac{\chi^*(p)}{p}\right) \sigma_p. \tag{7.1}$$

The following uniform asymptotic formula is Theorem 2 of Duke [6]. Without the explicit dependence on D, the result may be found already in Duke [5] as an application of bounds for sums of Kloosterman sums given by Iwaniec [10].

Lemma 26 *For m square-free, and $f \in \boldsymbol{G}$,*

$$r(f, m) = r(m, \boldsymbol{G}) + O_\epsilon(D^{11/2} m^{1/2 - 1/28} (Dm)^\epsilon). \tag{7.2}$$

Proof of Theorem 4. We adapt an argument from the beginning of §4. We decompose $r(f, m)$ in the form

$$r(f, m) = r_1(f, m) + r_2(f, m),$$

where

$$r_1(f, m) = \#\{\boldsymbol{x} \in \mathbb{Z}^3 : f(\boldsymbol{x}) = m,\ \pi_{\boldsymbol{x}} \neq 0\}.$$

Since f is positive-definite,

$$r_2(f, m) \ll_{f,\epsilon} m^\epsilon \tag{7.3}$$

from Lemma 1. Now

$$\begin{aligned} R(m) &= \sum_{\substack{\boldsymbol{y} \\ F(\boldsymbol{y})=0,\, \pi_{\boldsymbol{y}}\neq 0}} \prod_{i=1}^{3} \sum_{d_i^2 \mid y_i} \mu(d_i) \\ &= \sum_{\substack{\boldsymbol{d} \\ |\boldsymbol{d}| \ll P}} \mu(\boldsymbol{d}) \sum_{\substack{\boldsymbol{x} \\ F_{\boldsymbol{d}}(\boldsymbol{x})=0,\, \pi_{\boldsymbol{x}}\neq 0}} 1 \\ &= \sum_{\substack{\boldsymbol{d} \\ |\boldsymbol{d}| \ll P}} \mu(\boldsymbol{d}) r_1(f_{\boldsymbol{d}}, m). \end{aligned}$$

By a slight modification of the argument leading to (4.5), we deduce that

$$R(m) = \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \leq P^{8\gamma}}} \mu(\boldsymbol{d}) r_1(f_{\boldsymbol{d}}, m) + O_f(m^{\frac{1}{2}(1-\gamma)}).$$

Thus

$$R(m) = \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \leq P^{8\gamma}}} \mu(\boldsymbol{d}) r(f_{\boldsymbol{d}}, m) - \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \leq P^{8\gamma}}} \mu(\boldsymbol{d}) r_2(f_{\boldsymbol{d}}, m) + O_f(m^{\frac{1}{2}(1-\gamma)}). \tag{7.4}$$

Of course

$$r_2(f_{\boldsymbol{d}}, m) \leq r_2(f, m) \ll_{D,\epsilon} m^{\epsilon} \tag{7.5}$$

from (7.3). Since γ is sufficiently small, it follows from (7.4), (7.5) that

$$R(m) = \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \leq P^{8\gamma}}} \mu(\boldsymbol{d}) r(f_{\boldsymbol{d}}, m) + O_f(m^{\frac{1}{2}(1-\gamma)}). \tag{7.6}$$

We now apply Lemma 26 with $f_{\boldsymbol{d}}$ in place of f. In this case, the expression

$$L(1, \chi^*) \prod_p \left(1 - \frac{\chi^*(p)}{p}\right) \sigma_p$$

coincides with the quantity $\zeta(3, \boldsymbol{d})$ of Lemma 12, while clearly

$$\sigma_\infty(G_{\boldsymbol{d}}) = \frac{1}{\pi_{\boldsymbol{d}}^2}\,\sigma_\infty(G).$$

Hence Lemma 26 in conjunction with (7.1) yields

$$r(f_{\boldsymbol{d}}, m) = \frac{1}{\pi_{\boldsymbol{d}}^2}\,\sigma_\infty(G)m^{1/2}\zeta(3, \boldsymbol{d}) + O_{f,\epsilon}(\pi_{\boldsymbol{d}}^{22+\epsilon} m^{1/2-1/28+\epsilon}).$$

Using the approximation in (7.6), and the series expression for $\zeta(3, \boldsymbol{d})$ in Lemma 15,

$$R(m) = \sigma_\infty(G)m^{1/2} \sum_{\substack{\boldsymbol{d} \\ \pi_{\boldsymbol{d}} \le P^{8\gamma}}} \frac{\mu(\boldsymbol{d})}{\pi_{\boldsymbol{d}}^2} \sum_{q=1}^{\infty} q^{-3} S_q(\boldsymbol{d}, \mathbf{0}) + O(P^{200\gamma} m^{1/2-1/28}) + O(m^{\frac{1}{2}(1-\gamma)}). \tag{7.7}$$

We now use Lemma 23 to approximate the first term on the right-hand side of (7.7), and Theorem 4 follows.

References

[1] R. C. Baker, *Square-free points on ellipsoids*, Acta Arith. **50** (1988), 215–219.

[2] R. C. Baker and J. Brüdern, *Sums of cubes of square-free numbers*, Monatsh. Math. **111** (1991), 1–21.

[3] Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, 1966.

[4] H. Davenport, Analytic methods for Diophantine equations and Diophantine inequalities, 2nd edn., ed. T. D. Browning, Cambridge University Press, 2005.

[5] W. Duke, *Lattice points on ellipsoids*, Séminaire de Théorie des Nombres, 1987–1988, 7 pp., Univ. Bordeaux I, Talence 1988.

[6] W. Duke, *On ternary quadratic forms*, J. Number Theory **110** (2005), 37–43.

[7] W. Duke, J. B. Friedlander and H. Iwaniec, *Bounds for automorphic L-functions*, Invent. Math. **92** (1988), 73–90.

[8] T. Estermann, *On sums of squares of square-free numbers*, Proc. London Math. Soc. (2) **53** (1951), 125–137.

[9] 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.

[10] H. Iwaniec, *Fourier coefficients of modular forms of half-integral weight*, Invent. Math. **87** (1987), 385–401.

[11] H. D. Kloosterman, *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$, Acta Math. **49** (1926), 407–464.

[12] E. Landau, Elementary number theory, Chelsea, 1958.

[13] E. V. Podsypanin, *On the representation of the integer by positive quadratic forms with square-free variables*, Acta Arith. **27** (1975), 459–488.

[14] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*, Ann. Math. **36** (1935), 527–606.

[15] E. C. Titchmarsh, The theory of the Riemann zeta-function, 2nd edn., Oxford University Press, 1986.

Department of Mathematics
Brigham Young University
Provo, UT 84602
U.S.A.
baker@math.byu.edu