



COMPOSITIO MATHEMATICA

Rational points on singular intersections of quadrics

T. D. Browning and R. Munshi

Compositio Math. **149** (2013), 1457–1494.

[doi:10.1112/S0010437X13007185](https://doi.org/10.1112/S0010437X13007185)



FOUNDATION
COMPOSITIO
MATHEMATICA



LONDON
MATHEMATICAL
SOCIETY



Rational points on singular intersections of quadrics

T. D. Browning and R. Munshi

ABSTRACT

Given an intersection of two quadrics $X \subset \mathbb{P}^{m-1}$, with $m \geq 9$, the quantitative arithmetic of the set $X(\mathbb{Q})$ is investigated under the assumption that the singular locus of X consists of a pair of conjugate singular points defined over $\mathbb{Q}(i)$.

1. Introduction

The arithmetic of quadratic forms has long held a special place in number theory. In this paper we focus our efforts on algebraic varieties $X \subset \mathbb{P}^{m-1}$ which arise as the common zero locus of two quadratic forms $q_1, q_2 \in \mathbb{Z}[x_1, \dots, x_m]$. We will always assume that X is a geometrically integral complete intersection which is not a cone. Under suitable further hypotheses on q_1 and q_2 , we will be concerned with estimating the number of \mathbb{Q} -rational points on X of bounded height. Where successful this will be seen to yield a proof of the Hasse principle for the varieties under consideration.

The work of Colliot-Thélène *et al.* [CSS87a, CSS87b] provides a comprehensive description of the qualitative arithmetic associated to the set $X(\mathbb{Q})$ of \mathbb{Q} -rational points on X for large enough values of m . In fact it is known that the Hasse principle holds for any smooth model of X if $m \geq 9$. This can be reduced to $m \geq 5$ provided that X contains a pair of conjugate singular points and does not belong to a certain explicit class of varieties for which the Hasse principle is known to fail.

In this paper the quadratic forms q_1 and q_2 will have special structures. Let Q_1 and Q_2 be integral quadratic forms in n variables $\mathbf{x} = (x_1, \dots, x_n)$, with underlying symmetric matrices \mathbf{M}_1 and \mathbf{M}_2 , so that $Q_i(\mathbf{x}) = \mathbf{x}^T \mathbf{M}_i \mathbf{x}$ for $i = 1, 2$. Then we set

$$\begin{aligned} q_1(x_1, \dots, x_{n+2}) &= Q_1(x_1, \dots, x_n) - x_{n+1}^2 - x_{n+2}^2, \\ q_2(x_1, \dots, x_{n+2}) &= Q_2(x_1, \dots, x_n). \end{aligned}$$

We will henceforth assume that Q_2 is non-singular and that as a variety V in \mathbb{P}^{n-1} , the intersection of quadrics $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ is also non-singular. It then follows that X has a singular locus containing precisely two singular points which are conjugate over $\mathbb{Q}(i)$. The question of whether the Hasse principle holds for such varieties is therefore answered completely by [CSS87a, CSS87b] when $n \geq 3$. Furthermore, when $X(\mathbb{Q})$ is non-empty, it is well known (see [CSS87a, Proposition 2.3], for example) that X is \mathbb{Q} -unirational. In particular, $X(\mathbb{Q})$ is Zariski dense in X as soon as it is non-empty.

Let $r(M)$ be the function that counts the number of representations of an integer M as a sum of two squares and let $W : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$ be an infinitely differentiable bounded function of compact

Received 9 August 2011, accepted in final form 7 January 2013, published online 20 June 2013.

2010 Mathematics Subject Classification 11D72 (primary), 11E12, 11P55, 14G25, 14J20 (secondary).

Keywords: Hardy–Littlewood circle method, pairs of quadratic forms, rational points.

This journal is © Foundation Compositio Mathematica 2013.

support. Our analysis of the density of \mathbb{Q} -rational points on X will be activated via the weighted sum

$$S(B) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ 2 \nmid Q_1(\mathbf{x}) \\ Q_2(\mathbf{x})=0}} r(Q_1(\mathbf{x}))W\left(\frac{\mathbf{x}}{B}\right), \tag{1.1}$$

for $B \rightarrow \infty$. The requirement that $Q_1(\mathbf{x})$ be odd is not strictly necessary but makes our argument technically simpler. Simple heuristics lead one to expect that $S(B)$ has order of magnitude B^{n-2} , provided that there are points in $X(\mathbb{R})$ and $X(\mathbb{Q}_p)$ for every prime p . Confirmation of this fact is provided by the work of Birch [Bir61] when $n \geq 12$. Alternatively, when Q_1 and Q_2 are both diagonal and the form $b_1q_1 + b_2q_2$ is indefinite and has rank at least 5 for every non-zero pair $(b_1, b_2) \in \mathbb{R}^2$, then Cook [Coo71] shows that $n \geq 7$ is permissible. The following result offers an improvement over both of these results.

THEOREM 1. *Let $n \geq 7$ and assume that V is non-singular with Q_2 also non-singular. Assume that $Q_1(\mathbf{x}) \gg 1$ and $|\nabla Q_1(\mathbf{x})| \gg 1$, for an absolute implied constant, for every $\mathbf{x} \in \text{supp}(W)$. Suppose that $X(\mathbb{R})$ is non-empty. Then there exist constants $c > 0$ and $\delta > 0$ such that*

$$S(B) = cB^{n-2} + O(B^{n-2-\delta}).$$

The implied constant is allowed to depend on Q_1, Q_2 and W .

In § 8 an explicit value of δ will be given and it will be explained that the leading constant is an absolutely convergent product of local densities $c = \sigma_\infty \prod_p \sigma_p$, whose positivity is equivalent to the hypothesis that $X(\mathbb{R})$ and $X(\mathbb{Q}_p)$ are non-empty for each prime p . Work of Demjanov [Dem56] shows that p -adic solubility is automatic for pairs of quadratic forms in at least nine variables.

Our proof of Theorem 1 uses the circle method. An inherent technical difficulty in applying the circle method to systems of more than one equation lies in the lack of a suitable analogue of the Farey dissection of the unit interval, as required for the so-called ‘Kloosterman refinement’. In the present case this difficulty is circumvented by the specific shape of the quadratic forms q_1, q_2 . Thus it is possible to trade the equality $Q_1(\mathbf{x}) = x_{n+1}^2 + x_{n+2}^2$ for a family of congruences using the familiar identity

$$r(M) = 4 \sum_{d|M} \chi(d),$$

where χ is the real non-principal character modulo 4. In this fashion the sum $S(B)$ can be thought of as counting suitably weighted solutions $\mathbf{x} \in \mathbb{Z}^n$ of the quadratic equation $Q_2(\mathbf{x}) = 0$, for which $Q_1(\mathbf{x}) \equiv 0 \pmod{d}$, for varying d . Our approach ought to be compared with joint work of the second author with Iwaniec [IM10], wherein an upper bound is achieved for the number of integer solutions in a box to the pair of quadratic equations $Q_1(\mathbf{x}) = \square$ and $Q_2(\mathbf{x}) = 0$, when $n = 4$. In this case a simple upper bound sieve is used to detect the square, which thereby allows the first equation to be exchanged for a suitable family of congruences. In both settings, the circle method is used to detect the single equation $Q_2(\mathbf{x}) = 0$, in the form developed by Heath-Brown [Hea96, Theorem 1]. This sets the scene for a double Kloosterman refinement by way of Poisson summation.

We now come to the crux of our argument. For typical values of \mathbf{x} , with $W(\mathbf{x}/B) \neq 0$, we see that $Q_2(\mathbf{x})$ will have order B^2 . Applying [Hea96] to detect when $Q_2(\mathbf{x})$ vanishes leads to certain exponential sums indexed by d and q , for q typically of order B . Having to handle such large values of q would prevent us from achieving a version of Theorem 1, even for sufficiently large n . Instead, we shall first replace the desired equality $Q_2(\mathbf{x}) = 0$ by the congruence $Q_2(\mathbf{x}) \equiv 0 \pmod{d}$

and the equality $Q_2(\mathbf{x})/d = 0$. The resulting application of [Hea96, Theorem 1] then leads to exponential sums indexed by d and q , for q typically of order \sqrt{B} . This observation underpins our entire investigation. The exponential sums that feature take the shape

$$S_{d,q}(\mathbf{m}) = \sum_{a \pmod{q}}^* \sum_{\substack{\mathbf{k} \pmod{dq} \\ Q_1(\mathbf{k}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{k}) \equiv 0 \pmod{d}}} e_{dq}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}), \tag{1.2}$$

for positive integers d and q and varying $\mathbf{m} \in \mathbb{Z}^n$. The notation \sum^* means that the sum is taken over elements coprime to the modulus. We will extend it to summations over vectors in the obvious way.

There is a basic multiplicativity relation at work which renders it profitable to consider the cases $d = 1$ and $q = 1$ separately in (1.2). In the former case we will need to gain sufficient cancellation in the sums that emerge by investigating the analytic properties of the associated Dirichlet series

$$\xi(s; \mathbf{m}) = \sum_{q=1}^{\infty} \frac{S_{1,q}(\mathbf{m})}{q^s},$$

for $s \in \mathbb{C}$. This is facilitated by the fact that $S_{1,q}(\mathbf{m})$ can be evaluated explicitly using the formulae for quadratic Gauss sums. We will see in §4 that $\xi(s; \mathbf{m})$ is absolutely convergent for $\Re(s) > n/2 + 2$. In order to prove Theorem 1 it is important to establish an analytic continuation of $\xi(s; \mathbf{m})$ to the left of this line. This eventually allows us to establish an asymptotic formula for $S(B)$ provided that $n > 6$. The situation for $n = 6$ is more delicate and we are no longer able to win sufficient cancellation through an analysis of $\xi(s; \mathbf{m})$ alone. In fact it appears desirable to exploit cancellation due to sign changes in the exponential sum $S_{d,1}(\mathbf{m})$. The latter is associated to a pair of quadratic forms, rather than a single form, and this raises significant technical obstacles. We intend to return to this topic in a future publication.

With a view to subsequent refinements, much of our argument works under much greater generality than for the quadratic forms considered in Theorem 1. In line with this, unless otherwise indicated, any estimate concerning quadratic forms $Q_1, Q_2 \in \mathbb{Z}[x_1, \dots, x_n]$ is valid for arbitrary forms such that Q_2 is non-singular, $n \geq 4$ and the variety $V \subset \mathbb{P}^{n-1}$ defined by $Q_1(\mathbf{x}) = Q_2(\mathbf{x}) = 0$ is a geometrically integral complete intersection. We let

$$\varrho(d) = S_{d,1}(\mathbf{0}) = \#\{\mathbf{k} \pmod{d} : Q_1(\mathbf{k}) \equiv Q_2(\mathbf{k}) \equiv 0 \pmod{d}\}.$$

The Lang–Weil estimate yields $\varrho(p) = O(p^{n-2})$ when $d = p$ is a prime, since the affine cone over V has dimension $n - 2$. We will need upper bounds for $\varrho(d)$ of comparable strength for any d . It will be convenient to make the following hypothesis.

HYPOTHESIS. Let $d \in \mathbb{N}$ and $\varepsilon > 0$. Then we have $\varrho(d) = O(d^{n-2+\varepsilon})$.

Here, as throughout our work, the implied constant is allowed to depend upon the coefficients of the quadratic forms Q_1, Q_2 under consideration and the parameter ε . We will further allow all our implied constants to depend on the weight function W in (1.1), with any further dependence being explicitly indicated by appropriate subscripts. We will establish Hypothesis- ϱ in Lemma 2 when V is non-singular, as required for Theorem 1.

Notation and conventions. Throughout our work \mathbb{N} will denote the set of positive integers. The parameter ε will always denote a small positive real number, which is allowed to take different values at different parts of the argument. We shall use $\|\mathbf{x}\|$ to denote the norm $\max |x_i|$ of a

vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$. Next, given integers m and M , by writing $m \mid M^\infty$ we will mean that any prime divisor of m is also a prime divisor of M . Likewise (m, M^∞) is taken to mean the largest positive divisor h of m for which $h \mid M^\infty$. It will be convenient to record the bound

$$\#\{m \leq x : m \mid M^\infty\} \leq \sum_{p \mid m \Rightarrow p \mid M} \left(\frac{x}{m}\right)^\varepsilon = x^\varepsilon \prod_{p \mid M} (1 - p^{-\varepsilon})^{-1} \ll (x \mid M)^\varepsilon, \tag{1.3}$$

for any $x \geq 1$, a fact that we shall make frequent use of in our work. Finally we will write $e(x) = \exp(2\pi i x)$ and $e_q(x) = \exp(2\pi i x/q)$.

2. Auxiliary estimates

2.1 Linear congruences

Let $q \in \mathbb{N}$. For $n \times n$ matrices \mathbf{M} , with coefficients in \mathbb{Z} , and a vector $\mathbf{a} \in \mathbb{Z}^n$ we will often be led to consider the cardinality

$$K_q(\mathbf{M}; \mathbf{a}) = \#\{\mathbf{x} \pmod{q} : \mathbf{M}\mathbf{x} \equiv \mathbf{a} \pmod{q}\}. \tag{2.1}$$

The Chinese remainder theorem implies that $K_q(\mathbf{M}; \mathbf{a})$ is a multiplicative function of q , rendering it sufficient to conduct our analysis at prime powers $q = p^r$. We will need the following basic upper bound.

LEMMA 1. *Assume that \mathbf{M} has rank ϱ and let δ_p be the minimum of the p -adic orders of the $\varrho \times \varrho$ non-singular submatrices of \mathbf{M} . Then we have*

$$K_{p^r}(\mathbf{M}; \mathbf{a}) \leq \min\{p^{nr}, p^{(n-\varrho)r+\delta_p}\}.$$

In particular, $K_{p^r}(\mathbf{M}; \mathbf{a}) = O_{\mathbf{M}}(1)$ if $\varrho = n$.

This is established by Loxton [Lox00, Proposition 7], but is also a trivial consequence of earlier work by Smith [Smi71], which provides a precise equality for $K_{p^r}(\mathbf{M}; \mathbf{a})$. We present a proof of Lemma 1, for completeness, the upper bound $K_{p^r}(\mathbf{M}; \mathbf{a}) \leq p^{nr}$ being trivial.

Proof. Given \mathbf{M} as in the statement of the lemma, it follows from the theory of the Smith normal form that there exist unimodular integer matrices \mathbf{A}, \mathbf{B} such that

$$\mathbf{A}\mathbf{M}\mathbf{B} = \text{diag}(M_1, \dots, M_n),$$

with $M_1, \dots, M_n \in \mathbb{Z}$ satisfying $M_i \mid M_{i+1}$, for $1 \leq i < n$. In particular, since \mathbf{M} has rank ϱ , it follows that $M_i = 0$ for $i > \varrho$. Hence

$$\begin{aligned} K_{p^r}(\mathbf{M}; \mathbf{a}) &= \#\{\mathbf{x} \pmod{p^r} : M_i x_i \equiv (\mathbf{A}\mathbf{a})_i \pmod{p^r}, (1 \leq i \leq \varrho)\} \\ &\leq p^{(n-\varrho)r+v_p(M_1)+\dots+v_p(M_\varrho)}. \end{aligned}$$

This completes the proof of Lemma 1, since $\delta_p = v_p(M_1) + \dots + v_p(M_\varrho)$. □

We end this section by drawing a conclusion about the special case that \mathbf{M} is non-singular, with $\varrho = n$. Suppose that there exists a vector \mathbf{x} counted by $K_{p^r}(\mathbf{M}; \mathbf{0})$, but satisfying $p \nmid \mathbf{x}$. Then it follows from our passage to the Smith normal form that in fact $r \leq v_p(\det \mathbf{M})$.

2.2 Geometry of V

In this section we consider the geometry of the varieties $V \subset \mathbb{P}^{n-1}$ defined by the common zero locus of two quadratic forms $Q_1, Q_2 \in \mathbb{Z}[x_1, \dots, x_n]$, specifically in the case that V is non-singular. Suppose that Q_i has underlying symmetric matrix \mathbf{M}_i , with \mathbf{M}_2 non-singular.

Let $D = D(Q_1, Q_2)$ be the discriminant of the pair $\{Q_1, Q_2\}$, which is a non-zero integer by assumption. According to Gelfand *et al.* [GKZ94, § 13], D has total degree $(n + 2)2^{n+1}$ in the coefficients of Q_1, Q_2 and is equal to the discriminant of the bihomogeneous polynomial

$$F(\mathbf{b}, \mathbf{x}) = b_1Q_1(\mathbf{x}) + b_2Q_2(\mathbf{x}).$$

We write

$$\mathbf{M}(\mathbf{b}) = b_1\mathbf{M}_1 + b_2\mathbf{M}_2, \tag{2.2}$$

for the underlying symmetric matrix. It follows from [CSS87a, Lemma 1.13] that

$$\text{rank } \mathbf{M}(\mathbf{b}) \geq n - 1 \tag{2.3}$$

for any $[\mathbf{b}] \in \mathbb{P}^1$. Furthermore, the binary form $P(\mathbf{b}) = \det \mathbf{M}(\mathbf{b})$ has non-zero discriminant, by Reid’s thesis [Rei72].

An important rôle in our work will be played by the dual variety $V^* \subset \mathbb{P}^{n-1*} \cong \mathbb{P}^{n-1}$ of V . Consider the incidence relation

$$I = \{(x, H) \in V \times \mathbb{P}^{n-1*} : H \supseteq \mathbb{T}_x(V)\},$$

where $\mathbb{T}_x(V)$ denotes the tangent hyperplane to V at x . The projection $\pi_1 : I \rightarrow V$ makes I into a bundle over V whose fibres are subspaces of dimension $n - \dim V - 2 = 1$. In particular, I is an irreducible variety of dimension $n - 2$. Since V^* is defined to be the image of the projection $\pi_2 : I \rightarrow \mathbb{P}^{n-1*}$, it therefore follows that the dual variety V^* is irreducible. Furthermore, since I has dimension $n - 2$ one might expect that V^* is a hypersurface in \mathbb{P}^{n-1*} . This fact, which is valid for any irreducible non-linear complete intersection, is established by Ein [Ein86, Proposition 3.1]. Elimination theory shows that the defining homogeneous polynomial may be taken to have coefficients in \mathbb{Z} . Finally, by the work of Aznar [Azn80, Theorem 3], the degree of V^* is $4(n - 2)$. Hence V^* is defined by an equation $G = 0$, where $G \in \mathbb{Z}[x_1, \dots, x_n]$ is an absolutely irreducible form of degree $4(n - 2)$.

Given a prime p , which is sufficiently large in terms of the coefficients of V , the reduction of V modulo p will inherit many of the basic properties enjoyed by V as a variety over \mathbb{Q} . In particular, it will continue to be a non-singular complete intersection of codimension 2, satisfying the property that (2.3) holds for any $[\mathbf{b}] \in \mathbb{P}^1$, where now \mathbf{M}_i is taken to be the matrix obtained after reduction modulo p of the entries. Furthermore we may assume that $p \nmid 2 \det \mathbf{M}_2$ and that the discriminant of the polynomial $P(\mathbf{b})$ does not vanish modulo p . We will henceforth set

$$\Delta_V = O(1)$$

to be the product of all primes for which any one of these properties fails at that prime.

2.3 The function $\varrho(d)$

In this section we establish Hypothesis- ϱ when V is non-singular, where $\varrho(d) = S_{d,1}(\mathbf{0})$, in the notation of (1.2). Note that $\varrho^*(d) \leq \varrho(d)$, where

$$\varrho^*(d) = \#\{\mathbf{x} \pmod{d} : (d, \mathbf{x}) = 1, Q_1(\mathbf{x}) \equiv Q_2(\mathbf{x}) \equiv 0 \pmod{d}\}.$$

We proceed to establish the following result.

LEMMA 2. *Hypothesis- ϱ holds if V is non-singular.*

Proof. We adapt an argument of Hooley [Hoo88, § 10] used to handle the analogous situation for cubic hypersurfaces. By multiplicativity it suffices to examine the case $d = p^r$ for a prime p

and $r \in \mathbb{N}$. Extracting common factors between \mathbf{x} and p^r , we see that

$$\varrho(p^r) = \sum_{0 \leq k < r/2} p^{kn} \varrho^*(p^{r-2k}) + p^{(r-\lceil r/2 \rceil)n}. \tag{2.4}$$

Using additive characters to detect the congruences gives

$$\varrho^*(p^s) = \frac{1}{p^{2s}} \sum_{\mathbf{b} \pmod{p^s}} \sum_{\mathbf{x} \pmod{p^s}}^* e_{p^s}(b_1 Q_1(\mathbf{x}) + b_2 Q_2(\mathbf{x})),$$

where we recall that the notation \sum^* means only \mathbf{x} for which $p \nmid \mathbf{x}$ are of interest. Extracting common factors between p^s and \mathbf{b} yields

$$\varrho^*(p^s) = \frac{1}{p^{2s}} \sum_{0 \leq i < s} p^{in} S(s-i) + p^{(n-2)s} \left(1 - \frac{1}{p^n}\right),$$

with

$$S(k) = \sum_{\mathbf{b} \pmod{p^k}}^* \sum_{\mathbf{x} \pmod{p^k}}^* e_{p^k}(F(\mathbf{b}, \mathbf{x})),$$

with $F(\mathbf{b}, \mathbf{x}) = b_1 Q_1(\mathbf{x}) + b_2 Q_2(\mathbf{x})$. We claim that

$$S(k) = \begin{cases} O(p^n) & \text{if } k = 1, \\ O(1) & \text{if } k \geq 2. \end{cases}$$

Once achieved, this implies that $\varrho^*(p^s) = O(p^{(n-2)s})$. Inserting this into (2.4) gives the bound $\varrho(p^r) = O(rp^{(n-2)r})$, which suffices for the lemma.

The Lang–Weil estimate implies that there are $O(p^{n-1})$ choices of $\mathbf{x} \pmod{p}$ for which $Q_1(\mathbf{x})Q_2(\mathbf{x}) \equiv 0 \pmod{p}$. Likewise it implies that $\varrho^*(p) = O(p^{n-2})$. When $k = 1$, therefore, we conclude that

$$|S(1)| \leq p^2 \varrho^*(p) + p \sum_{i=1,2} \#\{\mathbf{x} \pmod{p} : Q_i(\mathbf{x}) \equiv 0 \pmod{p}\} + p^n \ll p^n.$$

To analyse $S(k)$, for $k \geq 2$, we introduce a dummy sum over $a \in (\mathbb{Z}/p^k\mathbb{Z})^*$ and replace \mathbf{b} by $a\mathbf{b}$ to get

$$\varphi(p^k)S(k) = \sum_{a \pmod{p^k}}^* \sum_{\mathbf{b} \pmod{p^k}}^* \sum_{\mathbf{x} \pmod{p^k}}^* e_{p^k}(aF(\mathbf{b}, \mathbf{x})).$$

Evaluating the resulting Ramanujan sum yields

$$S(k) = \left(1 - \frac{1}{p}\right)^{-1} \{N(p^k) - p^{n+1}N(p^{k-1})\}, \tag{2.5}$$

where $N(p^k)$ is the number of $(\mathbf{b}, \mathbf{x}) \pmod{p^k}$, with $p \nmid \mathbf{b}$ and $p \nmid \mathbf{x}$, for which $p^k \mid F(\mathbf{b}, \mathbf{x})$. We are therefore led to compare $N(p^k)$ with $N(p^{k-1})$, using an approach based on Hensel’s lemma.

Let $\nabla F(\mathbf{b}, \mathbf{x}) = (Q_1(\mathbf{x}), Q_2(\mathbf{x}), b_1 \nabla_{\mathbf{x}} Q_1(\mathbf{x}) + b_2 \nabla_{\mathbf{x}} Q_2(\mathbf{x}))$, where $\nabla_{\mathbf{x}}$ means that the partial derivatives are taken with respect to the \mathbf{x} variables. Using our alternative definition of the discriminant D as the discriminant of F , we may view D as the resultant of the $n + 2$ quadratic forms appearing in $\nabla F(\mathbf{b}, \mathbf{x})$. Writing $\mathbf{y} = (\mathbf{b}, \mathbf{x})$, elimination theory therefore produces $n + 2$ identities of the form

$$Dy_i^N = \sum_{1 \leq j \leq n+2} G_{ij}(\mathbf{y}) \frac{\partial F}{\partial y_i} \quad (1 \leq i \leq n + 2),$$

where G_{ij} are polynomials with coefficients in \mathbb{Z} . In particular, if the vector $(\mathbf{b}, \mathbf{x}) \in \mathbb{Z}^{n+2}$ satisfies $p^m \mid \nabla F(\mathbf{b}, \mathbf{x})$, but $p \nmid \mathbf{b}$ and $p \nmid \mathbf{x}$, it follows that $m \leq v_p(D)$. Let us put $\delta = v_p(D)$.

If $2 \leq k \leq 2\delta + 1$, then it trivially follows from (2.5) that $S(k) = O(1)$. If $k \geq 2\delta + 2$, which we assume for the remainder of the argument, we will show that $S(k) = 0$. Our work so far has shown that

$$N(p^k) = \sum_{0 \leq m \leq \delta} \#C_m(p^k),$$

where $C_m(p^k)$ denotes the set of $\mathbf{y} = (\mathbf{b}, \mathbf{x}) \pmod{p^k}$, with $p \nmid \mathbf{b}$ and $p \nmid \mathbf{x}$, for which $p^k \mid F(\mathbf{y})$ and $p^m \parallel \nabla F(\mathbf{y})$. Given any $\mathbf{y} \in C_m(p^k)$ it is easy to see that

$$\begin{aligned} F(\mathbf{y} + p^{k-m}\mathbf{y}') &\equiv F(\mathbf{y}) + p^{k-m}\mathbf{y}' \cdot \nabla F(\mathbf{y}) \pmod{p^k} \\ &\equiv 0 \pmod{p^k}, \end{aligned}$$

for any $\mathbf{y}' \in \mathbb{Z}^{n+2}$, with

$$\begin{aligned} \nabla F(\mathbf{y} + p^{k-m}\mathbf{y}') - \nabla F(\mathbf{y}) &\equiv \mathbf{0} \pmod{p^{k-m}} \\ &\equiv \mathbf{0} \pmod{p^{m+1}}. \end{aligned}$$

Thus $C_m(p^k)$ consists of cosets modulo p^{k-m} . Moreover, $\mathbf{y} + p^{k-m}\mathbf{y}' \in C_m(p^{k+1})$ if and only if

$$p^{-k}F(\mathbf{y}) + p^{-m}\mathbf{y}' \cdot \nabla F(\mathbf{y}) \equiv 0 \pmod{p},$$

for which there are p^{n+1} incongruent solutions modulo p . Hence $\#C_m(p^{k+1}) = p^{n+1}\#C_m(p^k)$, which therefore shows that $S(k) = 0$ in (2.5). This completes the proof of the lemma. \square

2.4 Treatment of bad d

Returning briefly to $S(B)$ in (1.1), we will need a separate argument to deal with the contribution from \mathbf{x} for which $Q_2(\mathbf{x}) = 0$ and $Q_1(\mathbf{x})$ is divisible by large values of d which share a common prime factor with Δ_V .

To begin with, we call upon joint work of the first author with Heath-Brown and Salberger [BHS06], which is concerned with uniform upper bounds for counting functions of the shape

$$M(f; B) = \#\{\mathbf{t} \in \mathbb{Z}^\nu : |\mathbf{t}| \leq B, f(\mathbf{t}) = 0\},$$

for polynomials $f \in \mathbb{Z}[t_1, \dots, t_\nu]$ of degree $\delta \geq 2$. Although the paper focuses on the situation for $\delta \geq 3$, the methods developed also permit a useful estimate in the case $\delta = 2$. Suppose that $\nu = 3$ and that the quadratic homogeneous part f_0 of f is absolutely irreducible. Using [BHS06, Lemmas 6 and 7] we can find a linear form $L \in \mathbb{Z}[t_1, t_2, t_3]$ of height $O(1)$ such that the intersection of the projective plane curves $f_0 = 0$ and $L = 0$ consists of two distinct points. After eliminating one of the variables, we are then free to apply [BHS06, Lemma 13] to all the affine curves defined by $f = 0$ and $L = c$, for each integer $c \ll B$. This gives the upper bound $M(f; B) \ll B^{1+\varepsilon}$ when $\nu = 3$. According to [BHS06, Lemma 8], we have therefore established the following result, which may be of independent interest.

LEMMA 3. *Let $\varepsilon > 0$, let $\nu \geq 3$ and let $f \in \mathbb{Z}[t_1, \dots, t_\nu]$ be a quadratic polynomial with absolutely irreducible quadratic homogeneous part. Then we have*

$$M(f; B) \ll B^{\nu-2+\varepsilon}.$$

The implied constant in this estimate depends at most on ν and the choice of ε .

We shall also require some facts about lattices, as established by Davenport [Dav63, Lemma 5]. Suppose that $\Lambda \subset \mathbb{Z}^n$ is a lattice of rank r and determinant $\det(\Lambda)$. Then there exists a ‘minimal’ basis $\mathbf{m}_1, \dots, \mathbf{m}_r$ of Λ such that $1 \leq |\mathbf{m}_1| \leq \dots \leq |\mathbf{m}_r|$, with the property that whenever one writes $\mathbf{y} \in \Lambda$ as $\mathbf{y} = \sum_{i=1}^r \lambda_i \mathbf{m}_i$, then $\lambda_i \ll |\mathbf{m}_i|^{-1} |\mathbf{y}|$, for $1 \leq i \leq r$. Furthermore,

$$\prod_{i=1}^r |\mathbf{m}_i| \ll \det(\Lambda) \leq \prod_{i=1}^r |\mathbf{m}_i|. \tag{2.6}$$

We now come to the key technical estimate in this section. Given any $d \in \mathbb{N}$ and $B \geq 1$, we will need an auxiliary upper bound for the quantity

$$N_d(B) = \#\{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| \leq B, d \mid Q_1(\mathbf{x}), Q_2(\mathbf{x}) = 0\}. \tag{2.7}$$

Simple heuristics suggest that $N_d(B)$ should have order $d^{-1} B^{n-2}$. For our purposes we require an upper bound in which any power of d is saved.

LEMMA 4. *Let $\varepsilon > 0, d \in \mathbb{N}$ and $n \geq 5$. Assume $B \geq d$ and Hypothesis- ϱ . Then we have*

$$N_d(B) \ll \frac{B^{n-2+\varepsilon}}{d^{1/n}} + dB^{n-3+\varepsilon}.$$

Note that this estimate is valid for any quadratic forms Q_1, Q_2 for which Q_2 is non-singular and the expected bound for $\varrho(d)$ holds. In our case the desired bound follows from Lemma 2 when V is non-singular.

Proof of Lemma 4. On extracting common factors between \mathbf{x} and d in $N_d(B)$, one quickly verifies that it suffices to prove the upper bound in the lemma for the quantity $N_d^*(B)$, in which the additional constraint $(d, \mathbf{x}) = 1$ is added. Breaking into residue classes modulo d , we see that

$$N_d^*(B) = \sum_{\substack{\boldsymbol{\xi} \pmod{d} \\ Q_1(\boldsymbol{\xi}) \equiv 0 \pmod{d} \\ Q_2(\boldsymbol{\xi}) \equiv 0 \pmod{d}}} \#\{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}| \leq B, \mathbf{x} \equiv \boldsymbol{\xi} \pmod{d}, Q_2(\mathbf{x}) = 0\}. \tag{2.8}$$

Let us denote the set whose cardinality appears in the inner sum by $S_d(B; \boldsymbol{\xi})$. If $S_d(B; \boldsymbol{\xi}) = \emptyset$, then there is nothing to prove. Alternatively, suppose we are given $\mathbf{x}_0 \in S_d(B; \boldsymbol{\xi})$. Then any other vector in the set must be congruent to \mathbf{x}_0 modulo d .

Making the change of variables $\mathbf{x} = \mathbf{x}_0 + d\mathbf{y}$ in $S_d(B; \boldsymbol{\xi})$, we note that $|\mathbf{y}| \leq Y$, with $Y = 2d^{-1}B$. Furthermore, Taylor’s formula yields

$$\mathbf{y} \cdot \nabla Q_2(\mathbf{x}_0) + dQ_2(\mathbf{y}) = 0, \tag{2.9}$$

since $Q_2(\mathbf{x}_0 + d\mathbf{y}) = 0$ and $Q_2(\mathbf{x}_0) = 0$. This equation implies that the \mathbf{y} under consideration are forced to satisfy the congruence $\mathbf{y} \cdot \nabla Q_2(\boldsymbol{\xi}) \equiv 0 \pmod{d}$, since $\mathbf{x}_0 \equiv \boldsymbol{\xi} \pmod{d}$. Let us write $\mathbf{a} = \nabla Q_2(\boldsymbol{\xi})$. Then it follows that

$$\#S_d(B; \boldsymbol{\xi}) \leq 1 + \#\{\mathbf{y} \in \Lambda_{\mathbf{a}} : |\mathbf{y}| \leq Y, (2.9) \text{ holds}\},$$

where $\Lambda_{\mathbf{a}} = \{\mathbf{y} \in \mathbb{Z}^n : \mathbf{a} \cdot \mathbf{y} \equiv 0 \pmod{d}\}$. This set defines an integer lattice of full rank and determinant $\det \Lambda_{\mathbf{a}} = d/(d, \mathbf{a})$. The conditions of summation in (2.8) demand that $(d, \boldsymbol{\xi}) = 1$. It therefore follows from the remark at the end of § 2.1 that $p^j \ll 1$, whenever $j \in \mathbb{N}$ and p is a prime for which $p^j \mid (d, \nabla Q_2(\boldsymbol{\xi}))$. Thus $(d, \mathbf{a}) \ll 1$ and so $\det \Lambda_{\mathbf{a}} \gg d$.

Let \mathbf{M} denote the non-singular matrix formed from taking a minimal basis $\mathbf{m}_1, \dots, \mathbf{m}_n$ for $\Lambda_{\mathbf{a}}$. Making the change of variables $\mathbf{y} = \mathbf{M}\boldsymbol{\lambda}$, and recalling the properties of the minimal basis recorded above, we see that

$$\#S_d(B; \boldsymbol{\xi}) \leq 1 + \#\{\boldsymbol{\lambda} \in \mathbb{Z}^n : \lambda_i \ll |\mathbf{m}_i|^{-1} Y \text{ for } 1 \leq i \leq n, q(\boldsymbol{\lambda}) = 0\},$$

where $q(\boldsymbol{\lambda})$ is obtained from (2.9) via substitution. In particular, the quadratic homogeneous part q_0 of q has underlying matrix $\mathbf{M}^T \mathbf{M}_2 \mathbf{M}$, which is non-singular. We are therefore left with the task of counting integer solutions to a quadratic equation, which are constrained to lie in a lop-sided region. Furthermore, since we require complete uniformity in d , we want an upper bound in which the implied constant does not depend on the coefficients of q .

It being difficult to handle a genuinely lopsided region, we will simply fix the smallest variable and then allow the remaining vectors $\boldsymbol{\lambda}' = (\lambda_1, \dots, \lambda_{n-1})$ to run over the full hypercube with side lengths $O(Y)$. In this way we find that

$$\#S_d(B; \boldsymbol{\xi}) \leq 1 + \sum_{t \ll |\mathbf{m}_n|^{-1} Y} \#\{\boldsymbol{\lambda}' \in \mathbb{Z}^{n-1} : |\boldsymbol{\lambda}'| \ll Y, q(\boldsymbol{\lambda}', t) = 0\}.$$

Viewed as a polynomial in $\boldsymbol{\lambda}'$, the quadratic homogeneous part of $q(\boldsymbol{\lambda}', t)$ is equal to $q_0(\boldsymbol{\lambda}', 0)$. This must have rank at least $n - 2 \geq 3$, since q_0 is non-singular and its rank cannot decrease by more than 2 on any hyperplane. In particular, $q_0(\boldsymbol{\lambda}', 0)$ is absolutely irreducible. We apply Lemma 3 with $\nu = n - 1$ and $f = q(\boldsymbol{\lambda}', t)$ to get

$$\#S_d(B; \boldsymbol{\xi}) \ll Y^{n-3+\varepsilon} \left(1 + \frac{Y}{|\mathbf{m}_n|}\right).$$

Now it follows from (2.6) that $|\mathbf{m}_n| \geq (\det \Lambda_{\mathbf{a}})^{1/n} \gg d^{1/n}$. Recalling that $Y = 2d^{-1}B$ and inserting this into (2.8), we conclude that

$$N_d^*(B) \ll \varrho(d) \left(\frac{B}{d}\right)^{n-3+\varepsilon} \left(1 + \frac{B}{d^{1+1/n}}\right).$$

The conclusion of the lemma therefore follows from Hypothesis- ϱ . □

3. Preliminary transformation of $S(B)$

In this section we initiate our analysis of $S(B)$ in (1.1). For any odd integer M it is clear that $r(M) = 0$ unless $M \equiv 1 \pmod{4}$. Hence our sum can be written

$$S(B) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ Q_1(\mathbf{x}) \equiv 1 \pmod{4} \\ Q_2(\mathbf{x}) = 0}} r(Q_1(\mathbf{x})) W\left(\frac{\mathbf{x}}{B}\right).$$

We proceed to open up the r -function in the summand. Let $\{V_T(t)\}_T$ be a collection of smooth functions, with V_T supported in the dyadic block $[T, 2T]$, such that $\sum_T V_T(t) = 1$ for $t \in [1, CB^2]$. The constant C will be large enough depending on Q_1 and W , so that $|Q_1(\mathbf{x})| \leq C$ whenever $\mathbf{x} \in \text{supp}(W)$. We will neither specify the function V_T nor the indexing set for T . However we will simply note that T can be restricted to lie in the interval $[\frac{1}{2}, 2CB^2]$, and that there are $O(\log B)$ many functions in the collection. Moreover we will stipulate that

$$t^j V_T^{(j)}(t) \ll_j 1,$$

for each integer $j \geq 0$. For a positive integer $M \leq CB^2$ we may write

$$r(M) = 4 \sum_T \sum_{d|M} \chi(d) V_T(d).$$

It follows that

$$S(B) = 4 \sum_T \sum_d \chi(d) V_T(d) \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ Q_1(\mathbf{x}) \equiv 1 \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{x}) = 0}} W\left(\frac{\mathbf{x}}{B}\right) = 4 \sum_T S_T(B),$$

say. Let $\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n$ be such that $Q_1(\mathbf{a}) \equiv 1 \pmod{4}$, and let $S_{T,\mathbf{a}}(B)$ be the part of $S_T(B)$ which comes from $\mathbf{x} \equiv \mathbf{a} \pmod{4}$.

In the analysis of $S_{T,\mathbf{a}}(B)$ we want to arrange things so that only values of d satisfying $d \ll B$ occur. When $T \leq B$ this is guaranteed by the presence of the factor $V_T(d)$. When $T > B$ we can use Dirichlet’s hyperbola trick, since $\chi(Q_1(\mathbf{x})) = \chi(Q_1(\mathbf{a})) = 1$, to get

$$S_{T,\mathbf{a}}(B) = \sum_d \chi(d) \sum_{\substack{\mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{x}) = 0}} W\left(\frac{\mathbf{x}}{B}\right) V_T\left(\frac{Q_1(\mathbf{x})}{d}\right).$$

In this case too we therefore have $d \ll B$. For notational simplicity we write

$$W_{d,T}(\mathbf{y}) = \begin{cases} W(\mathbf{y}) V_T(d) & \text{if } T \leq B, \\ W(\mathbf{y}) V_T\left(\frac{B^2 Q_1(\mathbf{y})}{d}\right) & \text{otherwise.} \end{cases} \tag{3.1}$$

Here $W : \mathbb{R}^n \rightarrow \mathbb{R}_{\geq 0}$ is an infinitely differentiable bounded function of compact support such that $Q_1(\mathbf{x}) \gg 1$ and $|\nabla Q_1(\mathbf{x})| \gg 1$, for some absolute implied constant, for every $\mathbf{x} \in \text{supp}(W)$.

Our plan is to use the circle method to analyse $S_{T,\mathbf{a}}(B)$, together with an application of Poisson summation. This leads us to study the exponential sums (1.2), for varying $\mathbf{m} \in \mathbb{Z}^n$. We will face significant technical issues in estimating this sum when d has a large prime power factor p^r , in which p divides the constant Δ_V that was introduced at the close of § 2.2. This issue will be handled by separating out the contribution from the awkward d as follows.

LEMMA 5. *Let Ξ be a parameter satisfying $1 \leq \Xi \leq B$. Then we have*

$$S(B) = 4 \sum_T \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} (S_{T,\mathbf{a}}^b(B) + S_{T,\mathbf{a}}^\sharp(B)),$$

with

$$S_{T,\mathbf{a}}^b(B) = \sum_{\substack{d=1 \\ (d, \Delta_V^\infty) > \Xi}}^\infty \chi(d) \sum_{\substack{\mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{x}) = 0}} W_{d,T}\left(\frac{\mathbf{x}}{B}\right),$$

$$S_{T,\mathbf{a}}^\sharp(B) = \sum_{\substack{d=1 \\ (d, \Delta_V^\infty) \leq \Xi}}^\infty \chi(d) \sum_{\substack{\mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{x}) = 0}} W_{d,T}\left(\frac{\mathbf{x}}{B}\right).$$

We will provide an upper bound for $S_{T,\mathbf{a}}^b(B)$ and an asymptotic formula for $S_{T,\mathbf{a}}^\sharp(B)$, always assuming that Ξ satisfies $1 \leq \Xi \leq B$. The following result deals with the first task.

LEMMA 6. *Let $\varepsilon > 0$ and assume Hypothesis- ρ . Then we have*

$$S_{T,\mathbf{a}}^b(B) \ll \Xi^{-1/n} B^{n-2+\varepsilon} + \Xi B^{n-3+\varepsilon}.$$

Proof. Write $e = (d, \Delta_V^\infty)$. Then

$$|S_{T,\mathbf{a}}^b(B)| \leq \sum_{\substack{e|\Delta_V^\infty \\ e > \Xi}} \sum_{d=1}^\infty \sum_{\substack{\mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{de} \\ Q_2(\mathbf{x}) = 0}} W_{de,T} \left(\frac{\mathbf{x}}{B} \right).$$

By the properties of (3.1), only d, e satisfying $de \ll B$ feature here. Inverting the sums over d and \mathbf{x} , we obtain

$$S_{T,\mathbf{a}}^b(B) \ll \sum_{\substack{e|\Delta_V^\infty \\ \Xi < e \ll B}} \sum_{\substack{|\mathbf{x}| \ll B \\ \mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{e} \\ Q_2(\mathbf{x}) = 0}} \tau \left(\frac{Q_1(\mathbf{x})}{e} \right),$$

where τ is the divisor function. Note that $Q_1(\mathbf{x}) \neq 0$, since $Q_1(\mathbf{x}) \equiv Q_1(\mathbf{a}) \equiv 1 \pmod{4}$, so that the inner summand is $O(B^\varepsilon)$ by the trivial estimate for τ . Hence we have

$$S_{T,\mathbf{a}}^b(B) \ll B^\varepsilon \sum_{\substack{e|\Delta_V^\infty \\ \Xi < e \leq cB}} N_e(cB), \tag{3.2}$$

for an absolute constant $c > 0$, in the notation of (2.7).

We will make crucial use of the monotonicity property $N_e(cB) \leq N_d(cB)$ for $d | e$. Suppose that we have a factorisation $\Delta_V = \prod_{i=1}^t p_i$. For $\mathbf{n} \in \mathbb{Z}_{\geq 0}^t$, let $\mathbf{p}^{\mathbf{n}} = \prod_{i=1}^t p_i^{n_i}$. Consider the collection of integers $\mathcal{B} = \{\mathbf{p}^{\mathbf{n}} : \mathbf{n} \in \mathbb{Z}_{\geq 0}^t\}$ and set $\mathcal{B}(A_1, A_2) = \mathcal{B} \cap (A_1, A_2]$. It follows from (1.3) that \mathcal{B} contains $O(B^\varepsilon)$ elements of order B . In this new notation the sum in (3.2) is over $e \in \mathcal{B}(\Xi, cB)$. We claim that

$$S_{T,\mathbf{a}}^b(B) \ll B^\varepsilon \sum_{e \in \mathcal{B}(\Xi, \Delta_V \Xi)} N_e(cB).$$

Once achieved, the statement of the lemma will then follow from Lemma 4.

By the monotonicity property, in order to establish the claim it will suffice to show that every $e \in \mathcal{B}(\Xi, cB)$ has a divisor $e' | e$, with $e' \in \mathcal{B}(\Xi, \Delta_V \Xi)$. To see this, we suppose that $e = \mathbf{p}^{\mathbf{n}}$ and consider the decreasing sequence of divisors of e . This sequence ends at 1, and the ratio between any two consecutive members is bounded by Δ_V . Thus one of the divisors must lie in the range $(\Xi, \Delta_V \Xi]$, as required. This completes the proof of the lemma. \square

Turning to $S_{T,\mathbf{a}}^\sharp(B)$, we now need a means of detecting the equation $Q_2(\mathbf{x}) = 0$. For any integer M let

$$\delta(M) = \begin{cases} 1, & \text{if } M = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Our primary tool in this endeavour will be a version of the circle method developed by Heath-Brown [Hea96], based on work by Duke *et al.* [DFI93]. The starting point for this is the following smooth approximation of δ (see [Hea96, Theorem 1]).

LEMMA 7. *For any $Q > 1$ there is a positive constant c_Q , and a smooth function $h(x, y)$ defined on $(0, \infty) \times \mathbb{R}$, such that*

$$\delta(M) = \frac{c_Q}{Q^2} \sum_{q=1}^\infty \sum_{a \pmod{q}}^* e_q(aM) h \left(\frac{q}{Q}, \frac{M}{Q^2} \right).$$

The constant c_Q satisfies $c_Q = 1 + O_N(Q^{-N})$ for any $N > 0$. Moreover $h(x, y) \ll x^{-1}$ for all y , and $h(x, y)$ is non-zero only for $x \leq \max\{1, 2|y|\}$.

In practice, to detect the equation $M = 0$ for a sequence of integers with $|M| < N/2$, it is logical to choose $Q = N^{1/2}$. We will use the above lemma to detect the equality $Q_2(\mathbf{x}) = 0$ in $S_{T,\mathbf{a}}^\sharp(B)$. However, since we already have the modulus d in the sum over \mathbf{x} we will use this modulus to reduce the size of the parameter Q . This is the key trick that underpins our entire argument. Our idea is to replace the equality $Q_2(\mathbf{x}) = 0$ by the congruence $Q_2(\mathbf{x}) \equiv 0 \pmod{d}$ and the equality $Q_2(\mathbf{x})/d = 0$. This leads to the expression

$$\begin{aligned} S_{T,\mathbf{a}}^\sharp(B) &= \sum_{\substack{d=1 \\ (d, \Delta_\infty^\vee) \leq \Xi}}^\infty \chi(d) \sum_{\substack{\mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{x}) \equiv 0 \pmod{d}}} \delta\left(\frac{Q_2(\mathbf{x})}{d}\right) W_{d,T}\left(\frac{\mathbf{x}}{B}\right) \\ &= \sum_{\substack{d=1 \\ (d, \Delta_\infty^\vee) \leq \Xi}}^\infty \frac{\chi(d)c_Q}{Q^2} \sum_{q=1}^\infty \sum_{a \pmod{q}}^* \sum_{\substack{\mathbf{x} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{x}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{x}) \equiv 0 \pmod{d}}} e_q\left(\frac{aQ_2(\mathbf{x})}{d}\right) h\left(\frac{q}{Q}, \frac{Q_2(\mathbf{x})}{dQ^2}\right) W_{d,T}\left(\frac{\mathbf{x}}{B}\right). \end{aligned}$$

We shall make the choice

$$Q = \frac{B}{\sqrt{d}}.$$

Since $d \ll B$, it follows that $Q \gg \sqrt{B}$.

With our choice of Q made, we remark that the size of the full modulus qd is typically of order $B^{3/2}$. Since this is much smaller than the square of the length of each x_i summation, it will be profitable to use the Poisson summation formula on the sum over \mathbf{x} .

LEMMA 8. For any $N > 0$ we have

$$S_{T,\mathbf{a}}^\sharp(B) = (1 + O_N(B^{-N})) \frac{B^{n-2}}{4^n} \sum_{\mathbf{m} \in \mathbb{Z}^n} \sum_{\substack{d=1 \\ (d, \Delta_\infty^\vee) \leq \Xi}}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{q=1}^\infty \frac{1}{q^n} T_{d,q}(\mathbf{m}) I_{d,q}(\mathbf{m}),$$

where

$$T_{d,q}(\mathbf{m}) = \sum_{a \pmod{q}}^* \sum_{\substack{\mathbf{k} \pmod{4dq} \\ \mathbf{k} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{k}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{k}) \equiv 0 \pmod{d}}} e\left(\frac{4aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}}{4dq}\right)$$

and

$$I_{d,q}(\mathbf{m}) = \int_{\mathbb{R}^n} h\left(\frac{q}{Q}, \frac{B^2 Q_2(\mathbf{y})}{dQ^2}\right) W_{d,T}(\mathbf{y}) e_{4dq}(-B\mathbf{m} \cdot \mathbf{y}) \, d\mathbf{y}.$$

Proof. Splitting the sum over \mathbf{x} into residue classes modulo $4dq$, we get that the inner sum over \mathbf{x} in our expression for $S_{T,\mathbf{a}}^\sharp(B)$ is given by

$$\sum_{\substack{\mathbf{k} \pmod{4dq} \\ \mathbf{k} \equiv \mathbf{a} \pmod{4} \\ Q_1(\mathbf{k}) \equiv 0 \pmod{d} \\ Q_2(\mathbf{k}) \equiv 0 \pmod{d}}} e\left(\frac{aQ_2(\mathbf{k})}{qd}\right) \sum_{\mathbf{x} \in \mathbb{Z}^n} f(\mathbf{x}),$$

where

$$f(\mathbf{x}) = h\left(\frac{q}{Q}, \frac{Q_2(\mathbf{k} + 4dq\mathbf{x})}{dQ^2}\right)W_{d,T}\left(\frac{\mathbf{k} + 4dq\mathbf{x}}{B}\right).$$

Poisson summation yields

$$\begin{aligned} \sum_{\mathbf{x} \in \mathbb{Z}^n} f(\mathbf{x}) &= \sum_{\mathbf{m} \in \mathbb{Z}^n} \int_{\mathbb{R}^n} f(\mathbf{y})e(-\mathbf{m} \cdot \mathbf{y}) \, d\mathbf{y} \\ &= \left(\frac{B}{4dq}\right)^n \sum_{\mathbf{m} \in \mathbb{Z}^n} e_{4dq}(\mathbf{m} \cdot \mathbf{k}) \int_{\mathbb{R}^n} h\left(\frac{q}{Q}, \frac{B^2Q_2(\mathbf{y})}{dQ^2}\right)W_{d,T}(\mathbf{y})e_{4dq}(-B\mathbf{m} \cdot \mathbf{y}) \, d\mathbf{y}. \end{aligned}$$

The lemma follows on rearranging and noting that $c_Q = 1 + O_N(B^{-N})$ and $Q^2 = B^2/d$. □

In this and the next few sections, we will analyse in detail the exponential sum $T_{d,q}(\mathbf{m})$ appearing in Lemma 8. We start with a multiplicativity relation which reduces the problem to analysing the sum for a prime power modulus. Observe that d is necessarily odd, but q can be of either parity. For any $d, q \in \mathbb{N}$ we recall the definition (1.2) of $S_{d,q}(\mathbf{m})$, and for any non-negative integer ℓ define

$$S_{1,2^\ell}^\pm(\mathbf{m}) = \sum_{a \pmod{2^\ell}}^* \sum_{\substack{\mathbf{k} \pmod{2^{2+\ell}} \\ \mathbf{k} \equiv \pm \mathbf{a} \pmod{4}}} e_{2^{2+\ell}}(4aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}). \tag{3.3}$$

We note that if $h \in \mathbb{N}$ is coprime to d and q , then $S_{d,q}(h\mathbf{m}) = S_{d,q}(\mathbf{m})$. The following result is now available.

LEMMA 9. For $q = 2^\ell q'$, with q' odd, we have

$$T_{d,q}(\mathbf{m}) = S_{d,q'}(\mathbf{m})S_{1,2^\ell}^{\chi(dq')}(\mathbf{m}).$$

Proof. Set

$$\mathbf{k} = \mathbf{k}'2^{\ell+2}\overline{2^{\ell+2}} + \mathbf{k}''dq'\overline{dq'}, \quad a = a'2^\ell\overline{2^\ell} + a''q'\overline{q'},$$

where $\mathbf{k}' \pmod{dq'}$, $\mathbf{k}'' \pmod{2^{\ell+2}}$, $a' \pmod{q'}$, and $a'' \pmod{2^\ell}$. The conditions on \mathbf{k} then translate into $\mathbf{k}'' \equiv \mathbf{a} \pmod{4}$, $Q_1(\mathbf{k}') \equiv 0 \pmod{d}$ and $Q_2(\mathbf{k}') \equiv 0 \pmod{d}$. Furthermore, we have

$$e\left(\frac{4aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}}{4dq}\right) = e\left(\frac{(4a'Q_2(\mathbf{k}') + \mathbf{m} \cdot \mathbf{k}')\overline{2^{\ell+2}}}{dq'}\right)e\left(\frac{(4a''Q_2(\mathbf{k}'') + \mathbf{m} \cdot \mathbf{k}'')\overline{dq'}}{2^{\ell+2}}\right).$$

The sum over a' and \mathbf{k}' gives $S_{d,q'}(\mathbf{m})$ after a change of variables. A similar change of variables in a'' and \mathbf{k}'' gives $S_{1,2^\ell}^\pm(\mathbf{m})$, where the sign is given by $\chi(dq')$. □

In a similar spirit we can prove the following multiplicativity property for the sum (1.2).

LEMMA 10. For $d = d_1d_2$ and $q = q_1q_2$, with $(d_1q_1, d_2q_2) = 1$, we have

$$S_{d,q}(\mathbf{m}) = S_{d_1,q_1}(\mathbf{m})S_{d_2,q_2}(\mathbf{m}).$$

This result reduces the problem of estimating $S_{d,q}(\mathbf{m})$ into three distinct cases. Accordingly, for $d, q \in \mathbb{N}$ we define the sums

$$\mathcal{Q}_q(\mathbf{m}) = S_{1,q}(\mathbf{m}), \quad \mathcal{D}_d(\mathbf{m}) = S_{d,1}(\mathbf{m}), \quad \mathcal{M}_{d,q}(\mathbf{m}) = S_{d,q}(\mathbf{m}),$$

the latter sum only being of interest when d and q exceed 1 and are constructed from the same set of primes. The analysis of these sums will be the focus of §§ 4–6. For the moment we content

ourselves with recording the crude upper bound

$$S_{1,2^\ell}^\pm(\mathbf{m}) \ll 2^{\ell(n/2+1)}, \tag{3.4}$$

for (3.3), whose truth will be established in the following section.

We close this section by presenting some facts concerning the exponential integral $I_{d,q}(\mathbf{m})$ which appears in Lemma 8, recalling the definition (3.1) of $W_{d,T}(\mathbf{y})$. The properties of h recorded in Lemma 7 ensure that $q \ll Q$ when $I_{d,q}(\mathbf{m})$ is non-zero. Likewise the properties of $W_{d,T}$ imply that $d \ll B$ under the same hypothesis. The underlying weight function W has bounded derivatives

$$\frac{\partial^{i_1+\dots+i_n}}{\partial y_1^{i_1} \dots \partial y_n^{i_n}} W(\mathbf{y}) \ll_{i_1, \dots, i_n} 1,$$

and the function V_T satisfies $t^j V_T^{(j)}(t) \ll_j 1$. It therefore follows that

$$\frac{\partial^{i_1+\dots+i_n}}{\partial y_1^{i_1} \dots \partial y_n^{i_n}} W_{d,T}(\mathbf{y}) \ll_{i_1, \dots, i_n} 1,$$

since $Q_1(\mathbf{y})$ has order of magnitude 1, uniformly for $\mathbf{y} \in \text{supp}(W)$.

In the notation of [Hea96, § 7] we have

$$I_{d,q}(\mathbf{m}) = I_r^*(\mathbf{v}) = \int_{\mathbb{R}^n} h(r, G(\mathbf{y})) \omega(\mathbf{y}) e_r(-\mathbf{v} \cdot \mathbf{y}) \, d\mathbf{y}, \tag{3.5}$$

where

$$r = \frac{q}{Q}, \quad \mathbf{v} = \frac{B\mathbf{m}}{4dQ}, \quad G(\mathbf{y}) = \frac{B^2 Q_2(\mathbf{y})}{dQ^2} = Q_2(\mathbf{y}), \quad \omega(\mathbf{y}) = W_{d,T}(\mathbf{y}).$$

We have

$$\frac{\partial^{i_1+\dots+i_n}}{\partial y_1^{i_1} \dots \partial y_n^{i_n}} G(\mathbf{y}) \ll_{i_1, \dots, i_n} 1, \quad \frac{\partial^{i_1+\dots+i_n}}{\partial y_1^{i_1} \dots \partial y_n^{i_n}} \omega(\mathbf{y}) \ll_{i_1, \dots, i_n} 1.$$

Using these bounds and integration by parts, as in [Hea96, § 7], we obtain the following bound.

LEMMA 11. For $\mathbf{m} \neq \mathbf{0}$ and any $N \geq 0$, we have

$$I_{d,q}(\mathbf{m}) \ll_N \frac{Q}{q} \left(\frac{dQ}{B|\mathbf{m}|} \right)^N.$$

As a consequence we get that \mathbf{m} with $|\mathbf{m}| > dQB^{-1+\varepsilon}$ will make a negligible contribution in our analysis of $S_{T,\mathbf{a}}^\sharp(B)$. For \mathbf{m} with $0 < |\mathbf{m}| \leq dQB^{-1+\varepsilon}$ a more refined bound is required. The following result is due to Heath-Brown [Hea96, Lemma 22] and is based on a close study of the function $h(x, y)$.

LEMMA 12. For $i \in \{0, 1\}$, $0 < |\mathbf{m}| \leq dQB^{-1+\varepsilon} = \sqrt{d}B^\varepsilon$ and $q \ll Q = B/\sqrt{d}$, we have

$$\frac{\partial^i}{\partial q^i} I_{d,q}(\mathbf{m}) \ll q^{-i} \left| \frac{B\mathbf{m}}{dq} \right|^{1-n/2} B^\varepsilon.$$

4. Analysis of $\mathcal{Q}_q(\mathbf{m})$

The aim of this section is to collect together everything we need to know about the sums

$$\mathcal{Q}_q(\mathbf{m}) = \sum_{a \pmod q}^* \sum_{\mathbf{k} \pmod q} e_q(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}),$$

for given $\mathbf{m} \in \mathbb{Z}^n$. This sum appears very naturally when the circle method is employed to analyse quadratic forms. Let \mathbf{M} be the underlying symmetric $n \times n$ integer matrix for a quadratic form Q , so that $Q(\mathbf{k}) = \mathbf{k}^T \mathbf{M} \mathbf{k}$. We begin with an easy upper bound for the inner sum in $\mathcal{Q}_q(\mathbf{m})$ when q is a prime power.

LEMMA 13. For any quadratic form $Q(\mathbf{x}) = \mathbf{x}^T \mathbf{M} \mathbf{x}$, we have

$$\left| \sum_{\mathbf{k} \pmod{p^r}} e_{p^r}(Q(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}) \right| \leq p^{nr/2} \sqrt{K_{p^r}(2\mathbf{M}; \mathbf{0})},$$

in the notation of (2.1).

Proof. Cauchy’s inequality implies that the square of the left-hand side is not greater than

$$\sum_{\mathbf{x}, \mathbf{y} \pmod{p^r}} e_{p^r}((Q(\mathbf{x}) - Q(\mathbf{y})) + \mathbf{m} \cdot (\mathbf{x} - \mathbf{y})).$$

Substituting $\mathbf{x} = \mathbf{y} + \mathbf{z}$ we see that the summand is equal to $e_{p^r}(\mathbf{m} \cdot \mathbf{z})e_{p^r}(Q(\mathbf{z}) + 2\mathbf{y}^T \mathbf{M} \mathbf{z})$. The sum over \mathbf{y} vanishes unless $p^r \mid 2\mathbf{M} \mathbf{z}$, in which case it is given by $p^{nr}e_{p^r}(Q(\mathbf{z}))$. The result now follows by executing the sum over \mathbf{z} trivially. \square

We apply Lemma 13 to estimate $\mathcal{Q}_q(\mathbf{m})$. Since Q_2 is non-singular it follows from Lemma 1 that there is an absolute constant $c \geq 1$ such that $K_{p^r}(2\mathbf{M}_2; \mathbf{0}) \leq c$, for any prime power p^r . Moreover one can take $c = 1$ when $p \nmid 2 \det \mathbf{M}_2$. On summing trivially over a one deduces that $|\mathcal{Q}_{p^r}(\mathbf{m})| \leq \sqrt{c} p^{(n/2+1)r}$, for any prime power p^r . Applying Lemma 10 therefore yields

$$\mathcal{Q}_q(\mathbf{m}) \ll q^{n/2+1}. \tag{4.1}$$

Likewise (3.4) is an easy consequence of Lemmas 1 and 13 when $p = 2$.

Using quadratic Gauss sums, it is possible to prove explicit formulae for $\mathcal{Q}_{p^r}(\mathbf{m})$ when the prime p is large enough. The oscillation in the sign of these sums will give cancellation in the sum over q in Lemma 8 which will be crucial for handling $n = 7$. Let $Q(\mathbf{x})$ be a quadratic form with associated matrix \mathbf{M} . We write $Q^*(\mathbf{x})$ for the adjoint quadratic form with underlying matrix $(\det \mathbf{M})\mathbf{M}^{-1}$. For any odd prime p let

$$\varepsilon(p) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ i & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

and let $\chi_p(\cdot)$ denote the Legendre symbol (\cdot/p) . We may now record the following formula.

LEMMA 14. Let p be a prime with $p \nmid 2 \det \mathbf{M}$. Then we have

$$\sum_{\mathbf{k} \pmod{p^r}} e_{p^r}(Q(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}) = \begin{cases} p^{nr/2} e_{p^r}(-\overline{-4 \det \mathbf{M} Q^*(\mathbf{m})}) & \text{if } r \text{ is even,} \\ p^{nr/2} \chi_p(\det \mathbf{M}) \varepsilon(p)^n e_{p^r}(-4 \det \mathbf{M} Q^*(\mathbf{m})) & \text{if } r \text{ is odd.} \end{cases}$$

Proof. Since p is odd there exists an $n \times n$ matrix \mathbf{U} with integer entries and $p \nmid \det \mathbf{U}$ such that $\mathbf{U}^T \mathbf{M} \mathbf{U}$ is diagonal modulo p^r . Hence in proving the lemma we may restrict ourselves to diagonal forms $Q(\mathbf{x}) = \alpha_1 x_1^2 + \dots + \alpha_n x_n^2$, with $\mathbf{M} = \text{diag}(\alpha_1, \dots, \alpha_n)$. In this case we have

$$Q^*(\mathbf{x}) = \det \mathbf{M} \left(\frac{x_1^2}{\alpha_1} + \dots + \frac{x_n^2}{\alpha_n} \right),$$

where $\det \mathbf{M} = \alpha_1 \dots \alpha_n$.

Let S denote the sum appearing on the left-hand side in the statement of the lemma. Then

$$S = \prod_{i=1}^n \left\{ \sum_{k \pmod{p^r}} e_{p^r}(\alpha_i k^2 + m_i k) \right\}.$$

Since $p \nmid 2\alpha_i$, we can complete the square. This yields

$$\sum_{k \pmod{p^r}} e_{p^r}(\alpha_i k^2 + m_i k) = e_{p^r}(-4\overline{\alpha_i m_i^2}) \sum_{k \pmod{p^r}} e_{p^r}(\alpha_i k^2).$$

The last sum is the quadratic Gauss sum, which satisfies

$$\sum_{k \pmod{p^r}} e_{p^r}(\alpha_i k^2) = \begin{cases} p^{r/2} & \text{if } r \text{ is even,} \\ \chi_p(\alpha_i) \varepsilon(p) p^{r/2} & \text{if } r \text{ is odd.} \end{cases}$$

The lemma follows on substituting this into the above expression for S . □

Lemma 14 directly yields an explicit evaluation of the sum $\mathcal{Q}_{p^r}(\mathbf{m})$ when the prime p is sufficiently large. To state the outcome of this let

$$c_{p^r}(a) = \sum_{x \pmod{p^r}}^* e_{p^r}(ax) = \sum_{d|(p^r, a)} d\mu\left(\frac{p^r}{d}\right)$$

be the Ramanujan sum and let

$$g_{p^r}(a) = \sum_{x \pmod{p^r}} \chi_p(x) e_{p^r}(ax)$$

be the Gauss sum. For the former we will make frequent use of the fact that $c_{p^r}(ab) = c_{p^r}(a)$ for any b coprime to p , and $c_{p^r}(a_1) = c_{p^r}(a_2)$ whenever $a_1 \equiv a_2 \pmod{p^r}$. Moreover, we have the obvious inequality $|c_{p^r}(a)| \leq (p^r, a)$.

It follows from Lemma 14 that

$$\mathcal{Q}_{p^r}(\mathbf{m}) = p^{nr/2} \sum_{a \pmod{p^r}}^* \begin{cases} e_{p^r}(-4a \det \mathbf{M}_2 Q_2^*(\mathbf{m})) & \text{if } r \text{ is even,} \\ \chi_p(\det \mathbf{M}_2) \chi_p(a)^n \varepsilon(p)^n e_{p^r}(-4a \det \mathbf{M}_2 Q_2^*(\mathbf{m})) & \text{if } r \text{ is odd,} \end{cases}$$

if $p \nmid 2 \det \mathbf{M}$. The following lemma now follows from executing the sum over a .

LEMMA 15. *Let p be a prime with $p \nmid 2 \det \mathbf{M}_2$. Then for even n we have*

$$\mathcal{Q}_{p^r}(\mathbf{m}) = \varepsilon(p)^{nr} \chi_p(\det \mathbf{M}_2)^r p^{nr/2} c_{p^r}(Q_2^*(\mathbf{m})).$$

For odd n we have

$$\mathcal{Q}_{p^r}(\mathbf{m}) = \begin{cases} p^{nr/2} c_{p^r}(Q_2^*(\mathbf{m})) & \text{if } r \text{ is even,} \\ \varepsilon(p)^n \chi_p(-1) p^{nr/2} g_{p^r}(Q_2^*(\mathbf{m})) & \text{if } r \text{ is odd.} \end{cases}$$

Let

$$N = \begin{cases} 2Q_2^*(\mathbf{m}) \det \mathbf{M}_2 & \text{if } Q_2^*(\mathbf{m}) \neq 0, \\ 2 \det \mathbf{M}_2 & \text{otherwise.} \end{cases} \tag{4.2}$$

We now turn to the average order of $\mathcal{Q}_q(\mathbf{m})$, as one sums over q coprime to M for some fixed $M \in \mathbb{N}$ divisible by N . For this we will use Perron’s formula unless n is even and $Q_2^*(\mathbf{m}) \neq 0$, a case that can be handled trivially as follows.

LEMMA 16. Let $M \in \mathbb{N}$ with $N \mid M$. Assume that n is even and $Q_2^*(\mathbf{m}) \neq 0$. Then we have

$$\sum_{\substack{q \leq x \\ (q,M)=1}} |\mathcal{Q}_q(\mathbf{m})| \leq x^{n/2+1}.$$

Proof. Combining Lemma 15 with the multiplicativity relation Lemma 10 we obtain

$$\sum_{\substack{q \leq x \\ (q,M)=1}} |\mathcal{Q}_q(\mathbf{m})| \leq x^{n/2} \sum_{\substack{q \leq x \\ (q,M)=1}} |c_q(Q_2^*(\mathbf{m}))|.$$

The lemma follows on noting that $|c_q(Q_2^*(\mathbf{m}))| \leq (q, Q_2^*(\mathbf{m})) = 1$. □

Let χ be a non-principal Dirichlet character with conductor c_χ . It will be convenient to recall some preliminary facts concerning the size of Dirichlet L -functions $L(s, \chi)$ in the critical strip. We begin by recalling the convexity bound

$$L(\sigma + it, \chi) \ll \{c_\chi(|t| + 1)\}^{(1-\sigma)/2+\varepsilon}, \tag{4.3}$$

for any $\sigma \in [0, 1]$. Next we claim that

$$\int_{1/2-iT}^{1/2+iT} |L(s, \chi)|^2 \frac{ds}{|s|} \ll c_\chi^{7/16+\varepsilon} T^\varepsilon. \tag{4.4}$$

For this we break the integral into dyadic blocks, deducing that it is dominated by

$$\sum_{\substack{Y \text{ dyadic} \\ 0 < Y \leq T}} \frac{1}{1+Y} \int_Y^{2Y} \left| L\left(\frac{1}{2} + it, \chi\right) \right|^2 dt.$$

For $Y \leq c_\chi^{1/8}$ we use Heath-Brown’s [Hea80] hybrid bound $L(\frac{1}{2} + it, \chi) \ll \{c_\chi(|t| + 1)\}^{3/16+\varepsilon}$, to get

$$\frac{1}{1+Y} \int_Y^{2Y} \left| L\left(\frac{1}{2} + it, \chi\right) \right|^2 dt \ll c_\chi^{3/8+\varepsilon} \sqrt{Y} \ll c_\chi^{7/16+\varepsilon}.$$

For $Y > c_\chi^{1/8}$ we use the approximate functional equation to replace the L -value by a series of length $\sqrt{c_\chi Y}$, and then use the mean value theorem for Dirichlet polynomials (see Iwaniec and Kowalski [IK04, Theorem 9.1], for example). This gives

$$\frac{1}{1+Y} \int_Y^{2Y} \left| \sum_{n \leq \sqrt{c_\chi Y T^\varepsilon}} \frac{\chi(n)}{\sqrt{n}} n^{-it} \right|^2 dt \ll \left(1 + \sqrt{\frac{c_\chi}{Y}}\right) T^\varepsilon \log c_\chi \ll c_\chi^{7/16+\varepsilon} T^\varepsilon.$$

Summing over all dyadic blocks, and redefining the choice of ε , we arrive at (4.4).

For $s \in \mathbb{C}$ let $\sigma = \Re(s)$. Returning now to the application of Perron’s formula, we set

$$\xi_M(s; \mathbf{m}) = \sum_{(q,M)=1} \frac{\mathcal{Q}_q(\mathbf{m})}{q^s}.$$

By (4.1) this series is absolutely convergent for $\sigma > n/2 + 2$. When n is even and $Q_2^*(\mathbf{m}) \neq 0$ it is absolutely convergent for $\sigma > n/2 + 1$, by Lemma 16. For any $x - 1/2 \in \mathbb{Z}$ and $T > 0$ we obtain

$$\sum_{\substack{q \leq x \\ (q,M)=1}} \mathcal{Q}_q(\mathbf{m}) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \xi_M(s; \mathbf{m}) x^s \frac{ds}{s} + O\left(\frac{x^c}{T}\right), \tag{4.5}$$

where $c > n/2 + 2$. We will take T large enough in terms of x and $|\mathbf{m}|$ so that the error term in the formula is negligible. The analytic nature of the L -series can be revealed using the explicit formulae that we enunciated in Lemma 15 and depends on the parity of n . For even n we get

$$\xi_M(s; \mathbf{m}) = \prod_{p \nmid M} \left\{ \sum_{r=0}^{\infty} \frac{\chi_p(\det \mathbf{M}_2)^r \varepsilon(p)^{nr} c_{p^r}(Q_2^*(\mathbf{m}))}{p^{(s-n/2)r}} \right\}. \tag{4.6}$$

For odd n we get

$$\xi_M(s; \mathbf{m}) = \prod_{p \nmid M} \left\{ \sum_{r \text{ even}} \frac{c_{p^r}(Q_2^*(\mathbf{m}))}{p^{(s-n/2)r}} + \chi_p(-1)\varepsilon(p)^n \sum_{r \text{ odd}} \frac{g_{p^r}(Q_2^*(\mathbf{m}))}{p^{(s-n/2)r}} \right\}. \tag{4.7}$$

The following result handles the case in which $Q_2^*(\mathbf{m}) = 0$.

LEMMA 17. *Let $M \in \mathbb{N}$ with $N \mid M$ and let $\varepsilon > 0$. Assume that $Q_2^*(\mathbf{m}) = 0$. Then we have*

$$\sum_{\substack{q \leq x \\ (q, M) = 1}} \mathcal{Q}_q(\mathbf{m}) \ll \begin{cases} x^{(n+3)/2+\varepsilon} M^\varepsilon & \text{if } (-1)^{n/2} \det \mathbf{M}_2 \neq \square, \\ x^{n/2+2} & \text{if } (-1)^{n/2} \det \mathbf{M}_2 = \square. \end{cases}$$

Here, and after, for any complex number z we write $z = \square$ if and only if there exists an integer j such that $z = j^2$. Thus the sum in question is bounded by $O(x^{(n+3)/2+\varepsilon} M^\varepsilon)$ when n is odd since it is then impossible for $(-1)^{n/2} \det \mathbf{M}_2$ to be the square of an integer.

Proof of Lemma 17. The second part of the lemma is a trivial consequence of (4.1) and the triangle inequality. Turning to the first part we begin by supposing that n is even and $(-1)^{n/2} \det \mathbf{M}_2 \neq \square$. If $Q_2^*(\mathbf{m}) = 0$, then $c_{p^r}(Q_2^*(\mathbf{m})) = \varphi(p^r)$. It follows from (4.6) that

$$\xi_M(s; \mathbf{m}) = L\left(s - 1 - \frac{n}{2}, \psi\right) E_M(s),$$

where $L(s, \psi)$ is the Dirichlet L -function associated to the Jacobi symbol

$$\psi(\cdot) = \left(\frac{(-1)^{n/2} \det \mathbf{M}_2}{\cdot} \right),$$

with conductor $c_\psi = O(1)$, and where $E_M(s)$ is an Euler product which converges absolutely in the half-plane $\sigma > n/2 + 1$ and satisfies the bound $E_M(s) \ll M^\varepsilon$ on any fixed half-plane $\sigma \geq n/2 + 1 + \eta$, with $\eta > 0$. This gives the analytic continuation of $\xi_M(s; \mathbf{m})$ up to $\sigma > n/2 + 1$.

Moving the contour of integration in (4.5) to $c_0 = (n + 3)/2$ and invoking the convexity estimate (4.3) to deal with the horizontal contours, we obtain

$$\sum_{\substack{q \leq x \\ (q, M) = 1}} \mathcal{Q}_q(\mathbf{m}) = \frac{1}{2\pi i} \int_{c_0 - iT}^{c_0 + iT} \xi_M(s; \mathbf{m}) x^s \frac{ds}{s} + O\left(\frac{x^c}{T} + \frac{x^{c_0} M^\varepsilon T^\varepsilon}{T^{3/4}}\right).$$

Here we note that $(-1)^{n/2} \det \mathbf{M}_2$ is not a square and so the L -series does not have a pole in the region $\sigma > c_0 - 1/2$. Taking $T = x^{n+4}$ the error term is seen to be $O(x^{-n/4-3/2+\varepsilon} M^\varepsilon)$. The remaining integral is estimated via (4.4), which thereby leads to the first part of Lemma 17 when n is even.

If n is odd and $Q_2^*(\mathbf{m}) = 0$, then $c_{p^r}(Q_2^*(\mathbf{m})) = \varphi(p^r)$ and $g_{p^r}(Q_2^*(\mathbf{m})) = 0$. Hence $\xi_M(s; \mathbf{m})$ is absolutely convergent and bounded by $O(M^\varepsilon)$ in any fixed half-plane $\sigma \geq (n + 3)/2 + \eta$, with $\eta > 0$. This implies that we can shift the contour in (4.5) to $c_0 = (n + 3)/2 + \varepsilon$, without

encountering any poles, leading to a similar but simpler situation to that considered for even n . This completes the proof of Lemma 17. \square

Let us turn to the size of the exponential sums $\mathcal{Q}_q(\mathbf{m})$ for generic \mathbf{m} , for which sharper bounds are required. Tracing through the proof one sees that if n is even and $Q_2^*(\mathbf{m}) \neq 0$, then one is instead led to compare $\xi_M(s; \mathbf{m})$ in (4.6) with $L(s - n/2, \psi)^{-1}$. To improve on Lemma 16 one therefore requires a good zero-free region for $L(s - n/2, \psi)$ to the left of the line $\sigma = n/2 + 1$, for which the unconditional picture is somewhat lacking. However, even if one is able to save a power of x in Lemma 16, this still does not seem to be enough to handle $n = 6$ in Theorem 1. The following result deals with the case of odd n when $Q_2^*(\mathbf{m}) \neq 0$.

LEMMA 18. *Let $M \in \mathbb{N}$ with $N \mid M$ and let $\varepsilon > 0$. Assume that n is odd and $Q_2^*(\mathbf{m}) \neq 0$. Then we have*

$$\sum_{\substack{q \leq x \\ (q, M) = 1}} \mathcal{Q}_q(\mathbf{m}) \ll \begin{cases} |\mathbf{m}|^{7/16 + \varepsilon} x^{n/2 + 1 + \varepsilon} M^\varepsilon, & \text{if } (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) \neq \square, \\ x^{(n+3)/2 + \varepsilon} M^\varepsilon, & \text{if } (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) = \square. \end{cases}$$

Proof. Recalling (4.7) we note that $g_p(a) = \chi_p(a)\varepsilon(p)p^{1/2}$, for any non-zero integer a that is coprime to p . Hence we deduce in this case that

$$\xi_M(s; \mathbf{m}) = L\left(s - \frac{n+1}{2}, \psi_{\mathbf{m}}\right) E_M(s),$$

where $\psi_{\mathbf{m}}$ is the Jacobi symbol

$$\psi_{\mathbf{m}}(\cdot) = \left(\frac{(-1)^{(n-1)/2} Q_2^*(\mathbf{m})}{\cdot}\right),$$

with conductor $4|Q_2^*(\mathbf{m})| = O(|\mathbf{m}|^2)$. Also $E_M(s)$ is an Euler product which now converges absolutely for $\sigma > n/2 + 1$ and satisfies the bound $E_M(s) \ll M^\varepsilon$ on any fixed half-plane $\sigma \geq n/2 + 1 + \eta$, with $\eta > 0$. Under the assumption that $(-1)^{(n-1)/2} Q_2^*(\mathbf{m}) \neq \square$, the L -series $\xi_M(s; \mathbf{m})$ does not have a pole in the region $\sigma > n/2 + 1$. Moving the contour of integration in (4.5) to $c_0 = n/2 + 1 + \varepsilon$, and using the convexity estimate (4.3), we therefore get

$$\sum_{\substack{q \leq x \\ (q, M) = 1}} \mathcal{Q}_q(\mathbf{m}) = \frac{1}{2\pi i} \int_{c_0 - iT}^{c_0 + iT} \xi_M(s; \mathbf{m}) x^s \frac{ds}{s} + O\left(\frac{x^c}{T} + \frac{|\mathbf{m}|^{1/2 + \varepsilon} x^{c_0} M^\varepsilon}{T^{3/4}}\right),$$

in this case. Estimating the remaining integral using (4.4), as before, we conclude the proof of the lemma when $(-1)^{(n-1)/2} Q_2^*(\mathbf{m}) \neq \square$ by taking T sufficiently large.

Finally, if $(-1)^{(n-1)/2} Q_2^*(\mathbf{m}) = \square$, then $\xi_M(s; \mathbf{m})$ is regularised by $\zeta(s - (n+1)/2)$ and has a pole at $s = (n+3)/2$. In this case we move the line of integration back to $c_0 = (n+3)/2 + \varepsilon$, which easily leads to the statement of the lemma. \square

5. Analysis of $\mathcal{D}_d(\mathbf{m})$

The aim of this section is to collect together everything we need to know about the sums

$$\mathcal{D}_d(\mathbf{m}) = \sum_{\mathbf{k} \in \hat{W}(\mathbb{Z}/d\mathbb{Z})} e_d(\mathbf{m} \cdot \mathbf{k}),$$

for given $\mathbf{m} \in \mathbb{Z}^n$ and $d \in \mathbb{N}$. Here we write \hat{W} to denote the affine cone above a projective variety W . The estimates in this section pertain to the quadratic forms considered in Theorem 1,

so that V is non-singular and we may make use of the geometric facts recorded in §2.2. Our starting point is Lemma 10, which yields $\mathcal{D}_{d_1 d_2}(\mathbf{m}) = \mathcal{D}_{d_1}(\mathbf{m})\mathcal{D}_{d_2}(\mathbf{m})$ if $(d_1, d_2) = 1$, rendering it sufficient to understand the behaviour of the sum at prime powers.

For any $\mathbf{m} \in \mathbb{Z}^n$ we begin by examining the case in which $d = p$, a prime. Introducing a free sum over elements of \mathbb{F}_p^* , we find that

$$\begin{aligned} (p - 1)\mathcal{D}_p(\mathbf{m}) &= \sum_{a=1}^{p-1} \sum_{\mathbf{x} \in \hat{V}(\mathbb{F}_p)} e_p(\mathbf{m} \cdot \mathbf{x}) \\ &= \sum_{\mathbf{x} \in \hat{V}(\mathbb{F}_p)} \sum_{a=1}^{p-1} e_p(a\mathbf{m} \cdot \mathbf{x}) \\ &= p\#\hat{V}_{\mathbf{m}}(\mathbb{F}_p) - \#\hat{V}(\mathbb{F}_p), \end{aligned}$$

where $V_{\mathbf{m}}$ is the variety obtained by intersecting V with the hyperplane $\mathbf{m} \cdot \mathbf{x} = 0$, and $\hat{V}_{\mathbf{m}}$ is the corresponding affine variety lying above it. Rearranging, we obtain

$$\mathcal{D}_p(\mathbf{m}) = \left(1 - \frac{1}{p}\right)^{-1} (\#\hat{V}_{\mathbf{m}}(\mathbb{F}_p) - p^{-1}\#\hat{V}(\mathbb{F}_p)). \tag{5.1}$$

Now for any complete intersection $W \subset \mathbb{P}^m$, which is non-singular modulo p and has dimension $e \geq 1$, it follows from Deligne’s resolution of the Weil conjectures [Del74] that

$$|\#W(\mathbb{F}_p) - (p^e + p^{e-1} + \dots + 1)| = O_{d,m}(p^{e/2}),$$

where d is the degree of W . In particular, since

$$\#W(\mathbb{F}_p) = \frac{\#\hat{W}(\mathbb{F}_p) - 1}{p - 1},$$

we deduce that

$$\#\hat{W}(\mathbb{F}_p) = p^{e+1} + O_{d,m}(p^{(e+2)/2}). \tag{5.2}$$

In our setting we have $e = n - 3$ for V and $e = n - 4$ for $V_{\mathbf{m}}$ if $p \nmid \mathbf{m}$. We may now record the following inequalities.

LEMMA 19. *We have*

$$\mathcal{D}_p(\mathbf{m}) \ll \begin{cases} p^{(n-2)/2} & \text{if } p \nmid G(\mathbf{m}), \\ p^{(n-1)/2} & \text{if } p \mid G(\mathbf{m}) \text{ and } p \nmid \mathbf{m}, \\ p^{n-2} & \text{if } p \mid \mathbf{m}. \end{cases}$$

Proof. We may assume that $p \nmid \Delta_V$, since otherwise the result is trivial. Our starting point is (5.1). If $p \mid \mathbf{m}$, then $\mathcal{D}_p(\mathbf{m}) = \#\hat{V}(\mathbb{F}_p)$ and the claim follows from (5.2).

If $p \nmid G(\mathbf{m})$, so that $V_{\mathbf{m}}$ is non-singular modulo p , then an application of (5.2) yields

$$\mathcal{D}_p(\mathbf{m}) = \left(1 - \frac{1}{p}\right)^{-1} (p^{n-3} + O(p^{(n-2)/2}) - p^{-1}(p^{n-2} + O(p^{(n-1)/2}))) = O(p^{(n-2)/2}),$$

if $n \geq 5$. When $n = 4$ this is trivial since then $\#V_{\mathbf{m}}(\mathbb{F}_p) = O(1)$. This establishes the claim.

Finally, if $p \mid G(\mathbf{m})$ and $p \nmid \mathbf{m}$, then $V_{\mathbf{m}}$ is singular and of codimension 1 in V modulo p . By a result of Zak (see [Hoo91, Appendix, Theorem 2]), the singular locus of $V_{\mathbf{m}}$ has projective dimension 0. Hence the work of Hooley [Hoo91] yields $\#\hat{V}_{\mathbf{m}}(\mathbb{F}_p) = p^{n-3} + O(p^{(n-1)/2})$, which once inserted into (5.1) yields the desired inequality. \square

We now turn our attention to higher prime powers. Let $d = p^r$ for $r \geq 2$ and suppose that $G(\mathbf{m}) \neq 0$. We assume that $p \nmid \Delta_V$ and $p \nmid \mathbf{m}$. Then it is easy to see that

$$\mathcal{D}_{p^r}(\mathbf{m}) = \sum_{\substack{\mathbf{x} \in \hat{V}(\mathbb{Z}/p^r\mathbb{Z}) \\ p \nmid \mathbf{x}}} e_{p^r}(\mathbf{m} \cdot \mathbf{x}).$$

Mimicking the argument leading to (5.1), a line of attack that we have already met in the proof of Lemma 2, we deduce from the explicit formula for the Ramanujan sum that

$$\varphi(p^r)\mathcal{D}_{p^r}(\mathbf{m}) = \sum_{a \pmod{p^r}}^* \sum_{\substack{\mathbf{x} \in \hat{V}(\mathbb{Z}/p^r\mathbb{Z}) \\ p \nmid \mathbf{x}}} e_{p^r}(a\mathbf{m} \cdot \mathbf{x}) = p^r \sum_{\substack{\mathbf{x} \in \hat{V}(\mathbb{Z}/p^r\mathbb{Z}) \\ p^r \mid \mathbf{m} \cdot \mathbf{x} \\ p \nmid \mathbf{x}}} 1 - p^{r-1} \sum_{\substack{\mathbf{x} \in \hat{V}(\mathbb{Z}/p^r\mathbb{Z}) \\ p^{r-1} \mid \mathbf{m} \cdot \mathbf{x} \\ p \nmid \mathbf{x}}} 1.$$

In the second sum we write $\mathbf{x} = \mathbf{y} + p^{r-1}\mathbf{z}$ with $\mathbf{y} \pmod{p^{r-1}}$ and $\mathbf{z} \pmod{p}$, to get

$$\sum_{\substack{\mathbf{x} \in \hat{V}(\mathbb{Z}/p^r\mathbb{Z}) \\ p^{r-1} \mid \mathbf{m} \cdot \mathbf{x} \\ p \nmid \mathbf{x}}} 1 = \sum_{\substack{\mathbf{y} \in \hat{V}(\mathbb{Z}/p^{r-1}\mathbb{Z}) \\ p^{r-1} \mid \mathbf{m} \cdot \mathbf{y} \\ p \nmid \mathbf{y}}} \#\{\mathbf{z} : Q_i(\mathbf{y} + p^{r-1}\mathbf{z}) \equiv 0 \pmod{p^r}, \text{ for } i = 1, 2\}.$$

Since $p \nmid \Delta_V$, the count for the number $\mathbf{z} \pmod{p}$ is given by p^{n-2} . Setting

$$N(p^j, \mathbf{m}) = \#\{\mathbf{x} \in \hat{V}(\mathbb{Z}/p^j\mathbb{Z}) : p \nmid \mathbf{x}, \mathbf{m} \cdot \mathbf{x} \equiv 0 \pmod{p^j}\},$$

we get

$$\mathcal{D}_{p^r}(\mathbf{m}) = \frac{p^r}{\varphi(p^r)} \{N(p^r, \mathbf{m}) - p^{n-3}N(p^{r-1}, \mathbf{m})\}.$$

In particular, an application of Hensel’s lemma yields the following conclusion.

LEMMA 20. *Let $r \geq 2$. Then we have $\mathcal{D}_{p^r}(\mathbf{m}) = 0$ unless $p \mid \Delta_V G(\mathbf{m})$.*

We also require a general bound for $\mathcal{D}_d(\mathbf{m})$. By the orthogonality of characters we may write

$$\mathcal{D}_d(\mathbf{m}) = \frac{1}{d^2} \sum_{\mathbf{b} \pmod{d}} \mathcal{D}_d(\mathbf{m}; \mathbf{b}),$$

where

$$\mathcal{D}_d(\mathbf{m}; \mathbf{b}) = \sum_{\mathbf{k} \pmod{d}} e_d(b_1Q_1(\mathbf{k}) + b_2Q_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}).$$

We proceed to extract the greatest common divisor h of \mathbf{b} with d , writing $d = hd'$ and $\mathbf{b} = h\mathbf{b}'$, with $(d', \mathbf{b}') = 1$. Breaking the sum into congruence classes modulo d' we then see that

$$\mathcal{D}_d(\mathbf{m}; \mathbf{b}) = \sum_{\mathbf{k}' \pmod{d'}} \sum_{\mathbf{k}'' \pmod{h}} e_{d'}(b'_1Q_1(\mathbf{k}') + b'_2Q_2(\mathbf{k}') + h^{-1}\mathbf{m} \cdot \mathbf{k}') e_h(\mathbf{m} \cdot \mathbf{k}'').$$

In particular, h must be a divisor of \mathbf{m} , and, furthermore, if we write $\mathbf{m} = h\mathbf{m}'$, then we have $\mathcal{D}_d(\mathbf{m}; \mathbf{b}) = h^n \mathcal{D}_{d'}(\mathbf{m}'; \mathbf{b}')$. Applying Lemma 13, we conclude that

$$|\mathcal{D}_d(\mathbf{m})| \leq \frac{1}{d^2} \sum_{h \mid (d, \mathbf{m})} h^n d'^{n/2} \sum_{\mathbf{b}' \pmod{d'}}^* \sqrt{K_{d'}(2\mathbf{M}(\mathbf{b}'); \mathbf{0})}, \tag{5.3}$$

in the notation of (2.1) and (2.2). The following result provides a good upper bound for the inner sum, provided that d' does not share a common prime factor with Δ_V .

LEMMA 21. For any $\varepsilon > 0$ and $e \in \mathbb{N}$ with $(e, \Delta_V) = 1$, we have

$$\sum_{\mathbf{b} \pmod e}^* K_e(2\mathbf{M}(\mathbf{b}); \mathbf{0}) \ll e^{2+\varepsilon}.$$

Proof. Let $g(e)$ denote the sum that is to be estimated and put $U_e(\mathbf{b}) = K_e(2\mathbf{M}(\mathbf{b}); \mathbf{0})$. One notes via the Chinese remainder theorem that g is a multiplicative arithmetic function which it will therefore suffice to understand at prime powers $e = p^r$, with $p \nmid \Delta_V$. We have

$$g(p^r) = \sum_{\substack{0 \leq b_1, b_2 < p^r \\ p \nmid \mathbf{b}}} U_{p^r}(\mathbf{b}).$$

Viewed as a matrix with coefficients in \mathbb{Z} , it follows from (2.3) that $\mathbf{M}(\mathbf{b})$ has rank n or $n - 1$, and furthermore $P(\mathbf{b}) = \det \mathbf{M}(\mathbf{b})$ has non-zero discriminant, as a polynomial in \mathbf{b} . For $i = 0, 1$ we write \mathcal{B}_i for the set of $\mathbf{b} \in \mathbb{Z}^2$ with $0 \leq b_1, b_2 < p^r$ and $p \nmid \mathbf{b}$, for which $\mathbf{M}(\mathbf{b})$ has rank $n - i$ over \mathbb{Z} .

We will provide two upper bounds for $U_{p^r}(\mathbf{b})$. We begin with Lemma 1, which gives

$$U_{p^r}(\mathbf{b}) \leq p^{r(n-\varrho)+\delta_p}, \tag{5.4}$$

where ϱ is the rank of $2\mathbf{M}(\mathbf{b})$ over \mathbb{Z} and δ_p is the minimum of the p -adic orders of the $\varrho \times \varrho$ non-singular submatrices of $2\mathbf{M}(\mathbf{b})$. Our second estimate for $U_{p^r}(\mathbf{b})$ is based on an analysis of the case $r = 1$. Since $p \nmid \Delta_V$ it follows that $2\mathbf{M}(\mathbf{b})$ has rank n or $n - 1$ modulo p . In the former case one obtains $U_p(\mathbf{b}) = 1$ and in the latter case $U_p(\mathbf{b}) = p$. An application of Hensel’s lemma therefore yields

$$U_{p^r}(\mathbf{b}) \leq \begin{cases} 1 & \text{if } p \nmid \Delta_V \det \mathbf{M}(\mathbf{b}), \\ p^r & \text{if } p \nmid \Delta_V \text{ and } p \mid \det \mathbf{M}(\mathbf{b}). \end{cases} \tag{5.5}$$

Combining (5.4) and (5.5) we deduce that

$$U_{p^r}(\mathbf{b}) \leq \begin{cases} p^{\min\{r, v_p(P(\mathbf{b}))\}} & \text{if } \mathbf{b} \in \mathcal{B}_0, \\ p^r & \text{if } \mathbf{b} \in \mathcal{B}_1. \end{cases}$$

It therefore follows that

$$g(p^r) \leq \sum_{\mathbf{b} \in \mathcal{B}_0} p^{\min\{r, v_p(P(\mathbf{b}))\}} + p^r \#\mathcal{B}_1.$$

Now it is clear that there are only $O(1)$ primitive integer solutions of the equation $P(\mathbf{b}) = 0$, whence $\#\mathcal{B}_1 = O(p^r)$. Moreover we have $v_p(P(\mathbf{b})) \leq \Delta$ with $\Delta = rn + O(1)$, for any $\mathbf{b} \in \mathcal{B}_0$. Our investigation so far has shown that for $p \nmid \Delta_V$ we have

$$g(p^r) \ll p^{2r} + \sum_{\ell=0}^{\Delta} p^{\min\{\ell, r\}} \#\mathcal{B}_0(\ell),$$

where $\mathcal{B}_0(\ell)$ is the set of $\mathbf{b} \in \mathcal{B}_0$ for which $p^\ell \mid P(\mathbf{b})$. If $\ell \leq r$, then

$$\#\mathcal{B}_0(\ell) \ll p^{2(r-\ell)} \#\{\mathbf{b} \pmod{p^\ell} : p \nmid \mathbf{b}, P(\mathbf{b}) \equiv 0 \pmod{p^\ell}\} \ll p^{2r-\ell},$$

since p does not divide the discriminant of P . Alternatively if $\ell > r$, then it follows that

$$\#\mathcal{B}_0(\ell) \ll p^r.$$

Putting this altogether we conclude that

$$g(p^r) \ll p^{2r} + \sum_{0 \leq \ell \leq r} p^{2\ell} + \sum_{r < \ell \leq \Delta} p^{2\ell} \ll rp^{2r},$$

for $p \nmid \Delta_V$. This suffices for the statement of the lemma. □

Applying Lemma 21 in (5.3), we conclude that

$$\mathcal{D}_d(\mathbf{m}) \ll d^{n/2+\varepsilon} (d, \mathbf{m})^{n/2-2},$$

if $(d, \Delta_V) = 1$. If $d \mid \Delta_V^\infty$, we will merely take the trivial bound

$$|\mathcal{D}_d(\mathbf{m})| \leq \varrho(d) \ll d^{n-2+\varepsilon},$$

which follows from Lemma 2. Combining these therefore leads to the following result.

LEMMA 22. *For any $\varepsilon > 0$ we have $\mathcal{D}_d(\mathbf{m}) \ll (d, \Delta_V^\infty)^{n/2-2} d^{n/2+\varepsilon} (d, \mathbf{m})^{n/2-2}$.*

We are now ready to record some estimates for the average order of $|\mathcal{D}_d(\mathbf{m})|$, as we range over appropriate sets of moduli d . Combining Lemma 19 with Lemma 20 and the multiplicativity property in Lemma 10, we are immediately led to the following conclusion.

LEMMA 23. *For any $\varepsilon > 0$ we have*

$$\sum_{\substack{d \leq x \\ (d, \Delta_V G(\mathbf{m}))=1}} |\mathcal{D}_d(\mathbf{m})| \ll x^{n/2+\varepsilon}.$$

Here Lemma 20 ensures that only square-free values of d are counted in this sum. Furthermore this result is trivial if $G(\mathbf{m}) = 0$, in which case we will need an allied estimate. This is provided by the following result.

LEMMA 24. *Assume that $G(\mathbf{m}) = 0$. For any $\varepsilon > 0$ we have*

$$\sum_{\substack{d \leq x \\ (d, \Delta_V \mathbf{m})=1}} |\mathcal{D}_d(\mathbf{m})| \ll x^{(n+1)/2+\varepsilon}.$$

Proof. We make the factorisation $d = uv$, where u is the square-free part of d and v is the square-full part. In particular, both u and v are assumed to be coprime to Δ_V and \mathbf{m} . Then Lemma 19 yields $\mathcal{D}_u(\mathbf{m}) \ll u^{(n-1)/2+\varepsilon}$, and it follows from Lemma 22 that $\mathcal{D}_v(\mathbf{m}) \ll v^{n/2+\varepsilon}$. Hence

$$\begin{aligned} \sum_{\substack{d \leq x \\ (d, \Delta_V \mathbf{m})=1}} |\mathcal{D}_d(\mathbf{m})| &\ll \sum_{uv \leq x} u^{(n-1)/2+\varepsilon} v^{n/2+\varepsilon} \\ &\ll x^{(n+1)/2+\varepsilon} \sum_{v \leq x} \frac{1}{v^{1/2}}. \end{aligned}$$

On noting that the number of square-full integers $v \leq V$ is $O(V^{1/2})$, this therefore concludes the proof of the lemma. □

6. Analysis of $\mathcal{M}_{d,q}(\mathbf{m})$

It remains to estimate the mixed character sums $\mathcal{M}_{d,q}(\mathbf{m})$, which it will suffice to analyse at prime powers. Our goal in this section will be a proof of the following result.

LEMMA 25. Assume that $q \mid d^\infty$ and $d \mid q^\infty$. Let $\varepsilon > 0$ and assume Hypothesis- ρ . Then we have

$$\mathcal{M}_{d,q}(\mathbf{m}) \ll (d, (2 \det \mathbf{M}_2)^\infty)^{n/2-2} d^{n/2+\varepsilon} q^{n/2+1}.$$

Our proof of this result is based on an analysis of the sum

$$\mathcal{M}_{p^r,p^\ell}(\mathbf{m}) = \sum_{a \pmod{p^\ell}}^* \sum_{\substack{\mathbf{k} \pmod{p^{r+\ell}} \\ Q_1(\mathbf{k}) \equiv 0 \pmod{p^r} \\ Q_2(\mathbf{k}) \equiv 0 \pmod{p^r}}} e_{p^{r+\ell}}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}),$$

for integers $r, \ell \geq 1$. We first split the inner sum by replacing \mathbf{k} by $\mathbf{k} + p^r \mathbf{x}$, where \mathbf{k} runs modulo p^r and \mathbf{x} runs modulo p^ℓ . This yields

$$\mathcal{M}_{p^r,p^\ell}(\mathbf{m}) = \sum_{\substack{\mathbf{k} \pmod{p^r} \\ Q_1(\mathbf{k}) \equiv 0 \pmod{p^r} \\ Q_2(\mathbf{k}) \equiv 0 \pmod{p^r}}} S(\mathbf{k}), \tag{6.1}$$

where

$$S(\mathbf{k}) = \sum_{a \pmod{p^\ell}}^* e_{p^{r+\ell}}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}) \sum_{\mathbf{x} \pmod{p^\ell}} e_{p^\ell}(aQ_2(\mathbf{x})p^r + a\nabla Q_2(\mathbf{k}) \cdot \mathbf{x} + \mathbf{m} \cdot \mathbf{x}).$$

We will argue differently according to which of r or ℓ is largest. Recall that Q_2^* is the dual of Q_2 , with matrix $\mathbf{M}_2^* = (\det \mathbf{M}_2)\mathbf{M}_2^{-1}$. Lemma 25 is a straightforward consequence of the following pair of results and the multiplicativity property in Lemma 10.

LEMMA 26. Suppose that $\ell > r$. Then $\mathcal{M}_{p^r,p^\ell}(\mathbf{m}) = 0$ unless $p^r \mid Q_2^*(\mathbf{m})$ or $p \mid 2 \det \mathbf{M}_2$, in which case $\mathcal{M}_{p^r,p^\ell}(\mathbf{m}) \ll p^{\ell+n(\ell+r)/2}$.

Proof. In the inner sum of $S(\mathbf{k})$ we take $\mathbf{x} = \mathbf{y} + p^{\ell-r} \mathbf{z}$, where \mathbf{y} runs modulo $p^{\ell-r}$ and \mathbf{z} runs modulo p^r . This gives

$$\sum_{\mathbf{y} \pmod{p^{\ell-r}}} e_{p^\ell}(aQ_2(\mathbf{y})p^r + a\nabla Q_2(\mathbf{k}) \cdot \mathbf{y} + \mathbf{m} \cdot \mathbf{y}) \sum_{\mathbf{z} \pmod{p^r}} e_{p^r}(a\nabla Q_2(\mathbf{k}) \cdot \mathbf{z} + \mathbf{m} \cdot \mathbf{z}),$$

for the sum over $\mathbf{x} \pmod{p^\ell}$. The sum over \mathbf{z} vanishes unless

$$a\nabla Q_2(\mathbf{k}) + \mathbf{m} \equiv \mathbf{0} \pmod{p^r}. \tag{6.2}$$

Recall from the conditions of summation in (6.1) that $p^r \mid Q_2(\mathbf{k})$. In particular, if $p \nmid 2 \det \mathbf{M}_2$, then it follows that $\mathcal{M}_{p^r,p^\ell}(\mathbf{m}) = 0$ unless $p^r \mid Q_2^*(\mathbf{m})$, as required for the first part of the lemma. For the second part, we let $\mathbf{v} \in \mathbb{Z}^n$ be such that $a\nabla Q_2(\mathbf{k}) + \mathbf{m} = p^r \mathbf{v}$. Then we have

$$S(\mathbf{k}) = p^{nr} \sum_{a \in A(\mathbf{k})} e_{p^{r+\ell}}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}) \sum_{\mathbf{y} \pmod{p^{\ell-r}}} e_{p^{\ell-r}}(aQ_2(\mathbf{y}) + \mathbf{v} \cdot \mathbf{y}),$$

where $A(\mathbf{k})$ denotes the set of $a \in (\mathbb{Z}/p^\ell\mathbb{Z})^*$ such that (6.2) holds. Applying Lemma 13 and then Lemma 1 we conclude that

$$|S(\mathbf{k})| \leq \sum_{a \in A(\mathbf{k})} p^{nr+n(\ell-r)/2} \sqrt{K_{p^{\ell-r}}(2\mathbf{M}_2; \mathbf{0})} \ll \sum_{a \in A(\mathbf{k})} p^{nr+n(\ell-r)/2}.$$

Inserting this into (6.1) therefore gives

$$\mathcal{M}_{p^r,p^\ell}(\mathbf{m}) \ll p^{n(\ell+r)/2} \sum_{a \pmod{p^\ell}}^* K_{p^r}(2a\mathbf{M}_2; -\mathbf{m}).$$

A further application of Lemma 1 therefore gives the bound in the lemma. □

LEMMA 27. Suppose that $\ell \leq r$ and assume Hypothesis- ϱ . Then $\mathcal{M}_{p^r, p^\ell}(\mathbf{m}) = 0$ unless $p^\ell \mid Q_2^*(\mathbf{m})$ or $p \mid 2 \det \mathbf{M}_2$, in which case $\mathcal{M}_{p^r, p^\ell}(\mathbf{m}) \ll p^{\ell+n(\ell+r)/2} (p, 2 \det \mathbf{M}_2)^{nr/2-2r+\varepsilon}$.

Note that when $p \mid 2 \det \mathbf{M}_2$ in Lemma 27, so that p is bounded absolutely, the bound for $\mathcal{M}_{p^r, p^\ell}(\mathbf{m})$ is $O(p^{(n/2+1)\ell+(n-2)r+\varepsilon})$, which grows like C^r for an absolute constant $C > 0$.

Proof of Lemma 27. The expression in (6.1) now features

$$S(\mathbf{k}) = \sum_{a \pmod{p^\ell}}^* e_{p^{r+\ell}}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}) \sum_{\mathbf{x} \pmod{p^\ell}} e_{p^\ell}(a\nabla Q_2(\mathbf{k}) \cdot \mathbf{x} + \mathbf{m} \cdot \mathbf{x}).$$

The sum over \mathbf{x} vanishes unless

$$a\nabla Q_2(\mathbf{k}) + \mathbf{m} \equiv \mathbf{0} \pmod{p^\ell}. \tag{6.3}$$

Recall that $p^r \mid Q_2(\mathbf{k})$ in (6.1), which implies that $p^\ell \mid Q_2(\mathbf{k})$ since $r \geq \ell$. If $p \nmid 2 \det \mathbf{M}_2$, it follows from (6.3) that

$$a\mathbf{k} \equiv -\overline{2 \det \mathbf{M}_2} \mathbf{M}_2^* \mathbf{m} \pmod{p^\ell},$$

whence $p^\ell \mid Q_2^*(\mathbf{m})$, as required for the first part of the lemma. For the second part we deduce that

$$S(\mathbf{k}) = p^{n\ell} \sum_{\substack{a \pmod{p^\ell} \\ (6.3) \text{ holds}}}^* e_{p^{r+\ell}}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}).$$

Re-introducing the sum over \mathbf{k} and using exponential sums to detect the divisibility constraints $p^{r-\ell} \mid p^{-\ell} Q_i(a\mathbf{k})$, which are clearly equivalent to $p^{r-\ell} \mid p^{-\ell} Q_i(\mathbf{k})$ when a is coprime to p , we deduce that

$$\mathcal{M}_{p^r, p^\ell}(\mathbf{m}) = \frac{p^{n\ell}}{p^{2(r-\ell)}} \sum_{\mathbf{b} \pmod{p^{r-\ell}}} T(\mathbf{b}), \tag{6.4}$$

where

$$T(\mathbf{b}) = \sum_{a \pmod{p^\ell}}^* \sum_{\mathbf{k} \in K} e_{p^{r+\ell}}(aQ_2(\mathbf{k}) + \mathbf{m} \cdot \mathbf{k}) e_{p^r}(b_1 Q_1(a\mathbf{k}) + b_2 Q_2(a\mathbf{k})),$$

and K denotes the set of $\mathbf{k} \pmod{p^r}$ for which (6.3) holds and $Q_i(\mathbf{k}) \equiv 0 \pmod{p^\ell}$, for $i = 1, 2$.

We proceed by writing $a\mathbf{k} = \mathbf{x} + p^\ell \mathbf{y}$, for \mathbf{y} modulo $p^{r-\ell}$. For each value of a coprime to p , choose an integer \bar{a} such that $a\bar{a} \equiv 1 \pmod{p^{r+\ell}}$. This leads to the expression

$$T(\mathbf{b}) = \sum_{a \pmod{p^\ell}}^* \sum_{\substack{\mathbf{x} \pmod{p^\ell} \\ \nabla Q_2(\mathbf{x}) + \mathbf{m} \equiv \mathbf{0} \pmod{p^\ell} \\ Q_i(\mathbf{x}) \equiv 0 \pmod{p^\ell}}} \sum_{\mathbf{y} \pmod{p^{r-\ell}}} f(\mathbf{x}, \mathbf{y}),$$

for $i = 1, 2$, with

$$f(\mathbf{x}, \mathbf{y}) = e_{p^{r+\ell}}(\bar{a}Q_2(\mathbf{x} + p^\ell \mathbf{y}) + \bar{a}\mathbf{m} \cdot (\mathbf{x} + p^\ell \mathbf{y})) e_{p^r}(b_1 Q_1(\mathbf{x} + p^\ell \mathbf{y}) + b_2 Q_2(\mathbf{x} + p^\ell \mathbf{y})).$$

Recall the notation $\mathbf{M}(\mathbf{b})$ introduced in (2.2). One concludes that

$$\left| \sum_{\mathbf{y} \pmod{p^{r-\ell}}} f(\mathbf{x}, \mathbf{y}) \right| = \left| \sum_{\mathbf{y} \pmod{p^{r-\ell}}} e_{p^{r-\ell}}(Q(\mathbf{y}) + \mathbf{n} \cdot \mathbf{y}) \right|,$$

with $\mathbf{n} = p^{-\ell} \bar{a}(\nabla Q_2(\mathbf{x}) + \mathbf{m}) + 2\mathbf{M}(\mathbf{b})\mathbf{x}$ and

$$Q(\mathbf{y}) = \bar{a}Q_2(\mathbf{y}) + p^\ell(b_1 Q_1(\mathbf{y}) + b_2 Q_2(\mathbf{y})).$$

This quadratic form has underlying matrix $\mathbf{M}(p^\ell b_1, p^\ell b_2 + \bar{a})$. The number of $\mathbf{x} \pmod{p^\ell}$ appearing in our expression for $T(\mathbf{b})$ is $O(1)$ by Lemma 1. Applying Lemma 13, we deduce that

$$T(\mathbf{b}) \ll p^{(r-\ell)n/2} \sum_{a \pmod{p^\ell}}^* \sqrt{K_{p^{r-\ell}}(2\mathbf{M}(p^\ell b_1, p^\ell b_2 + \bar{a}); \mathbf{0})}.$$

As b_2 runs modulo $p^{r-\ell}$ and a runs over elements modulo p^ℓ which are coprime to p , so $c_2 = p^\ell b_2 + \bar{a}$ runs over the set of residue classes modulo p^r , which are coprime to p . Replacing b_1 by $b_1 c_2$, and recalling (6.4), we obtain

$$\begin{aligned} \mathcal{M}_{p^r, p^\ell}(\mathbf{m}) &\ll \frac{p^{n(\ell+r)/2}}{p^{2(r-\ell)}} \sum_{b_1 \pmod{p^{r-\ell}}} \sum_{c_2 \pmod{p^r}}^* \sqrt{K_{p^{r-\ell}}(2\mathbf{M}(p^\ell b_1 c_2, c_2); \mathbf{0})} \\ &\ll \frac{p^{n(\ell+r)/2}}{p^{r-\ell}} \sum_{b_1 \pmod{p^{r-\ell}}} \sqrt{K_{p^{r-\ell}}(2\mathbf{M}(p^\ell b_1, 1); \mathbf{0})}. \end{aligned}$$

It will be convenient to put $\delta = v_p(2^n \det \mathbf{M}_2)$. We may assume that $\ell > \delta$. Indeed, if $\ell \leq \delta$, then we may take the trivial bound $S(\mathbf{k}) = O(1)$ in (6.1). Applying Hypothesis- ϱ we go on to deduce that $\mathcal{M}_{p^r, p^\ell}(\mathbf{m}) = O(p^{r(n-2)+\varepsilon})$, which is satisfactory.

Using Taylor’s formula we may write

$$\begin{aligned} \det 2\mathbf{M}(p^\ell b_1, 1) &= p^\ell f(b_1) + \det 2\mathbf{M}(0, 1) \\ &= p^\ell f(b_1) + 2^n \det \mathbf{M}_2, \end{aligned}$$

for an appropriate polynomial $f(b_1)$ with integer coefficients. Viewing b_1 as an element of \mathbb{Z} , it follows that $p^\ell f(b_1) + 2^n \det \mathbf{M}_2 \neq 0$, since $\ell > \delta$. Hence

$$v_p(\det 2\mathbf{M}(p^\ell b_1, 1)) = \delta$$

and Lemma 1 yields $K_{p^{r-\ell}}(2\mathbf{M}(p^\ell b_1, 1); \mathbf{0}) \ll 1$. The overall contribution to $\mathcal{M}_{p^r, p^\ell}(\mathbf{m})$ from this case is therefore $O(p^{\ell+n(\ell+r)/2})$, which is satisfactory. \square

7. Proof of Theorem 1: initial steps

We henceforth assume that $n \geq 5$. From Lemma 8 we have

$$S_{T, \mathbf{a}}^\sharp(B) = (1 + O_N(B^{-N})) \frac{B^{n-2}}{4^n} \sum_{\mathbf{m} \in \mathbb{Z}^n} \sum_{\substack{d=1 \\ (d, \Delta_\infty^*) \leq \Xi}}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{q=1}^\infty \frac{1}{q^n} T_{d,q}(\mathbf{m}) I_{d,q}(\mathbf{m}),$$

for any $N > 0$. We expect that the main term of the sum comes from the zero frequency $\mathbf{m} = \mathbf{0}$. This we will compute explicitly in §8 and it will turn out to have size B^{n-2} , as expected. Our immediate task, however, is to produce a satisfactory upper bound for the contribution from the non-zero frequencies. In view of the properties of $I_{d,q}(\mathbf{m})$ recorded in §3 the sums over d and q are effectively restricted to $d \ll B$ and $q \ll Q$, respectively. Moreover, Lemma 11 implies that the contribution of the tail $|\mathbf{m}| > dQB^{-1+\varepsilon}$ is arbitrarily small. Finally, Lemma 2 confirms Hypothesis- ϱ for the quadratic forms considered here.

As reflected in the various estimates collected together in §§4–6, the behaviour of the exponential sum $T_{d,q}(\mathbf{m})$ will depend intimately on \mathbf{m} . We must therefore give some thought to the question of controlling the number of $\mathbf{m} \in \mathbb{Z}^n$ which are constrained in appropriate ways. The constraints that feature in our work are of three basic sorts: either $Q_2^*(\mathbf{m}) = 0$ or $G(\mathbf{m}) = 0$

or $(-1)^{(n-1)/2}Q_2^*(\mathbf{m}) = \square$, the last case only being distinct from the first case when n is odd. The first two cases correspond to averaging \mathbf{m} over rational points $[\mathbf{m}]$ belonging to a projective variety $W \subset \mathbb{P}^{n-1}$, with W equal to the quadric $Q_2^* = 0$ or the dual hypersurface V^* , respectively. For such W we claim that

$$\#\{\mathbf{m} \in \mathbb{Z}^n : [\mathbf{m}] \in W(\mathbb{Q}), |\mathbf{m}| \leq M\} \ll M^{n-2+\varepsilon}, \tag{7.1}$$

for any $M \geq 1$ and $\varepsilon > 0$. When W is the quadric, in which case we recall that Q_2^* is non-singular, this follows from Lemma 3. When $W = V^*$ our discussion in § 2.2 shows that W is an irreducible hypersurface of degree $4(n - 2) \geq 12$. Hence the desired bound follows directly from joint work of the first author with Heath-Brown and Salberger [BHS06, Corollary 2]. Finally, we note that

$$\#\{\mathbf{m} \in \mathbb{Z}^n : (-1)^{(n-1)/2}Q_2^*(\mathbf{m}) = \square, |\mathbf{m}| \leq M\} \ll M^{n-1+\varepsilon}, \tag{7.2}$$

for any $M \geq 1$ and $\varepsilon > 0$. Indeed, the contribution from \mathbf{m} for which $Q_2^*(\mathbf{m}) = 0$ is satisfactory by (7.1) and the remaining contribution leads us to count points of height $O(M)$ on a non-singular quadric in $n + 1$ variables, for which we may appeal to Lemma 3.

We may now return to the task of estimating the contribution to $S_{T,\mathbf{a}}^\sharp(B)$ from \mathbf{m} for which $0 < |\mathbf{m}| \leq dQB^{-1+\varepsilon} = \sqrt{dB}^\varepsilon$. In this endeavour it will suffice to study the expression

$$U_{T,\mathbf{a}}(B, D) = B^{n-2} \sum_{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon} \sum'_{\substack{d \sim D \\ (d, \Delta_{\mathbb{V}}^\infty) \leq \Xi}} \frac{1}{d^{n-1}} \left| \sum_q \frac{1}{q^n} T_{d,q}(\mathbf{m}) I_{d,q}(\mathbf{m}) \right|, \tag{7.3}$$

for $D \geq 1$, where \sum' indicates that the sum should be taken over odd integers only and the notation $d \sim D$ means $D/2 < d \leq D$. In our analysis of this sum we will clearly only be interested in values of $D \ll B$. However, for the time being we allow $D \geq 1$ to be an arbitrary parameter.

Recall the definition (4.2) of the non-zero integer N . We split q as δq with $(q, dN) = 1$ and $\delta \mid (dN)^\infty$. Since q is restricted to have size $O(Q)$ in (7.3), by the properties of $I_{d,q}(\mathbf{m})$ recorded in § 3, we may assume that $\delta \ll B$. We deduce from the multiplicativity relations Lemmas 9 and 10 that

$$U_{T,\mathbf{a}}(B, D) \leq B^{n-2} \sum_{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon} \sum'_{\substack{d \sim D \\ (d, \Delta_{\mathbb{V}}^\infty) \leq \Xi}} \frac{1}{d^{n-1}} \sum_{\substack{\delta \mid (dN)^\infty \\ \delta \ll B}} \frac{|T_{d,\delta}(\mathbf{m})|}{\delta^n} \left| \sum_{\substack{q \\ (q, dN)=1}} \frac{1}{q^n} \mathcal{Q}_q(\mathbf{m}) I_{d,\delta q}(\mathbf{m}) \right|.$$

To estimate the inner sum over q we see via partial summation that it is

$$-\int_1^\infty \left(\sum_{\substack{q \leq y \\ (q, dN)=1}} \mathcal{Q}_q(\mathbf{m}) \right) \frac{\partial}{\partial y} \left(\frac{I_{d,\delta y}(\mathbf{m})}{y^n} \right) dy.$$

The integral is over $y \leq cQ/\delta$, for some absolute constant $c > 0$. Define the quantities

$$\theta_1(n; \mathbf{m}) = \begin{cases} \frac{7}{16} & \text{if } 2 \nmid n \text{ and } (-1)^{(n-1)/2}Q_2^*(\mathbf{m}) \neq \square, \\ 0 & \text{otherwise,} \end{cases}$$

and

$$\theta_2(n; \mathbf{m}) = \begin{cases} 1 & \text{if } Q_2^*(\mathbf{m}) = 0 \text{ and } (-1)^{n/2} \det \mathbf{M}_2 = \square, \\ \frac{1}{2} & \text{if } Q_2^*(\mathbf{m}) = 0 \text{ and } (-1)^{n/2} \det \mathbf{M}_2 \neq \square, \\ \frac{1}{2} & \text{if } Q_2^*(\mathbf{m}) \neq 0 \text{ and } (-1)^{(n-1)/2}Q_2^*(\mathbf{m}) = \square, \\ 0 & \text{otherwise.} \end{cases}$$

According to our conventions we note that the first case in the definition of $\theta_2(n; \mathbf{m})$ only arises for even n and likewise the third case only arises for odd n . Drawing together Lemmas 16–18, and using Lemma 12, we therefore obtain the estimate

$$\begin{aligned} &\ll |\mathbf{m}|^{\theta_1(n; \mathbf{m})} (dN)^\varepsilon \int_1^{cQ/\delta} y^{n/2+1+\theta_2(n; \mathbf{m})+\varepsilon} \left| \frac{\partial}{\partial y} \left(\frac{I_{d, \delta y}(\mathbf{m})}{y^n} \right) \right| dy \\ &\ll \left(\frac{d\delta}{B|\mathbf{m}|} \right)^{n/2-1} |\mathbf{m}|^{\theta_1(n; \mathbf{m})} (dNB)^\varepsilon \int_1^{cQ/\delta} y^{n/2+1+\theta_2(n; \mathbf{m})} \cdot y^{-n/2-2} dy, \end{aligned}$$

for the above integral. Let

$$\theta_1(n) = \begin{cases} 0 & \text{if } n \text{ is even,} \\ \frac{7}{16} & \text{if } n \text{ is odd,} \end{cases} \quad \theta_2(n) = \begin{cases} \frac{1}{2} & \text{if } 2 \mid n \text{ and } (-1)^{n/2} \det \mathbf{M}_2 = \square, \\ 0 & \text{otherwise.} \end{cases} \tag{7.4}$$

Returning to our initial estimate for $U_{T, \mathbf{a}}(B, D)$ and recalling the definition (1.2) of $S_{d, q}(\mathbf{m})$, we now have everything in place to establish the following result.

LEMMA 28. *We have*

$$U_{T, \mathbf{a}}(B, D) \ll \frac{B^{n/2-1+\varepsilon}}{D^{n/2}} (U^{(1)} + U^{(2)}),$$

where

$$\begin{aligned} U^{(1)} &= \sum_{\substack{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) = \square}} \frac{(B/\sqrt{D})^{1/2+\theta_2(n)}}{|\mathbf{m}|^{n/2-1}} \sum_{\substack{d \sim D \\ (d, \Delta_\infty^\varphi) \leq \Xi}} \sum_{\substack{\delta | d^\infty \\ \delta \ll B}} \frac{|S_{d, \delta}(\mathbf{m})|}{\delta^{n/2+1}}, \\ U^{(2)} &= \sum_{\substack{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) \neq \square}} \frac{|\mathbf{m}|^{\theta_1(n)}}{|\mathbf{m}|^{n/2-1}} \sum_{\substack{d \sim D \\ (d, \Delta_\infty^\varphi) \leq \Xi}} \sum_{\substack{\delta | d^\infty \\ \delta \ll B}} \frac{|S_{d, \delta}(\mathbf{m})|}{\delta^{n/2+1}}. \end{aligned}$$

Proof. Our work so far shows that $U_{T, \mathbf{a}}(B, D) \ll C^{(1)} + C^{(2)}$, with

$$\begin{aligned} C^{(1)} &= \frac{B^{n-2+\varepsilon}}{B^{n/2-1}} \sum_{\substack{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) = \square}} \frac{(B/\sqrt{D})^{\theta_2(n; \mathbf{m})}}{|\mathbf{m}|^{n/2-1}} \sum'_{\substack{d \sim D \\ (d, \Delta_\infty^\varphi) \leq \Xi}} \frac{1}{d^{n/2}} \sum_{\substack{\delta | (dN)^\infty \\ \delta \ll B}} \frac{|T_{d, \delta}(\mathbf{m})|}{\delta^{n/2+1+\theta_2(n; \mathbf{m})}}, \\ C^{(2)} &= \frac{B^{n-2+\varepsilon}}{B^{n/2-1}} \sum_{\substack{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) \neq \square}} \frac{|\mathbf{m}|^{\theta_1(n)}}{|\mathbf{m}|^{n/2-1}} \sum'_{\substack{d \sim D \\ (d, \Delta_\infty^\varphi) \leq \Xi}} \frac{1}{d^{n/2}} \sum_{\substack{\delta | (dN)^\infty \\ \delta \ll B}} \frac{|T_{d, \delta}(\mathbf{m})|}{\delta^{n/2+1}}. \end{aligned}$$

We note that $\theta_2(n; \mathbf{m}) = 1/2 + \theta_2(n)$ in $C^{(1)}$, but take $n/2 + 1$ for the exponent of δ . Drawing together Lemma 9, (3.4) and (4.1), it follows that

$$\sum_{\substack{\delta | N^\infty \\ \delta \ll B}} \frac{|T_{1, \delta}(\mathbf{m})|}{\delta^{n/2+1}} \ll \sum_{\substack{\delta | N^\infty \\ \delta \ll B}} 1 \ll (NB)^\varepsilon,$$

where the final inequality follows from (1.3). Thus we can restrict δ to be a divisor of d^∞ in $C^{(1)}$ and $C^{(2)}$ at the cost of enlarging the bound by B^ε . In particular, since d is odd, it follows that δ is odd and so Lemma 9 implies that $T_{d, \delta}(\mathbf{m}) = S_{d, \delta}(\mathbf{m})$. Finally, on taking $d > D/2$ in the denominator of both expressions, we arrive at the statement of the lemma. \square

We are now ready to commence our detailed estimation of $U_{T,\mathbf{a}}(B, D)$, based on Lemma 28. We begin by directing our attention to the estimation of $U^{(2)}$. Pulling out the greatest common divisor h of \mathbf{m} , and then splitting $d = d_1 d_2$ and $\delta = \delta_1 \delta_2$, with $\delta_1 \mid d_1^\infty$, $d_1 \mid h^\infty$, $\delta_2 \mid d_2^\infty$ and $(d_2, h) = 1$, it follows that

$$U^{(2)} = \sum_{0 < h \leq \sqrt{DB^\varepsilon}} \frac{h^{\theta_1(n)}}{h^{n/2-1}} \sum_{\substack{0 < |\mathbf{m}| \leq \sqrt{DB^\varepsilon}/h \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) \neq \square \\ \gcd(\mathbf{m})=1}} \frac{|\mathbf{m}|^{\theta_1(n)}}{|\mathbf{m}|^{n/2-1}} \sum_{\substack{d_1 \leq D \\ d_1 \mid h^\infty \\ (d_1, \Delta_{\tilde{V}}^\infty) \leq \Xi}} \sum_{\substack{\delta_1 \mid d_1^\infty \\ \delta_1 \ll B}} \frac{|S_{d_1, \delta_1}(h\mathbf{m})|}{\delta_1^{n/2+1}} \Sigma_1, \tag{7.5}$$

where if $\Xi_{d_1} = \Xi / (d_1, \Delta_{\tilde{V}}^\infty)$, then

$$\Sigma_1 = \sum_{\substack{d_2 \sim D/d_1 \\ (d_2, h)=1 \\ (d_2, \Delta_{\tilde{V}}^\infty) \leq \Xi_{d_1}}} \sum_{\substack{\delta_2 \mid d_2^\infty \\ \delta_2 \ll B}} \frac{|S_{d_2, \delta_2}(h\mathbf{m})|}{\delta_2^{n/2+1}}.$$

Here we recall from § 3 that $S_{d_2, \delta_2}(h\mathbf{m}) = S_{d_2, \delta_2}(\mathbf{m})$ since $(\delta_2 d_2, h) = 1$. Now set

$$H(\mathbf{m}) = \begin{cases} \Delta_V G(\mathbf{m}) Q_2^*(\mathbf{m}) \det \mathbf{M}_2 & \text{if } G(\mathbf{m}) \neq 0, \\ \Delta_V Q_2^*(\mathbf{m}) \det \mathbf{M}_2 & \text{if } G(\mathbf{m}) = 0, \end{cases}$$

where G is the dual form introduced in § 2.2. Note that $Q_2^*(\mathbf{m}) \neq 0$ in this definition, so that $H(\mathbf{m})$ is a non-zero integer.

We further split $d_2 = d_{21} d_{22}$ and $\delta_2 = \delta_{21} \delta_{22}$ with $\delta_{21} \mid d_{21}^\infty$, $d_{21} \mid H(\mathbf{m})^\infty$, $\delta_{22} \mid d_{22}^\infty$ and $(d_{22}, H(\mathbf{m})) = 1$. It follows that

$$\Sigma_1 \leq \sum_{\substack{d_{21} \leq D/d_1 \\ d_{21} \mid H(\mathbf{m})^\infty \\ (d_{21}, h)=1 \\ (d_{21}, \Delta_{\tilde{V}}^\infty) \leq \Xi_{d_1}}} \sum_{\substack{\delta_{21} \mid d_{21}^\infty \\ \delta_{21} \ll B}} \sum_{\substack{d_{22} \sim D/d_1 d_{21} \\ (d_{22}, hH(\mathbf{m}))=1}} \sum_{\substack{\delta_{22} \mid d_{22}^\infty \\ \delta_{22} \ll B}} \frac{|S_{d_{21}, \delta_{21}}(\mathbf{m})| |S_{d_{22}, \delta_{22}}(\mathbf{m})|}{(\delta_{21} \delta_{22})^{n/2+1}}.$$

In view of the fact that $(d_{22}, 2Q_2^*(\mathbf{m}) \det \mathbf{M}_2) = 1$, it follows from Lemmas 26 and 27 that $S_{d_{22}, \delta_{22}}(\mathbf{m})$ vanishes unless $\delta_{22} = 1$. Hence we may conclude that the sum over d_{22} and δ_{22} is

$$\sum_{\substack{d_{22} \sim D/d_1 d_{21} \\ (d_{22}, hH(\mathbf{m}))=1}} |\mathcal{D}_{d_{22}}(\mathbf{m})| \ll \left(\frac{D}{d_1 d_{21}} \right)^{n/2 + \psi_1(\mathbf{m}) + \varepsilon},$$

by Lemmas 23 and 24, where

$$\psi_1(\mathbf{m}) = \begin{cases} \frac{1}{2} & \text{if } G(\mathbf{m}) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\Sigma_1 \ll \left(\frac{D}{d_1} \right)^{n/2 + \psi_1(\mathbf{m}) + \varepsilon} \sum_{\substack{d_{21} \leq D/d_1 \\ d_{21} \mid H(\mathbf{m})^\infty \\ (d_{21}, h)=1 \\ (d_{21}, \Delta_{\tilde{V}}^\infty) \leq \Xi_{d_1}}} \sum_{\substack{\delta_{21} \mid d_{21}^\infty \\ \delta_{21} \ll B}} \frac{|S_{d_{21}, \delta_{21}}(\mathbf{m})|}{d_{21}^{n/2 + \psi_1(\mathbf{m})} \delta_{21}^{n/2+1}}.$$

Now there is a factorisation $d_{21} = d'_{21}d''_{21}$ such that $(d'_{21}, d''_{21}) = 1$ and $d'_{21} \mid \delta_{21}^\infty$ and $\delta_{21} \mid d''_{21}^\infty$, with $S_{d_{21}, \delta_{21}}(\mathbf{m}) = \mathcal{M}_{d'_{21}, \delta_{21}}(\mathbf{m})\mathcal{D}_{d''_{21}}(\mathbf{m})$. It therefore follows from Lemmas 22 and 25 that

$$S_{d_{21}, \delta_{21}}(\mathbf{m}) \ll (d_{21}, \Delta_V^\infty)^{n/2-2} d_{21}^{n/2+\varepsilon} \delta_{21}^{n/2+1},$$

since \mathbf{m} is primitive. Hence

$$\Sigma_1 \ll \Xi_{d_1}^{n/2-2} \left(\frac{D}{d_1}\right)^{n/2+\psi_1(\mathbf{m})+\varepsilon} B^\varepsilon.$$

Substituting this into (7.5) we now examine

$$\begin{aligned} \Sigma_2 &= \sum_{\substack{d_1 \leq D \\ d_1 \mid h^\infty \\ (d_1, \Delta_V^\infty) \leq \Xi}} \sum_{\substack{\delta_1 \mid d_1^\infty \\ \delta_1 \ll B}} \frac{|S_{d_1, \delta_1}(h\mathbf{m})|}{\delta_1^{n/2+1}} \Sigma_1 \\ &\ll D^{n/2+\psi_1(\mathbf{m})+\varepsilon} B^\varepsilon \sum_{\substack{d_1 \leq D \\ d_1 \mid h^\infty \\ (d_1, \Delta_V^\infty) \leq \Xi}} \frac{\Xi^{n/2-2}}{(d_1, \Delta_V^\infty)^{n/2-2}} \sum_{\substack{\delta_1 \mid d_1^\infty \\ \delta_1 \ll B}} \frac{|S_{d_1, \delta_1}(h\mathbf{m})|}{d_1^{n/2+\psi_1(\mathbf{m})} \delta_1^{n/2+1}}. \end{aligned}$$

We repeat the process that we undertook above to estimate $S_{d_1, \delta_1}(h\mathbf{m})$, using Lemmas 22 and 25. This gives

$$\frac{|S_{d_1, \delta_1}(h\mathbf{m})|}{d_1^{n/2+\psi_1(\mathbf{m})} \delta_1^{n/2+1}} \ll (d_1, \Delta_V^\infty)^{n/2-2} d_1^\varepsilon h^{n/2-2-\psi_1(\mathbf{m})}.$$

By (1.3) there are only $O(B^\varepsilon D^\varepsilon)$ values of δ_1 that feature in this analysis. In this way we arrive at the estimate

$$\Sigma_2 \ll \Xi^{n/2-2} D^{n/2+\psi_1(\mathbf{m})+\varepsilon} B^\varepsilon h^{n/2-2-\psi_1(\mathbf{m})}. \tag{7.6}$$

It is time to distinguish between whether $G(\mathbf{m}) = 0$ or $G(\mathbf{m}) \neq 0$ in our analysis of $U^{(2)}$. Accordingly, let us write $U^{(2)} = U^{(21)} + U^{(22)}$ for the corresponding decomposition. We begin with a discussion of $U^{(22)}$, for which $\psi_1(\mathbf{m}) = 0$ in (7.6). We deduce from (7.5) that

$$\begin{aligned} U^{(22)} &\ll \Xi^{n/2-2} D^{n/2+\varepsilon} B^\varepsilon \sum_{0 < h \leq \sqrt{DB}^\varepsilon} h^{\theta_1(n)-1} \sum_{0 < |\mathbf{m}| \leq \sqrt{DB}^\varepsilon/h} \frac{|\mathbf{m}|^{\theta_1(n)}}{|\mathbf{m}|^{n/2-1}} \\ &\ll \Xi^{n/2-2} D^{n/2+\varepsilon} B^\varepsilon \sum_{0 < h \leq \sqrt{DB}^\varepsilon} h^{\theta_1(n)-1} \left(\frac{\sqrt{DB}^\varepsilon}{h}\right)^{n/2+1+\theta_1(n)}, \end{aligned}$$

on breaking the sum over \mathbf{m} into dyadic intervals for $|\mathbf{m}|$. The sum over h is therefore convergent and we conclude that

$$\begin{aligned} U^{(22)} &\ll \Xi^{n/2-2} D^{n/2+\varepsilon} B^\varepsilon (\sqrt{D})^{n/2+1+\theta_1(n)} \\ &= \Xi^{n/2-2} D^{3n/4+(1+\theta_1(n))/2+\varepsilon} B^\varepsilon. \end{aligned} \tag{7.7}$$

We now turn to a corresponding analysis of $U^{(21)}$, for which $\psi_1(\mathbf{m}) = 1/2$ in (7.6). It follows from (7.5) that

$$\begin{aligned}
 U^{(21)} &\ll \Xi^{n/2-2} D^{(n+1)/2+\varepsilon} B^\varepsilon \sum_{0 < h \leq \sqrt{DB^\varepsilon}} h^{\theta_1(n)-3/2} \sum_{\substack{0 < |\mathbf{m}| \leq (\sqrt{DB^\varepsilon})/h \\ G(\mathbf{m})=0}} \frac{|\mathbf{m}|^{\theta_1(n)}}{|\mathbf{m}|^{n/2-1}} \\
 &\ll \Xi^{n/2-2} D^{(n+1)/2+\varepsilon} B^\varepsilon \max_{1/2 < M \leq \sqrt{DB^\varepsilon}} M^{\theta_1(n)+1-n/2} \sum_{\substack{|\mathbf{m}| \leq M \\ G(\mathbf{m})=0}} 1.
 \end{aligned}$$

Appealing to (7.1), we therefore deduce that

$$\begin{aligned}
 U^{(21)} &\ll \Xi^{n/2-2} D^{(n+1)/2+\varepsilon} B^\varepsilon (\sqrt{D})^{n/2-1+\theta_1(n)} \\
 &= \Xi^{n/2-2} D^{3n/4+\theta_1(n)/2+\varepsilon} B^\varepsilon.
 \end{aligned} \tag{7.8}$$

Our final task in this section is to estimate $U^{(1)}$ in Lemma 28, for which we will be able to recycle most of the treatment of $U^{(2)}$. Following the steps up to (7.6) we find that

$$U^{(1)} \ll \Xi^{n/2-2} D^{n/2+\varepsilon} \left(\frac{B}{\sqrt{D}} \right)^{1/2+\theta_2(n)+\varepsilon} \sum_{\substack{0 < |\mathbf{m}| \leq \sqrt{DB^\varepsilon} \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) = \square}} D^{\psi_1(\mathbf{m})} |\mathbf{m}|^{1-n/2}.$$

One notes that in the absence of the function $\theta_1(n)$, the exponent of h is at most -1 , so that the summation over h can be carried out immediately. As previously it will be necessary to write $U^{(1)} = U^{(11)} + U^{(12)}$, where $U^{(11)}$ denotes the contribution from the case $G(\mathbf{m}) = 0$ and $U^{(12)}$ is the remaining contribution. Beginning with the latter, in which case $\psi_1(\mathbf{m}) = 0$, we deduce that

$$U^{(12)} \ll \Xi^{n/2-2} D^{n/2+\varepsilon} \left(\frac{B}{\sqrt{D}} \right)^{1/2+\theta_2(n)+\varepsilon} \max_{1/2 < M \leq \sqrt{DB^\varepsilon}} M^{1-n/2} \sum_{\substack{|\mathbf{m}| \leq M \\ (-1)^{(n-1)/2} Q_2^*(\mathbf{m}) = \square}} 1.$$

Applying (7.2) we therefore obtain

$$\begin{aligned}
 U^{(12)} &\ll \Xi^{n/2-2} D^{n/2+\varepsilon} \left(\frac{B}{\sqrt{D}} \right)^{1/2+\theta_2(n)} B^\varepsilon (\sqrt{D})^{n/2} \\
 &= \Xi^{n/2-2} D^{3n/4-1/4-\theta_2(n)/2+\varepsilon} B^{1/2+\theta_2(n)+\varepsilon}.
 \end{aligned} \tag{7.9}$$

For the remaining contribution, with $\psi_1(\mathbf{m}) = 1/2$, we will drop the fact that $(-1)^{(n-1)/2} Q_2^*(\mathbf{m})$ should be a square from the sum over \mathbf{m} since there is already sufficient gain from the fact that $G(\mathbf{m})$ vanishes. Arguing as above, but this time with recourse to (7.1), we conclude that

$$\begin{aligned}
 U^{(11)} &\ll \Xi^{n/2-2} D^{(n+1)/2+\varepsilon} \left(\frac{B}{\sqrt{D}} \right)^{1/2+\theta_2(n)} B^\varepsilon (\sqrt{D})^{n/2-1} \\
 &= \Xi^{n/2-2} D^{3n/4-1/4-\theta_2(n)/2+\varepsilon} B^{1/2+\theta_2(n)+\varepsilon}.
 \end{aligned} \tag{7.10}$$

Recall the definitions (7.4) of θ_1 and θ_2 . Combining (7.7)–(7.10) in Lemma 28, we may now record our final bound for $U_{T,\mathbf{a}}(B, D)$.

LEMMA 29. *Let $n \geq 5$ and $D \geq 1$. Then we have*

$$U_{T,\mathbf{a}}(B, D) \ll \Xi^{n/2-2} B^{n/2-1+\varepsilon} (D^{n/4+1+\theta_1(n)/2+\varepsilon} + D^{n/4-1/4-\theta_2(n)/2+\varepsilon} B^{1/2+\theta_2(n)}).$$

8. Proof of Theorem 1: conclusion

Recall the expression for $S_{T,\mathbf{a}}^\sharp(B)$ recorded at the start of § 7. We now have everything in place to estimate the overall contribution to this sum from the non-zero \mathbf{m} . An upper bound for this contribution is obtained by taking $D \ll B$ in Lemma 29’s estimate for the quantity introduced in (7.3). This gives the overall contribution

$$\begin{aligned} &\ll \Xi^{n/2-2} B^{n/2-1+\varepsilon} (B^{n/4+(1+\theta_1(n))/2} + B^{n/4+1/4+\theta_2(n)/2}) \\ &\ll \Xi^{n/2-2} B^{3n/4-1/2+\theta_1(n)/2+\varepsilon}. \end{aligned}$$

Combining this with Lemmas 5, 6 and 8, our work so far has shown that

$$S(B) = M^\sharp(B) + O(\Xi^{-1/n} B^{n-2+\varepsilon} + \Xi B^{n-3+\varepsilon} + \Xi^{n/2-2} B^{3n/4-1/2+\theta_1(n)/2+\varepsilon}), \tag{8.1}$$

where

$$M^\sharp(B) = \frac{B^{n-2}}{4^{n-1}} \sum_T \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{\substack{d=1 \\ (d, \Delta_{\mathbb{V}}^\infty) \leq \Xi}}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{q=1}^\infty \frac{1}{q^n} T_{d,q}(\mathbf{0}) I_{d,q}(\mathbf{0}). \tag{8.2}$$

We begin with a few words about the integral

$$I_{d,q}(\mathbf{0}) = \int_{\mathbb{R}^n} h\left(\frac{q\sqrt{d}}{B}, Q_2(\mathbf{y})\right) W_{d,T}(\mathbf{y}) \, d\mathbf{y},$$

where $W_{d,T}$ is given by (3.1) and we have made the substitution $Q = B/\sqrt{d}$. Recall the correspondence (3.5) between $I_{d,q}(\mathbf{0})$ and $I_r^*(\mathbf{0})$. Recall additionally the properties of $h(x, y)$ and the weight function $W_{d,T}$ that were recorded in § 3. In particular, $|\nabla Q_2(\mathbf{y})| \gg 1$ on $\text{supp}(W_{d,T})$ and we have $d \ll B$ and $q\sqrt{d} \ll B$ if $I_{d,q}(\mathbf{0})$ is non-zero. Combining [Hea96, Lemma 14] and [Hea96, Lemma 15] it follows that

$$I_{d,q}(\mathbf{0}) \ll 1. \tag{8.3}$$

Furthermore, according to [Hea96, Lemma 13], we have

$$I_{d,q}(\mathbf{0}) = \tau_\infty(Q_2, W_{d,T}) + O_N \left\{ \left(\frac{q\sqrt{d}}{B} \right)^N \right\}, \tag{8.4}$$

for any $N > 0$, where for any infinitely differentiable bounded function $\omega : \mathbb{R}^n \rightarrow \mathbb{R}$ of compact support we set

$$\tau_\infty(Q_2, \omega) = \lim_{\varepsilon \rightarrow 0} (2\varepsilon)^{-1} \int_{|Q_2(\mathbf{y})| \leq \varepsilon} \omega(\mathbf{y}) \, d\mathbf{y}. \tag{8.5}$$

In fact $\tau_\infty(Q_2, \omega)$ is the real density of points on the affine cone over the hypersurface $Q_2 = 0$, weighted by ω . We will use these facts to extract the dependence on $I_{d,q}(\mathbf{0})$ from (8.2).

Returning to (8.2), our main goal in this section will be a proof of the following asymptotic formula.

LEMMA 30. *Let $n \geq 5$, let $\varepsilon > 0$ and assume Hypothesis- ρ . Then we have*

$$M^\sharp(B) = B^{n-2} \sigma_\infty \prod_p \sigma_p + O(\Xi^{-1} B^{n-2} + B^{n-5/2+\varepsilon} + B^{3n/4-1+\varepsilon}),$$

where σ_∞ and σ_p are the expected local densities of points on $X(\mathbb{R})$ and $X(\mathbb{Q}_p)$, respectively. In particular, $\sigma_\infty \prod_p \sigma_p > 0$ if $X(\mathbb{R})$ and $X(\mathbb{Q}_p)$ are non-empty for each prime p .

In the context of Theorem 1, for which $n \geq 7$, we note that Hypothesis- ρ follows from Lemma 2. Moreover, $X(\mathbb{Q}_p)$ is non-empty for every prime p by the work of Demjanov [Dem56].

We now wish to apply Lemma 30 in (8.1) to complete the proof of Theorem 1. Our estimates will be optimised by the choice $\Xi = B^{\xi(n)}$, with

$$\xi(n) = \left(\frac{n}{4} - \frac{3 + \theta_1(n)}{2}\right) \left(\frac{2n}{n^2 - 4n + 2}\right),$$

which comes from balancing the first and third error terms in (8.1). We make the observation that $\xi(n) < \xi(n)(1 + 1/n) < 1$, for $n \geq 7$. Hence we obtain the overall error term $O(B^{n-2-\eta(n)+\varepsilon})$, with

$$\eta(n) = \min\left\{\frac{\xi(n)}{n}, 1 - \xi(n), \frac{1}{2}, \frac{n}{4} - 1\right\} = \frac{\xi(n)}{n}.$$

Observe that $\eta(n) > 0$ if $n \geq 7$. At this point we stress that if we had exponent 1/2 instead of 7/16 in (4.4), which corresponds to the convexity bound, we would have $\theta_1(n) = 1/2$ for odd n and hence our result would only hold for $n \geq 8$. This completes the proof of Theorem 1, subject to Lemma 30.

The remainder of this section will be devoted to the proof of Lemma 30. Combining (3.4), (4.1) and Lemma 25 it follows from Hypothesis- ρ that

$$T_{d,q}(\mathbf{0}) \ll d^{n-2+\varepsilon} q^{n/2+1}, \tag{8.6}$$

for any $d, q \in \mathbb{N}$. We will also make use of the bound (8.3) and the fact that $d \ll B$ whenever $I_{d,q}(\mathbf{0})$ is non-zero. Let $M(B)$ be defined as in (8.2), but in which the sum over d runs over all positive integers with $d \ll B$. It follows from (8.6) that $M^\sharp(B) = M(B) + O(\Xi^{-1}B^{n-2+\varepsilon})$. Write

$$M(B) = \frac{B^{n-2}}{4^{n-1}} \sum_T M_T(B),$$

say.

For given $\theta > 0$, let us consider the contribution to $M_T(B)$ from $q > B^{1/2-\theta}$. Invoking (8.6), this contribution is seen to be

$$\begin{aligned} &\ll \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{d \ll B} \frac{1}{d^{n-1}} \sum_{q > B^{1/2-\theta}} \frac{|T_{d,q}(\mathbf{0})|}{q^n} \\ &\ll \sum_{d \ll B} d^{-1+\varepsilon} \sum_{q > B^{1/2-\theta}} q^{-n/2+1+\varepsilon} \\ &\ll B^{(1/2-\theta)(-n/2+2)+\varepsilon}, \end{aligned}$$

since $n \geq 5$. Turning to the contribution from $q \leq B^{1/2-\theta}$ we see that the error term in (8.4) is $O_N(B^{-N})$ for arbitrary $N > 0$, since $d \ll B$. Hence such q make the overall contribution

$$\sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{d \ll B} \frac{\chi(d)\tau_\infty(Q_2, W_{d,T})}{d^{n-1}} \sum_{q \leq B^{1/2-\theta}} \frac{T_{d,q}(\mathbf{0})}{q^n} + O_N(B^{-N}),$$

to $M_T(B)$. The previous paragraph shows that the summation over q can be extended to infinity with error $O(B^{(1/2-\theta)(-n/2+2)+\varepsilon})$. Moreover, for any fixed T , the function $\tau_\infty(Q_2, W_{d,T})$ vanishes unless

$$d \ll \begin{cases} T & \text{if } T \leq B, \\ B^2/T & \text{otherwise.} \end{cases}$$

Hence we may also extend the summation over d to infinity. Taking θ to be a suitably small positive multiple of ε , we may therefore conclude that

$$M_T(B) = \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{d=1}^{\infty} \frac{\chi(d)\tau_{\infty}(Q_2, W_{d,T})}{d^{n-1}} \sum_{q=1}^{\infty} \frac{T_{d,q}(\mathbf{0})}{q^n} + O(B^{-n/4+1+\varepsilon}).$$

Let us denote by $L_T(B)$ the main term in this expression. We proceed to introduce the summation over T via the following result, in which $\varrho(d) = \mathcal{D}_d(\mathbf{0})$.

LEMMA 31. *Let $\varepsilon > 0$ and $M \in \mathbb{N}$. Assume Hypothesis- ϱ . Then for any $1 \leq y < x$ we have*

$$\sum_{\substack{y < d \leq x \\ (d,M)=1}} \frac{\chi(d)\varrho(d)}{d^{n-1}} \ll \frac{M^\varepsilon}{\sqrt{y}}.$$

Proof. Let $s = \sigma + it \in \mathbb{C}$. In the usual way we consider the Dirichlet series

$$\eta_M(s) = \sum_{(d,M)=1} \frac{\chi(d)\varrho(d)}{d^s} = \prod_{p \nmid M} \left(1 + \frac{\chi(p)\varrho(p)}{p^s} + O(p^{2n-4-2\sigma+\varepsilon}) \right),$$

where the error term comes from Hypothesis- ϱ . Since $\varrho(p) = p^{n-2} + O(p^{n-5/2})$, by the Lang–Weil estimate, we conclude that

$$\eta_M(s) = L(s - (n - 2), \chi)E_M(s),$$

where $E_M(s)$ is absolutely convergent and bounded by $O(M^\varepsilon)$ in any fixed complex half-plane $\sigma \geq n - 3/2 + \eta$, with $\eta > 0$. The conclusion of the lemma is now available through a straightforward application of Perron’s formula in the form (4.5). \square

We deduce from Lemma 31 that

$$\sum_{(d,q)=1} \frac{\chi(d)\varrho(d)V_T(d)}{d^{n-1}} \ll \frac{q^\varepsilon}{\sqrt{T}} \tag{8.7}$$

and

$$\sum_{(d,q)=1} \frac{\chi(d)\varrho(d)V_T(B^2Q_1(\mathbf{y})/d)}{d^{n-1}} \ll \frac{q^\varepsilon\sqrt{T}}{B\sqrt{Q_1(\mathbf{y})}} \ll \frac{q^\varepsilon\sqrt{T}}{B}, \tag{8.8}$$

uniformly for $\mathbf{y} \in \text{supp}(W)$. Here we recall that $Q_1(\mathbf{y})$ is positive and has order of magnitude 1 on $\text{supp}(W)$.

We now claim that

$$\sum_T L_T(B) = 2C + O(B^{-1/2+\varepsilon}),$$

with

$$C = \tau_{\infty}(Q_2, W) \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{d=1}^{\infty} \frac{\chi(d)}{d^{n-1}} \sum_{q=1}^{\infty} \frac{T_{d,q}(\mathbf{0})}{q^n}. \tag{8.9}$$

Now the weight function $W_{d,T}$ differs according to whether $T \leq B$ or $T > B$. It will be convenient to set $W_{d,T}^{(1)}(\mathbf{y}) = W(\mathbf{y})V_T(d)$ and $W_{d,T}^{(2)}(\mathbf{y}) = W(\mathbf{y})V_T(B^2Q_1(\mathbf{y})/d)$. In either case we wish to

extend the sum over T to the full range, since $\sum_T V_T(t) = 1$ for $1 \leq t \ll B^2$. We have

$$\sum_{T \leq B} L_T(B) = C - \sum_{T > B} L_T^{(1)}(B)$$

and

$$\sum_{T > B} L_T(B) = C - \sum_{T \leq B} L_T^{(2)}(B),$$

where $L_T^{(i)}(B)$ is defined as for $L_T(B)$ but with the weight function $W_{d,T}^{(i)}$, for $i = 1, 2$. To estimate the tails we employ the factorisation properties of $T_{d,q}(\mathbf{0})$, finding that

$$L_T^{(i)}(B) = \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{q=1}^{\infty} \frac{1}{q^n} \sum_{\substack{\delta | q^\infty \\ \delta \ll B}} \frac{T_{\delta,q}(\mathbf{0})}{\delta^{n-1}} \sum_{(d,q)=1} \frac{\chi(d)\varrho(d)\tau_\infty(Q_2, W_{\delta d,T}^{(i)})}{d^{n-1}},$$

for $i = 1, 2$. The inner sum over d is estimated by substituting the expression (8.5) for $\tau_\infty(Q_2, W_{\delta d,T}^{(i)})$, and then interchanging the limit integral and sum. Note that the sum over d is finite since $\tau_\infty(Q_2, W_{\delta d,T}^{(i)}) = 0$ unless $\delta d \ll B$. The resulting sum over d is then estimated using (8.7) or (8.8), according to whether $i = 1$ or 2 , respectively. After estimating the limit integral trivially, the claim follows on invoking our hypothesised bound (8.6). Bringing everything together, we have therefore shown that

$$M(B) = \frac{2B^{n-2}}{4^{n-1}}C + O(B^{n-5/2+\varepsilon} + B^{3n/4-1+\varepsilon}), \tag{8.10}$$

with C given by (8.9).

To close, we wish to show that the leading constant admits an interpretation in terms of local densities for the intersection of quadrics X considered in Theorem 1. For a prime p the relevant p -adic density is equal to

$$\sigma_p = \lim_{k \rightarrow \infty} p^{-kn} N(p^k),$$

where

$$N(p^k) = \# \left\{ (\mathbf{x}, u, v) \in (\mathbb{Z}/p^k\mathbb{Z})^{n+2} : \begin{array}{l} Q_1(\mathbf{x}) \equiv u^2 + v^2 \pmod{p^k}, \\ Q_2(\mathbf{x}) \equiv 0 \pmod{p^k} \end{array} \right\},$$

if $p > 2$, and

$$N(2^k) = \# \left\{ (\mathbf{x}, u, v) \in (\mathbb{Z}/2^k\mathbb{Z})^{n+2} : \begin{array}{l} Q_1(\mathbf{x}) \equiv u^2 + v^2 \pmod{2^k}, \\ Q_2(\mathbf{x}) \equiv 0 \pmod{2^k}, 2 \nmid Q_1(\mathbf{x}) \end{array} \right\}.$$

The restriction to odd values of $Q_1(\mathbf{x})$ in $N(2^k)$ comes from the definition of the counting function $S(B)$. In order to relate these densities to the local factors that arise in our analysis, we set

$$S(A; p^k) = \#\{(u, v) \in (\mathbb{Z}/p^k\mathbb{Z})^2 : u^2 + v^2 \equiv A \pmod{p^k}\},$$

for any $A \in \mathbb{Z}$ and any prime power p^k . According to Heath-Brown [Hea03, § 8] we have

$$S(A; p^k) = \begin{cases} p^k + kp^k(1 - 1/p) & \text{if } v_p(A) \geq k, \\ (1 + v_p(A))p^k(1 - 1/p) & \text{if } v_p(A) < k, \end{cases}$$

when $p \equiv 1 \pmod{4}$. When $p \equiv 3 \pmod{4}$, we have

$$S(A; p^k) = \begin{cases} p^{2\lfloor k/2 \rfloor} & \text{if } v_p(A) \geq k, \\ p^k(1 + 1/p) & \text{if } v_p(A) < k \text{ and } 2 \mid v_p(A), \\ 0 & \text{if } v_p(A) < k \text{ and } 2 \nmid v_p(A). \end{cases}$$

Finally, for odd A , when $p = 2$ and $k \geq 2$ we have

$$S(A; 2^k) = \begin{cases} 2^{k+1} & \text{if } A \equiv 1 \pmod{4}, \\ 0 & \text{otherwise.} \end{cases}$$

We now have everything in place to reinterpret the densities σ_p . We begin by analysing the case $p = 2$, obtaining

$$\sigma_2 = \lim_{k \rightarrow \infty} 2^{1-k(n-1)} \# \left\{ \mathbf{x} \in (\mathbb{Z}/2^k\mathbb{Z})^n : \begin{array}{l} Q_1(\mathbf{x}) \equiv 1 \pmod{4}, \\ Q_2(\mathbf{x}) \equiv 0 \pmod{2^k} \end{array} \right\}. \tag{8.11}$$

Alternatively, when $p > 2$, it is straightforward to deduce that

$$\sigma_p = \left(1 - \frac{\chi(p)}{p} \right) \lim_{k \rightarrow \infty} p^{-k(n-1)} \sum_{0 \leq e \leq k} \chi(p^e) \tilde{N}_k(e), \tag{8.12}$$

where

$$\tilde{N}_k(e) = \# \left\{ \mathbf{x} \in (\mathbb{Z}/p^k\mathbb{Z})^n : \begin{array}{l} Q_1(\mathbf{x}) \equiv 0 \pmod{p^e}, \\ Q_2(\mathbf{x}) \equiv 0 \pmod{p^k} \end{array} \right\}.$$

Finally, for the real density σ_∞ of points, we claim that

$$\sigma_\infty = \pi \tau_\infty(Q_2, W), \tag{8.13}$$

in the notation of (8.5). Supposing that the equations for X are taken to be $Q_1(\mathbf{x}) = u^2 + v^2$ and $Q_2(\mathbf{x}) = 0$, the real density is equal to

$$\sigma_\infty = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{(\mathbf{x}, u, v) \in \mathbb{R}^{n+2}} W(\mathbf{x}) e(\alpha\{Q_1(\mathbf{x}) - u^2 - v^2\} + \beta Q_2(\mathbf{x})) \, d\mathbf{x} \, du \, dv \, d\alpha \, d\beta.$$

We restrict u, v to be non-negative and substitute $t = Q_1(\mathbf{x}) - u^2 - v^2$ for v . Writing

$$F(t) = \frac{1}{2} \int_{-\infty}^{\infty} \int_{\mathbf{x}, u} \frac{W(\mathbf{x}) e(\beta Q_2(\mathbf{x}))}{\sqrt{Q_1(\mathbf{x}) - u^2 - t}} \, d\mathbf{x} \, du \, d\beta,$$

where the integral is over $(\mathbf{x}, u) \in \mathbb{R}^{n+1}$ such that $u \geq 0$ and $Q_1(\mathbf{x}) - u^2 - t \geq 0$, we therefore obtain

$$\sigma_\infty = 4 \int_{-\infty}^{\infty} \int_t^\infty F(t) e(\alpha t) \, dt \, d\alpha.$$

By the Fourier inversion theorem this reduces to $4F(0)$. Noting that

$$\int_0^{\sqrt{A}} \frac{du}{\sqrt{A - u^2}} = \frac{\pi}{2},$$

for any $A > 0$, we arrive at the expression

$$\sigma_\infty = 4 \times \frac{1}{2} \times \frac{\pi}{2} \int_{-\infty}^{\infty} \int_{\mathbf{x} \in \mathbb{R}^n} W(\mathbf{x}) e(\beta Q_2(\mathbf{x})) \, d\mathbf{x} \, d\beta.$$

However, the remaining integral is just the real density $\tau_\infty(Q_2, W)$, by [Hea96, Theorem 3]. This concludes the proof of (8.13).

It is now time to interpret the constant C in (8.9) in terms of the local densities σ_p and σ_∞ . Invoking Lemma 9 we may write

$$C = \tau_\infty(Q_2, W) \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{d=1}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{\ell=0}^\infty \sum_{\substack{q'=1 \\ 2 \nmid q'}}^\infty \frac{1}{(2^\ell q')^n} S_{d,q'}(\mathbf{0}) S_{1,2^\ell}^{\chi(dq')}(\mathbf{0}).$$

Recall (3.3). We therefore see that for fixed d and q' the sum over \mathbf{a} and ℓ is

$$\begin{aligned} \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/4\mathbb{Z})^n \\ Q_1(\mathbf{a}) \equiv 1 \pmod{4}}} \sum_{\ell=0}^\infty \frac{1}{2^{\ell n}} S_{1,2^\ell}^{\chi(dq')}(\mathbf{0}) &= \sum_{\ell=0}^\infty \frac{1}{2^{\ell n}} \sum_{a \pmod{2^\ell}}^* \sum_{\substack{\mathbf{k} \pmod{2^{2+\ell}} \\ Q_1(\mathbf{k}) \equiv 1 \pmod{4}}} e_{2^\ell}(aQ_2(\mathbf{k})) \\ &= \lim_{\ell \rightarrow \infty} 2^{-\ell(n-1)} \# \left\{ \mathbf{k} \in (\mathbb{Z}/2^{2+\ell}\mathbb{Z})^n : \begin{array}{l} Q_1(\mathbf{k}) \equiv 1 \pmod{4}, \\ Q_2(\mathbf{k}) \equiv 0 \pmod{2^\ell} \end{array} \right\} \\ &= 4^n \times \frac{\sigma_2}{2}, \end{aligned}$$

on carrying out the sum over a and comparing with (8.11). Hence it follows that

$$C = 4^n \times \frac{\sigma_2}{2} \times \tau_\infty(Q_2, W) \sum_{d=1}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{\substack{q'=1 \\ 2 \nmid q'}}^\infty \frac{1}{q'^n} S_{d,q'}(\mathbf{0}).$$

Expressing the sum over d and q' as an Euler product one finds that

$$\sum_{d=1}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{\substack{q'=1 \\ 2 \nmid q'}}^\infty \frac{1}{q'^n} S_{d,q'}(\mathbf{0}) = \prod_{p>2} \sum_{r,\ell \geq 0} \frac{p^r \chi(p^r)}{p^{(r+\ell)n}} S_{p^r,p^\ell}(\mathbf{0}).$$

Here $S_{p^r,1}(\mathbf{0}) = \tilde{N}_r(r)$ and $S_{p^r,p^\ell}(\mathbf{0}) = p^\ell \tilde{N}_{r+\ell}(r) - p^{\ell-1+n} \tilde{N}_{r+\ell-1}(r)$, when $\ell \geq 1$, in the notation of (8.12). It easily follows that

$$\sum_{d=1}^\infty \frac{\chi(d)}{d^{n-1}} \sum_{\substack{q'=1 \\ 2 \nmid q'}}^\infty \frac{1}{q'^n} S_{d,q'}(\mathbf{0}) = \prod_{p>2} \tau_p,$$

with

$$\tau_p = \lim_{k \rightarrow \infty} p^{-k(n-1)} \sum_{0 \leq r \leq k} \chi(p^r) \tilde{N}_k(r) = \left(1 - \frac{\chi(p)}{p} \right)^{-1} \sigma_p.$$

Finally, on appealing to the identity (8.13) and noting that $L(1, \chi) = \pi/4$, we deduce that

$$C = 4^n \times \frac{\sigma_2}{2} \times \tau_\infty(Q_2, W) L(1, \chi) \prod_{p>2} \sigma_p = \frac{4^{n-1}}{2} \times \sigma_\infty \prod_p \sigma_p.$$

Once inserted into (8.10) we therefore arrive at the statement of Lemma 30.

ACKNOWLEDGEMENTS

Some of this work was done while the authors were both visiting the *Institute for Advanced Study* in Princeton, the hospitality and financial support of which is gratefully acknowledged. While working on this paper the first author was supported by EPSRC grant EP/E053262/1. The authors are very grateful to the anonymous referee for numerous helpful comments and for drawing our attention to an error in the original treatment of Lemma 21.

REFERENCES

- Azn80 V. N. Aznar, *On the Chern classes and the Euler characteristic for nonsingular complete intersections*, Proc. Amer. Math. Soc. **78** (1980), 143–148.
- Bir61 B. J. Birch, *Forms in many variables*, Proc. R. Soc. Lond. Ser. A **265** (1962), 245–263.
- BHS06 T. D. Browning, D. R. Heath-Brown and P. Salberger, *Counting rational points on algebraic varieties*, Duke Math. J. **132** (2006), 545–578.
- CSS87a J.-L. Colliot-Thélène, J.-J. Sansuc and P. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces, I*, J. Reine Angew. Math. **373** (1987a), 37–107.
- CSS87b J.-L. Colliot-Thélène, J.-J. Sansuc and P. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces, II*, J. Reine Angew. Math. **374** (1987b), 72–168.
- Coo71 R. J. Cook, *Simultaneous quadratic equations*, J. Lond. Math. Soc. (2) **4** (1971), 319–326.
- Dav63 H. Davenport, *Cubic forms in 16 variables*, Proc. R. Soc. Lond. Ser. A **272** (1963), 285–303.
- Del74 P. Deligne, *La conjecture de Weil. I*, Publ. Math. Inst. Hautes Études Sci. **43** (1974), 273–307.
- Dem56 V. B. Dem'yanov, *Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes*, Izv. Akad. Nauk SSSR. Ser. Mat. **20** (1956), 307–324 (in Russian).
- DFI93 W. Duke, J. B. Friedlander and H. Iwaniec, *Bounds for automorphic L-functions*, Invent. Math. **112** (1993), 1–8.
- Ein86 L. Ein, *Varieties with small dual varieties, I*, Invent. Math. **86** (1986), 63–74.
- GKZ94 I. Gelfand, M. Kapranov and A. Zelevinsky, *Discriminants, resultants, and multidimensional determinants* (Birkhäuser, 1994).
- Hea80 D. R. Heath-Brown, *Hybrid bounds for Dirichlet L-functions, II*, Q. J. Math. **31** (1980), 157–167.
- Hea96 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.
- Hea03 D. R. Heath-Brown, *Linear relations amongst sums of two squares*, in *Number theory and algebraic geometry*, London Mathematical Society Lecture Note Series, vol. 303 (Cambridge University Press, Cambridge, 2003), 133–176.
- Hoo88 C. Hooley, *On nonary cubic forms*, J. Reine Angew. Math. **386** (1988), 32–98.
- Hoo91 C. Hooley, *On the number of points on a complete intersection over a finite field*, J. Number Theory **38** (1991), 338–358.
- IK04 H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society. Colloquium Publications, vol. 53 (American Mathematical Society, Providence, RI, 2004).
- IM10 H. Iwaniec and R. Munshi, *The circle method and pairs of quadratic forms*, J. Théor. Nombres Bordeaux **22** (2010), 403–419.
- Lox00 J. H. Loxton, *Estimates for complete multiple exponential sums*, Acta Arith. **92** (2000), 277–290.
- Rei72 M. Reid, *The complete intersection of two or more quadrics*. PhD thesis, University of Cambridge (1972).
- Smi71 H. J. S. Smith, *Arithmetical notes*, Proc. Lond. Math. Soc. **4** (1873), 236–253.

T. D. Browning t.d.browning@bristol.ac.uk

School of Mathematics, University of Bristol, Bristol, BS8 1TW, UK

R. Munshi rmunshi@math.tifr.res.in

School of Mathematics, Tata Institute of Fundamental Research, 1 Homi Bhabha Road, Colaba, Mumbai 400005, India