LOCAL DENSITIES AND EXPLICIT BOUNDS FOR REPRESENTABILITY BY A QUADRATIC FORM

Jonathan Hanke

§1 Introduction

One of the oldest questions in number theory is the question of when a number m is represented by an integral quadratic form Q in n variables, meaning that $Q(\vec{x}) = m$ for some $\vec{x} \in \mathbb{Z}^n$. In fact, it suffices to answer the question for any form $\widetilde{Q}$ which differs from Q by some invertible integral change of variables, since they represent the same numbers. We call the set of such forms the **class** of Q. To begin to answer this question, people first considered the weaker condition of m being **locally represented** by Q, meaning that m is represented by Q mod p^α for all $\alpha \geq 0$ and also that it is represented over the real numbers $\mathbb{R}$. The condition that m is locally represented by Q leads to finitely many congruence conditions on m. Since these are easy to check, the question then becomes when is some locally represented m actually represented by Q?

However, in general there are finitely many classes of quadratic forms which are locally equivalent to Q (called the **genus** of Q), so local conditions are not enough to determine the numbers represented by Q. To answer this question, one would need to somehow distinguish the class of Q from among these finitely many classes.

The first major quantitative result along these lines was that of Siegel, who gave a description of a certain weighted average of representations by forms in the genus of Q as an infinite product of local factors. He further showed that these averages are the Fourier coefficients of the Eisenstein series appearing in the theta function

$$\Theta_Q(z) = \sum_{m\in\mathbb{Z}} r_Q(m) e^{2\pi i m z}, \tag{1.1}$$

where $r_Q(m)$ denotes the number of representations of m by Q (suitably normalized in the case where the $r_Q(m)$ are infinite). It is this interpretation of the Eisenstein series that allows one to make precise effective statements, provided enough is known about the local factors.

There is a more refined local equivalence one can use which divides the genus into **spinor genera**. It is an amazing fact, again due to Siegel, that his weighted averages above only depend on the spinor genus of Q when $n \geq 4$.

The author would like to thank Ken Ono for suggesting to him that one could obtain an effective bound within a fixed square class when $n = 3$, which is how this project began. The author would also like to thank Manjul Bhargava for many useful conversations and his enduring interest in the case $n = 4$, and Rainer Schulze-Pillot for several helpful comments.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX

In the case where $n \geq 3$ and the form Q is **indefinite**, meaning that it locally represents both positive and negative numbers (over $\mathbb{R}$), one can show that each form in the genus of Q is its own spinor genus. So by Siegel's weighted average result, we have local conditions for the representability of a given number by Q.

If Q is not indefinite, then we say Q is **positive definite** or **negative definite** depending on whether Q represents positive or negative numbers. By replacing Q by $-Q$, we may assume Q is positive definite. In this case, the spinor genus remains a useful notion, but it does not provide as complete of an answer as when Q is indefinite.

In this paper, we seek to give explicit lower bounds for an integer m which ensure that m is represented by a given integral positive definite quadratic form Q in $n \geq 3$ variables. Our main interest is in the cases $n = 3$ and 4, since a reasonable bound in these cases was not previously known and they allow us to compute which (spinor) locally represented numbers are not represented by Q. These bounds also help us to describe the general representation behavior of Q when $n = 3$. In this case, Duke and Schulze-Pillot [Du-SP] showed an ineffective lower bound over $\mathbb{Q}$, avoiding discussion of the primes $p \mid N$ and the spinor exceptional-type square classes. We give an effective version of their result, including an effective asymptotic statement for these square classes. For completeness, we actually give bounds for all $n \geq 3$. In fact, we work quite generally over a totally real number field F and only restrict to $F = \mathbb{Q}$ to avoid mentioning Hilbert modular forms. However, using Hilbert modular forms, our results could easily be extended to any totally real F.

In §2 we introduce some basic facts and notation. In §3 we describe an explicit reduction procedure which helps us to compute the number of solutions $Q(\vec{x}) \equiv m \pmod{\mathfrak{p}^k}$, the main idea being that either Hensel's Lemma applies or we can divide the representation by a power of the local uniformizer $\pi_\mathfrak{p}$. In §4 we review some essential facts about modular forms that we will need, with special attention to the Shimura lift when $n = 3$ where it plays a crucial role because of its close relationship with spinor genera. In §5 we establish explicit lower bounds for the main term of our asymptotic for $r_Q(m)$. When $n \geq 4$ this comes from the Fourier coefficients of an Eisenstein series, while when $n = 3$ there is an additional spinor term which comes into play. In §6 we state our main results, which provide effective lower bounds on m which, when satisfied, guarantee that m is represented by Q. Here our main emphasis is on $n = 3$ and $n = 4$, where such bounds provide theoretically interesting and computationally useful information about the representation behavior of Q respectively. In §7.1 we use the results of §5 to describe the asymptotics of the main term, and in §7.2 we describe how to modify our results find the numbers represented by a quadratic polynomial. In §8 we apply these results to answer affirmatively the long-standing conjecture of Kneser (popularized by Kaplansky) that for $Q = x^2 + 3y^2 + 5z^2 + 7w^2$ the only integers ≥ 0 which fail to be represented are 2 and 22. In §9, for completeness we include some straightforward Gauss sum computations, originally due to Siegel, which are used to understand the generic local factors $\beta_\mathfrak{p}(m)$.

§2 Setup and Notation

We will use the standard notation $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}, p, \mathbb{Q}_v, \mathbb{Z}_v$ to denote the complex numbers, real numbers, rational numbers, rational integers, natural numbers, a positive prime number, the completion of $\mathbb{Q}$ at the valuation v, and ring of integers in $\mathbb{Q}_v$.

Similarly, we let $F, \mathfrak{o}_F, \mathfrak{p}, F_v, \mathfrak{o}_v$ denote a totally real number field, its ring of integers, a prime ideal in $\mathfrak{o}_F$, the completion of F at the valuation v, and the ring of integers in F_v. We note that if v is archimedian then $\mathfrak{o}_v = F_v$. We also let $q = N_{F/\mathbb{Q}}(\mathfrak{p}) = \#(\mathfrak{o}_F/\mathfrak{p})$ and $\pi_\mathfrak{p}$ denote a choice of uniformizer at $\mathfrak{p}$. When discussing divisibility we may abuse notation slightly, writing $\mathfrak{p} \mid m$ when strictly speaking we should write $\pi_\mathfrak{p} \mid m$. We denote by $\mathbb{A}_F$ and $\mathbb{A}_F^\times$ respectively the adeles and ideles of F, and let $\mathbb{A}_{\mathfrak{o}_F} = \prod_v \mathfrak{o}_v$.

We abbreviate $e^{2\pi i z}$ as $\mathbf{e}(z)$, let $\mathbb{C}^1$ denote the unit circle in $\mathbb{C}$, and let μ_N denote the N^{th} roots of unity. We also write $a \mid b$, $\gcd\{x_i\}$, $\operatorname{lcm}\{x_i\}$, $\lfloor x \rfloor$, $\tau(m)$, $\sigma(m)$, $\varphi(m)$, $\mu(m)$ for a divides b, the greatest common divisor and least common multiple of finitely many numbers x_i, the greatest integer $\leq x$, the number of positive divisors of m, the sum of the positive divisors of m, the Euler phi and Möebuis function, respectively. We write $k >> 1$ to mean k is sufficiently large (i.e., there is some positive constant M such that the following statements are true when $k > M$).

If $\vec{x} \in \mathbb{Z}^n$ and P is a partition of $\{1, \cdots, n\}$, then for each $j \in P$ we let $\vec{x_j}$ denote the vector whose components are x_i for all $i \in j$. Similarly, for any $\mathbb{S} \subseteq P$ we take $\vec{x_\mathbb{S}}$ to be the vector whose components are x_i for all $i \in \cup_{j \in \mathbb{S}} j$. Implicit in this notation is a fixed ordering of $\mathbb{S}$, which we always take to be the natural ordering on $\{1, \cdots, n\}$.

Throughout this paper we will be considering an integral totally definite quadratic form Q of dimension n over F, by which we mean a function

$$Q(\vec{x}) = \sum_{i,j=1}^{n} c_{ij} x_i x_j, \qquad \text{with } c_{ij} = c_{ji} \in F \tag{2.1}$$

such that $Q(\vec{x}) \in \mathfrak{o}_F$ for all $\vec{x}$ in some fixed $\mathfrak{o}_F$-lattice L of rank n, and for which $Q(F_v) \subseteq \mathbb{R}$ is either ≥ 0 or ≤ 0 (but not both) for all archimedian places v of F. Since L is locally free, at each place v of F we may choose a local basis $\{y_i\}$ so that

$$L = \sum_{i=1}^{n} \mathfrak{o}_v \, y_i. \tag{2.2}$$

In this basis we may represent Q by a matrix Q_v as in (2.1) (denoted as $Q_\mathfrak{p}$ if v corresponds to $\mathfrak{p}$). At every non-archimedian place corresponding to $\mathfrak{p}$, we may use Lemma 1.1 below to write Q in the local normalized form

$$Q(\vec{x}) \underset{\mathfrak{o}_\mathfrak{p}}{\cong} \sum_j \pi_\mathfrak{p}^{\nu_j} Q_j(\vec{x_j}) \tag{2.3}$$

with $\dim(Q_j) \leq 2$. When $\mathfrak{p} \nmid 2$ we have $\dim(Q_j) = 1$, and when v is archimedian, we may take $Q \underset{\mathbb{R}}{\cong} \sum_{i=1}^{n} x_i^2$.

Lemma 2.1. *Over $\mathfrak{o}_\mathfrak{p}$ we may locally write the integral quadratic form Q as a direct sum of forms $\pi_\mathfrak{p}^{\nu_j} Q_j$ where either $Q_j(x) = ux^2$ for some $u \in \mathfrak{o}_\mathfrak{p}^\times$ or $Q_j(x, y) = ax^2 + bxy + cy^2$ with $b \in \mathfrak{o}_\mathfrak{p}^\times$, $a, c \in \mathfrak{o}_\mathfrak{p}$, and $ord_\mathfrak{p}(a) = ord_\mathfrak{p}(c)$. If $\mathfrak{p} \nmid 2$ then the Q_j appearing are all 1-dimensional.*

Proof. Follwing the method in [C-S, pp369–70] we consider the symmetric matrix of the bilinear form associated to Q with half-integral entries and integral diagonal.

If the least $\mathfrak{p}$ divisible entry is on the diagonal, then by elementary symmetric row-column operations we may clear its row and column isolating it as a direct summand. If the (strictly) least $\mathfrak{p}$ divisible entry is not on the diagonal, we may reorder our variables so that it is adjacent to the diagonal. Since Q is integral, this gives an upper left 2×2 submatrix of the form $\begin{bmatrix} \pi_{\mathfrak{p}}^{\nu}\alpha & \pi_{\mathfrak{p}}^{\nu}\beta \\ \pi_{\mathfrak{p}}^{\nu}\beta & \pi_{\mathfrak{p}}^{\nu}\gamma \end{bmatrix}$ with $\beta \in \frac{1}{2}\mathfrak{o}_{\mathfrak{p}}^{\times}$ and $\alpha, \gamma \in \mathfrak{p}\mathfrak{o}_{\mathfrak{p}}$. Further, since the determinant $\alpha\gamma - \beta^2$ is in $\frac{1}{4}\mathfrak{o}_{\mathfrak{p}}^{\times}$, these form a basis for the $\mathfrak{o}_{\mathfrak{p}}$-module $\frac{1}{2}\mathfrak{o}_{\mathfrak{p}}$ and we may clear the two associated rows and columns as above to isolate it as a direct summand. If $\mathfrak{p} \nmid 2$ or $\mathrm{ord}_{\mathfrak{p}}(\alpha) > \mathrm{ord}_{\mathfrak{p}}(\gamma)$, we may add the second row-column to the first, replacing α by $\alpha + 2\beta + \gamma$. When $\mathfrak{p} \nmid 2$ this reduces us to the diagonal case, and when $\mathfrak{p} \mid 2$ this ensures $\mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\gamma)$. Passing to the associated quadratic form gives the desired normalized form for Q with $a = \alpha$, $b = 2\beta$, and $c = \gamma$ in the 2×2 blocks. $\square$

We now define the determinant $D = D_Q$ and level $N = N_Q$ of Q. We take D_Q to be the fractional ideal of F generated locally at each prime $\mathfrak{p}$ by the elements $D_{Q,\mathfrak{p}} = D_{\mathfrak{p}} = \det(Q_{\mathfrak{p}})$, and N_Q as the least ideal $N_{\mathfrak{p}} \subseteq \mathfrak{o}_{\mathfrak{p}}$ so that $N_{\mathfrak{p}}(2Q_{\mathfrak{p}})^{-1}$ is a matrix of integral ideals whose diagonal entries lie in $2\mathfrak{o}_F$. When the class number of F is 1 (e.g. $F = \mathbb{Q}$), we may choose a global basis for L in which case we can take $D_Q = \det(Q)$ as an element of F, which is unique up to multiplication by ${\mathfrak{o}_F}^{\times}$. When $F = \mathbb{Q}$ we will understand D_Q to be such an element. We also let $\mathrm{Gen}(Q)$ and $\mathrm{Spn}(Q)$ denote the genus and spinor genus of Q respectively.

Since in general D_Q is not an integral ideal, it is often more convenient to discuss its integrality properites in terms of D_{2Q}. However, N_Q is always an integral ideal.

Lemma 2.2. *Let Q be an integral quadratic form over a number field F. Then*

$$\mathfrak{p} \mid N_Q \iff \mathfrak{p} \mid D_{2Q} \iff \begin{array}{l} \text{for some } j \text{ either } \nu_j \geq 1 \\ \text{or } \mathfrak{p}|2 \text{ and } \dim(Q_j) = 1, \end{array}$$

where N_Q and D_Q are respectively the level and determinant of Q, and for each prime ideal $\mathfrak{p}$ of F we define the ν_j as in (2.3) above.

Proof. From the local normal form (2.3) and Lemma 2.1, we see that

$$\mathrm{ord}_{\mathfrak{p}}(D_{2Q,\mathfrak{p}}) = \sum_j \lambda'_j \quad \text{where} \quad \lambda'_j = \begin{cases} \nu_j + \mathrm{ord}_{\mathfrak{p}}(2) & \text{if } \dim(Q_j) = 1, \\ \nu_j & \text{if } \dim(Q_j) = 2, \end{cases} \tag{2.4}$$

and

$$\mathrm{ord}_{\mathfrak{p}}(N_{\mathfrak{p}}) = \max_j\{\lambda''_j\} \quad \text{where} \quad \lambda''_j = \begin{cases} \nu_j + 2\,\mathrm{ord}_{\mathfrak{p}}(2) & \text{if } \dim(Q_j) = 1, \\ \nu_j & \text{if } \dim(Q_j) = 2. \end{cases} \tag{2.5}$$

Our Lemma follows by using these formulas to check when $\mathrm{ord}_p(\cdot) \geq 1$. $\square$

We say that an integer $m \in \mathfrak{o}_F$ is **represented** by Q if $Q(\vec{x}) = m$ has a solution with $\vec{x} \in L$, and that m is **locally represented** by Q if it has a solution with $\vec{x} \in L_v$ for all places v of F. A prime $\mathfrak{p}$ is said to be **anisotropic** (resp. **isotropic**) with respect to Q when Q is anisotropic (resp. isotropic) over $\mathfrak{o}_{\mathfrak{p}}$. We often omit the explicit mention of Q when our meaning is clear.

For $m \in \mathbb{Z}$ we let $(m)_{\mathbb{S}}$ denote the maximal positive divisor of m divisible only by primes $p \in \mathbb{S}$. For $m \in \mathfrak{o}_F$, we let $N_{F/\mathbb{Q}}(m)_{\mathbb{S}}$ denote the norm of the maximal integral ideal dividing $m\mathfrak{o}_F$ divisible only by primes $\mathfrak{p} \in \mathbb{S}$. We let *Iso* and *Aniso* respectively denote the set of isotropic and anisotropic primes of F. We also say that $m \in \mathfrak{o}_F$ is **supported** on some set $\mathbb{S}$ of primes when $|m|_\mathfrak{p} = 1$ for all $\mathfrak{p} \notin \mathbb{S}$, and take $m \to \infty_\mathbb{S}$ to mean $m \to \infty$ in such a way that $\mathrm{ord}_\mathfrak{p}(m) \to \infty$ for all $\mathfrak{p} \in \mathbb{S}$.

We define

$$R_Q(m) = \{\vec{x} \in L \mid Q(\vec{x}) = m\}$$
$$R_{\mathfrak{p}^k,Q}(m) = \{\vec{x} \in L/\mathfrak{p}^k L \mid Q(\vec{x}) \equiv m \pmod{\mathfrak{p}^k}\}$$

and let $r_Q(m) = \#R_Q(m)$, $r_{\mathfrak{p}^k,Q}(m) = \#R_{\mathfrak{p}^k,Q}(m)$. Solutions (mod $\mathfrak{p}^k$) satisfying additional congruence conditions are denoted as above with the relevant conditions as a superscript (e.g., $R^{Good}_{\mathfrak{p}^k,Q}(m)$, $r^{Good}_{\mathfrak{p}^k,Q}(m)$, etc.). We adopt the convention that $\vec{x}_\mathbb{S} \equiv \vec{0} \mod \mathfrak{p} \iff$ either $\mathbb{S} = \emptyset$ or $\mathbb{S} \neq \emptyset$ and $\vec{x}_\mathbb{S} \equiv \vec{0} \mod \mathfrak{p}$. Therefore $\vec{x}_\mathbb{S} \not\equiv \vec{0} \mod \mathfrak{p}$ implies $\mathbb{S} \neq \emptyset$ and $\vec{x}_\mathbb{S} \not\equiv \vec{0} \mod \mathfrak{p}$. When our meaning is clear, we often omit the subscript Q to simplify our notation.

For $a \in \mathfrak{o}_F$ we let $\left(\frac{a}{\mathfrak{p}}\right) = \pm 1$ denote the usual Legendre symbol given by $a^{\frac{q-1}{2}} \mod \mathfrak{p}$. When $F = \mathbb{Q}$, we let $\left(\frac{a}{b}\right)$ denote the quadratic residue symbol defined in [Sh, pp442–3], where the sign of a determines the parity of the character $\left(\frac{a}{\cdot}\right)$. For a Dirichlet character ϕ, we define its twist $\phi_{(u)}(\cdot) = \phi(\cdot)\left(\frac{-u}{\cdot}\right)$ by $-u$.

For any fixed $u \in \mathfrak{o}_F$ we let Φ_n denote a Hecke character on F defined for all primes $\mathfrak{p} \nmid 2N$ by

$$\Phi_n(\mathfrak{p}) = \Phi_n(\mathfrak{p}, u) = \begin{cases} \left(\frac{(-1)^{\frac{n}{2}} D_\mathfrak{p}}{\mathfrak{p}}\right) & \text{if } n \text{ is even,} \\ \left(\frac{(-1)^{\frac{n-1}{2}} D_\mathfrak{p} u}{\mathfrak{p}}\right) & \text{if } n \text{ is odd.} \end{cases}$$

When n is odd the extra 2 is unnecessary since N is already even. Also, when the class number of F is 1 (e.g. $F = \mathbb{Q}$) we may replace the local $D_\mathfrak{p}$ by D, in which case Φ_n is just a quadratic Dirichlet character.

We define the spaces of modular forms $M_k(N, \phi)$ and $S_k(N, \phi)$ of weight k, level N and character ϕ. If $k \in \mathbb{Z} + \frac{1}{2}$ then these are defined as in [Sh, pp443–4] (however his subscript is twice ours). There is a natural (Petersson) inner product on $M_k(N, \phi)$ given by

$$< f, g >= \frac{1}{\mathrm{Vol}(\mathcal{H}/\Gamma_0(N))} \int_{\mathcal{H}/\Gamma_0(N)} f(z)\overline{g(z)}\, y^k \frac{dx dy}{y^2},$$

assuming that the product fg is a cusp form. (We always assume $y^{1/2} > 0$.)

Warning: We will often speak about a **square class** $T\mathbb{Z}^2$, $T\mathfrak{o}_F{}^2$, or $T(\mathbb{A}_{\mathfrak{o}_F})^2$, however this is an abuse of notation since our meaning is to allow all *non-zero* square multiples of T. Therefore, to be precise we should write $T(\mathbb{Z} - \{0\})^2$, $T(\mathfrak{o}_F - \{0\})^2$, or $T\prod_v(\mathfrak{o}_v - \{0\})^2$ respectively.

§3 Reduction maps

We begin by giving a recursive procedure to compute the number of representations $r_{\mathfrak{p}^k,Q}(m)$ for $k >> 1$ using Hensel's Lemma and 3 reduction maps. This will be useful later for understanding the behavior of the local factors $\beta_{\mathfrak{p}}(m)$ appearing in Siegel's product formula, and will allow us to obtain explicit lower bounds for the growth of the Fourier coefficients of the Eisenstein series $E(z)$ within a square class. A simpler version of our approach can be found in [M-H, pp51–3].

Throughout this section, we fix a prime $\mathfrak{p}$ of F and assume $Q = Q_{\mathfrak{p}}$ is of the form (2.3). We also implicitly use the letter j to index the forms $\pi_{\mathfrak{p}}^{\nu_j} Q_j$ and the vectors $\vec{x_j}$ appearing there.

Definition 3.1. We say that $\vec{x} \in R_{\mathfrak{p}^k,Q}(m)$ is of **Zero-type** if $\vec{x} \equiv \vec{0} \bmod \mathfrak{p}$, of **Good-type** if $\pi_{\mathfrak{p}}^{\nu_j} \vec{x_j} \not\equiv \vec{0} \bmod \mathfrak{p}$ for some j, and of **Bad-type** otherwise. The set of all such $\vec{x}$ are denoted respectively by $R^{Zero}_{\mathfrak{p}^k,Q}(m)$, $R^{Good}_{\mathfrak{p}^k,Q}(m)$, and $R^{Bad}_{\mathfrak{p}^k,Q}(m)$ (which have sizes $r^{Zero}_{\mathfrak{p}^k,Q}(m)$, $r^{Good}_{\mathfrak{p}^k,Q}(m)$, and $r^{Bad}_{\mathfrak{p}^k,Q}(m)$).

Our definition of Good-type solutions was motivated by the following property:

Lemma 3.2. *We have*

$$r^{Good}_{\mathfrak{p}^{k+l},Q}(m) = q^{(n-1)l} r^{Good}_{\mathfrak{p}^k,Q}(m), \tag{3.1}$$

for all $k \geq 2\, ord_{\mathfrak{p}}(2) + 1$.

Proof. Suppose $\vec{x}$ is a Good-type solution to $Q(\vec{x}) \equiv m \pmod{\mathfrak{p}^k}$, so $\pi_{\mathfrak{p}}^{\nu_j} \vec{x_j} \not\equiv 0$ mod $\mathfrak{p}$ for some j. We choose an arbitrary lift (mod $\mathfrak{p}^{k+l}$) for the variables outside $\vec{x_j}$ and collect all terms outside Q_j together, writing them as m'.

If $\dim(Q_j) = 1$ then we wish to solve $ux^2 \equiv m' \bmod \mathfrak{p}^{k+l}$ with $x \equiv x_j \bmod \mathfrak{p}^k$. By Hensel's Lemma such a solution exists when $k \geq 2\,\mathrm{ord}_{\mathfrak{p}}(2) + 1$, and it is clearly unique.

If $\dim(Q_j) = 2$ then we wish to apply Hensel's Lemma as above to $f = ax^2 + bxy + cy^2$ after choosing an arbitrary lift of one of the coordinates, say y. To meet the criterion of Hensel's Lemma, we must find some coordinates in which $\frac{\partial f}{\partial x}(\vec{x_j}) \not\equiv 0$, which is to say that f is non-singular at $\vec{x_j}$ (mod $\mathfrak{p}$). Checking when both partials vanish, we see that the only possible singular point is $\vec{x_j} \equiv (0,0)$, which contradicts our assumption that $\vec{x}$ is of Good-type. Since b is a unit, we may even lift these solutions when $k = 1$. □

Let $\vec{x}$ denote a general solution of a given type. We now describe several reduction maps useful for understanding the number of solutions of each type, allowing the possibility that $\vec{x}$ satisfies additional congruence conditions of the form $\vec{x_j} \equiv \vec{0}$ or $\vec{x_j} \not\equiv \vec{0} \pmod{\mathfrak{p}}$ for each j so long as these extra conditions are not implied or contradicted by the reduction-type congruence conditions on $\vec{x}$. If such conditions on $\vec{x_j}$ are allowed for all $j \in \mathbb{S}$, we denote them by $\vec{x}_{\mathbb{S}} \in C$.

Good-type Solutions: For these we have the map

$$R^{Good,\, \vec{x}\in C}_{\mathfrak{p}^k}(m) \xrightarrow{\pi_G} R^{Good,\, \vec{x}\in C}_{\mathfrak{p}^{k-1}}(m)$$

defined by reducing $\vec{x}$ mod $\mathfrak{p}^{k-1}$. By Lemma 2.1 this is surjective with multiplicity q^{n-1}, so the number of Good-type solutions can be computed explicitly either from the mod $\mathfrak{p}$ solutions (if $\mathfrak{p} \nmid 2$) or from the solutions mod $4\mathfrak{p}$ (if $\mathfrak{p} \mid 2$).

Zero-type Solutions: These solutions are characterized by the congruence $\vec{x} \equiv \vec{0}$ mod $\mathfrak{p}$, thus arise only when $\mathfrak{p}^2 \mid m$. Reduction of these solutions depends on the map

$$R^{Zero}_{\mathfrak{p}^k}(m) \xrightarrow{\pi_Z} R_{\mathfrak{p}^{k-2}}(m/\pi_{\mathfrak{p}}^2)$$

defined by $\vec{x} \mapsto \vec{x}'' = \frac{1}{\pi_\mathfrak{p}}\vec{x} \mod \mathfrak{p}^{k-2}$. This is well-defined since $\frac{1}{\pi_\mathfrak{p}}\vec{x}$ is defined modulo $\mathfrak{p}^{k-1}$.

We observe that π_Z is surjective with multiplicity q^n since the elements $\vec{x}' \bmod \mathfrak{p}^{k-1}$ which reduce to a fixed $\vec{x}''$ are in 1-to-1 correspondence with $\pi_Z^{-1}(\vec{x}'')$ under $\vec{x} = \pi_\mathfrak{p}\vec{x}'$, and there are q^n such $\vec{x}'$.

Bad-type Solutions: These arise only when $\mathfrak{p} \mid m$. To describe their reduction we define

$$\mathbb{S}_0 = \{j \mid \nu_j = 0\}, \qquad \mathbb{S}_1 = \{j \mid \nu_j = 1\}, \qquad \mathbb{S}_2 = \{j \mid \nu_j \geq 2\},$$

and let $s_i = \sum_{j\in\mathbb{S}_i} \dim(Q_j)$. Then the Bad-type solutions are characterized by the (mod $\mathfrak{p}$) congruences $\vec{x} \not\equiv \vec{0}$ and $\vec{x}_{\mathbb{S}_0} \equiv \vec{0}$. We will have two reduction maps $\pi_{B'}$ and $\pi_{B'}$ which respectively correspond to division by $\pi_\mathfrak{p}$ and division by $\pi_\mathfrak{p}^2$. In the process, we introduce two auxiliary forms Q' and Q'' whose data is denoted with a $'$ or $''$ accordingly. For these we have $Q_j = Q'_j = Q''_j$ for all j.

Bad-type I: Division by $\pi_\mathfrak{p}$ is appropriate for the case when $\mathbb{S}_1 \neq \emptyset$ and $\vec{x}_{\mathbb{S}_1} \not\equiv \vec{0}$. Then we have the map

$$R^{Bad,\, \vec{x}_{\mathbb{S}_1}\not\equiv\vec{0},\, \vec{x}_{\mathbb{S}_1\cup\mathbb{S}_2}\in C}_{\mathfrak{p}^k,Q}(m) \xrightarrow{\pi_{B'}} R^{Good,\, \vec{x}_{\mathbb{S}_1\cup\mathbb{S}_2}\in C}_{\mathfrak{p}^{k-1},Q'}(m/\pi_\mathfrak{p})$$

defined for each index j by

$$\begin{aligned} \vec{x_j} \mapsto \tfrac{1}{\pi_\mathfrak{p}}\vec{x_j}, \quad \nu'_j &= \nu_j + 1 \qquad \text{if } j \in \mathbb{S}_0, \\ \vec{x_j} \mapsto \vec{x_j}, \quad \nu'_j &= \nu_j - 1 \qquad \text{if } j \notin \mathbb{S}_0, \end{aligned}$$

which is surjective with multiplicity $q^{s_1+s_2}$ since we are free to choose lifts of the components of the image at $\mathbb{S}_1 \cup \mathbb{S}_2$.

Bad-type II: Division by $\pi_\mathfrak{p}^2$ is appropriate for the remaining case where either $\mathbb{S}_1 = \emptyset$ or $\vec{x}_{\mathbb{S}_1} \equiv \vec{0}$, and can occur only when $\mathbb{S}_2 \neq \emptyset$. In this case, we define the map

$$R^{Bad,\, \vec{x}_{\mathbb{S}_1}\equiv\vec{0},\, \vec{x}_{\mathbb{S}_2}\in C}_{\mathfrak{p}^k,Q}(m) \xrightarrow{\pi_{B''}} R^{\vec{x}_{\mathbb{S}_2}\not\equiv\vec{0},\, \vec{x}_{\mathbb{S}_2}\in C}_{\mathfrak{p}^{k-2},Q''}(m/\pi_\mathfrak{p}^2)$$

given componentwise by

$$\begin{aligned} \vec{x_j} \mapsto \tfrac{1}{\pi_\mathfrak{p}}\vec{x_j}, \quad \nu''_j &= \nu_j \qquad \text{if } j \in \mathbb{S}_0 \cup \mathbb{S}_1, \\ \vec{x_j} \mapsto \vec{x_j}, \quad \nu''_j &= \nu_j - 2 \qquad \text{if } j \in \mathbb{S}_2, \end{aligned}$$

which is surjective and has multiplicity $q^{2n-s_0-s_1}$. To see this, notice that the map is q-to-1 over the $\mathbb{S}_0\cup\mathbb{S}_1$ components by the same reasoning as for π_Z, and is q^2-to-1 over the $\mathbb{S}_2$ components since the inverse map there corresponds to multiplication by $\pi_\mathfrak{p}^2$.

Definition 3.3. We define the **depth** of each type of solution (i.e., Good, Zero, Bad) of $R_{\mathfrak{p}^k,Q}(m)$ to be the maximal difference $k - k'$ for any $\vec{x} \in R_{\mathfrak{p}^k,Q}(m)$ to be mapped into $R_{\mathfrak{p}^{k'},\widehat{Q}}(\widehat{m})$ under consecutive application of the respective type of maps π_G, π_Z, and $\pi_{B^*} \in \{\pi_{B'}, \pi_{B''}\}$ (for some $\widehat{Q}$ and $\widehat{m}$).

Lemma 3.4. *Suppose Q is an integral quadratic form over F, $\mathfrak{p}$ is prime ideal in $\mathfrak{o}_F$, and $m \in \mathfrak{o}_F$. Then for $k >> 1$ we can compute $r_{\mathfrak{p}^k,Q}(m)$ recursively in terms of solutions mod $\mathfrak{p}$ (or $4\mathfrak{p}$ if $\mathfrak{p} \mid 2$) using the maps π_G, π_Z, $\pi_{B'}$, and $\pi_{B''}$. In fact, the Good, Zero, and Bad-type depths of $R_{\mathfrak{p}^k,Q}(m)$ are bounded by k, $ord_{\mathfrak{p}}(m)$, and $ord_{\mathfrak{p}}(N)+1$ respectively, where N is the level of Q.*

Proof. By definition, the maps π_G and $\pi_{B'}$ give Good-type solutions. The map π_Z gives all types of solutions, which may be broken down into Good, Zero, and Bad-type solutions. The image of the map $\pi_{B''}$ is less clear, but can be written as

$$R_{\mathfrak{p}^{k-2},Q''}^{\vec{x}_{\mathbb{S}_2}\not\equiv\vec{0},\, \vec{x}_{\mathbb{S}_2}\in C}(m/\pi_{\mathfrak{p}}^2) = R_{\mathfrak{p}^{k-2},Q''}^{\vec{x}_{\mathbb{S}_2''}\not\equiv\vec{0},\, \vec{x}_{\mathbb{S}_2}\in C}(m/\pi_{\mathfrak{p}}^2) \cup R_{\mathfrak{p}^{k-2},Q''}^{\vec{x}_{\mathbb{S}_2''}\equiv\vec{0}, \vec{x}_{\mathbb{S}_2-\mathbb{S}_2''}\not\equiv\vec{0},\, \vec{x}_{\mathbb{S}_2}\in C}(m/\pi_{\mathfrak{p}}^2),$$

where $\mathbb{S}_2''$ is the set $\mathbb{S}_2$ with respect to the form Q'' defined above. Each of these terms can be handled recursively by considering Good-type and Bad-type solutions with extra congruence conditions mod $\mathfrak{p}$ of the kind we allow. The Bad-type solutions of the first term can be handled by the maps $\pi_{B'}$ and $\pi_{B''}$ (since the condition $\vec{x}_{\mathbb{S}_2'} \not\equiv \vec{0}$ is trivial in the setting of $\pi_{B''}$), while the Bad-type solutions of the second term only require $\pi_{B'}$. Therefore we are reduced to counting certain types of solutions mod $\mathfrak{p}$ (or mod $4\mathfrak{p}$ if $\mathfrak{p} \mid 2$).

From Lemma 3.2 the Good-type depth is bounded by $k-1$, and the Zero-type depth is clearly bounded by $ord_{\mathfrak{p}}(m)$ since it involves division by $\pi_{\mathfrak{p}}^2$ and if $\vec{x}$ is of Zero-type then $\mathrm{ord}_{\mathfrak{p}}(m) \geq 2$. The Bad-type depth is controlled by largest ν_j in (1.4) since we may have at most $\lfloor \frac{\nu_j}{2} \rfloor$ consecutive maps $\pi_{B''}$ (each with depth 2), and then possibly an additional $\pi_{B'}$ (with depth 1). From (2.5), we see that this is $\leq \max_j\{\nu_j\} + 1 \leq \mathrm{ord}_{\mathfrak{p}}(N) + 1$. $\square$

Remark 3.4.1.

a) When $\pi_{\mathfrak{p}} \nmid m$ then all solutions are of Good-type.

b) When $\pi_{\mathfrak{p}} \nmid N$ then all solutions are of Good-type or Zero-type.

c) From Lemma 3.4, the Bad-type term $r_{\mathfrak{p}^k,Q}^{Bad}(m)$ has depth $\leq \mathrm{ord}_{\mathfrak{p}}(N)+1$. To guarantee the constancy of the Bad-type term as m becomes more $\mathfrak{p}$-divisible, we must assume divisibility of m by an additional $\pi_{\mathfrak{p}}$ so that all of our Good-type solutions count representations of 0 mod $\mathfrak{p}$. Thus our condition for constancy becomes $\mathrm{ord}_{\mathfrak{p}}(m) \geq \mathrm{ord}_{\mathfrak{p}}(N)+2$.

d) Some authors like to speak about *primitive representations* of m, meaning those representations which are not a multiple of a representation of some proper divisor of m. In our terminology, primitive representations are those representations not of Zero-type (see Definition 5.3).

e) For $k >> 1$, we may use Lemma 3.2 together with the reduction maps above to obtain recursion formulas for the number of solutions mod $\mathfrak{p}^k$ in terms of other solutions mod $\mathfrak{p}^k$. The factors associated to the maps π_Z, $\pi_{B'}$, and $\pi_{B''}$ are q^{2-n}, q^{1-s_0}, and $q^{2-s_0-s_1}$ respectively.

Definition 3.5. We say that a number m is **locally represented at $\mathfrak{p}$ (by Q)** if $r_{\mathfrak{p}^k}(m) > 0$ for all $k >> \nu$. Also, we say that m is **locally represented** if it is locally represented at p for all primes $\mathfrak{p}$.

Remark 3.5.1. When $n \geq 3$ and $\mathfrak{p} \nmid N$, every number m is locally represented at $\mathfrak{p}$. In general, to check whether m is locally represented at $\mathfrak{p}$, Lemma 3.4 tells us that it suffices to check locally whether any of the quotients of m by a square factor are represented mod $\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(4N)+2}$ when $\mathfrak{p} \mid N$, and mod $\mathfrak{p}$ when $\mathfrak{p} \nmid N$.

Definition 3.6. We define a number m to be $\mathfrak{p}$**-stable** if m is locally represented ay $\mathfrak{p}$, and for all $k >> \nu$ the quantity

$$r_{\mathfrak{p}^k}^{Good}(\pi_\mathfrak{p}^{2\nu} m) + r_{\mathfrak{p}^k}^{Bad}(\pi_\mathfrak{p}^{2\nu} m)$$

is constant for all $\nu \geq 1$. We further define m to be **stable** if it is $\mathfrak{p}$-stable for all primes $\mathfrak{p}$, and $\mathbb{S}$**-stable** if it is $\mathfrak{p}$-stable for all $\mathfrak{p} \in \mathbb{S}$.

Remark 3.6.1. From Remark 3.4.1(b) we know that all m are $\mathfrak{p}$-stable when $\mathfrak{p} \nmid N$, and using Lemma 3.4 and Remark 3.4.1(c) we see that all $m \in \mathfrak{s}_\mathfrak{p} = \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(N)}$ locally represented at $\mathfrak{p}$ are $\mathfrak{p}$-stable when $\mathfrak{p} \mid N$. Together, these imply that the ideal $\mathfrak{s} = \prod_{\mathfrak{p}|N} \mathfrak{s}_\mathfrak{p} = N\mathfrak{o}_F$ is a **stable ideal** in the sense that m is stable for all locally represented $m \in \mathfrak{s}$.

To do explicit calculations with Lemma 3.2 when $n = 3$ or 4, it is useful to have on hand the number of solutions mod $\mathfrak{p} \nmid 2$ of quadratic forms in ≤ 4 variables provided in Table 1 below. These can be verified by computing the appropriate Gauss sums (see Appendix). If $\mathfrak{p} \mid 2$ then we are interested in the number of solutions mod $4\mathfrak{p}$ which is not as straightforward and so must be computed on a case-by-case basis.

Table 1 - Number of solutions mod $\mathfrak{p}$ when $\mathfrak{p} \nmid 2N$, $u \in (\mathfrak{o}_F/\mathfrak{p})^\times$, and $n \leq 4$:

	$n=1$	$n=2$	$n=3$	$n=4$
$r_\mathfrak{p}(0)$	1	$q + (q-1)\left(\frac{-D_\mathfrak{p}}{\mathfrak{p}}\right)$	q^2	$q^3 + q\,(q-1)\left(\frac{D_\mathfrak{p}}{\mathfrak{p}}\right)$
$r_\mathfrak{p}(u)$	$1 + \left(\frac{D_\mathfrak{p} u}{\mathfrak{p}}\right)$	$q - \left(\frac{-D_\mathfrak{p}}{\mathfrak{p}}\right)$	$q^2 + q\left(\frac{-D_\mathfrak{p} u}{\mathfrak{p}}\right)$	$q^3 - q\left(\frac{D_\mathfrak{p}}{\mathfrak{p}}\right)$

Definition 3.7. We say that a prime $\mathfrak{p}$ is **anisotropic** for Q (or alternatively, that Q is *anisotropic* at $\mathfrak{p}$) if for every vector $\vec{x} \in (F_\mathfrak{p})^n$, we have

$$Q(\vec{x}) = 0 \implies \vec{x} = \vec{0}.$$

If this is not so, we say that a prime $\mathfrak{p}$ is **isotropic** for Q (or alternatively, that Q is *isotropic* at $\mathfrak{p}$). We denote the set of anisotropic (resp. isotropic) primes by *Aniso* (resp. *Iso*), and often omit Q when our meaning is clear.

Lemma 3.8. *Suppose Q is a non-degenerate integral quadratic form over F, $\mathfrak{p}$ is a prime ideal in $\mathfrak{o}_F$, $k >> 1$, and m is $\mathfrak{p}$-stable with $\mathfrak{p} \mid m$. Then*

$$Q \textit{ is anisotropic at } \mathfrak{p} \iff r_{\mathfrak{p}^k,Q}(m) = r_{\mathfrak{p}^k,Q}^{Zero}(m).$$

Proof. Since m is $\mathfrak{p}$-stable and $\mathfrak{p} \mid m$, it suffices to prove the Lemma under the assumption that m is sufficiently $\mathfrak{p}$-divisible, and we assume this in what follows.

($\Rightarrow$) Suppose Q is anisotropic at $\mathfrak{p}$. Then we know $r_{\mathfrak{p}^k,Q}^{Good}(m) = 0$ since by Lemma 3.2 any such solution would lift to a non-zero representation of zero in $\mathfrak{o}_\mathfrak{p}$, hence in $F_\mathfrak{p}$, which do not exist by assumption.

From [OM, pp153, 167–171] (or more clearly [Ca, pp58–9] when $F = \mathbb{Q}$) we know

$$(3.2) \quad Q \text{ is anisotropic at } \mathfrak{p} \iff \begin{cases} -D_\mathfrak{p} \notin (F_\mathfrak{p}^\times)^2 & \text{if } n = 2, \\ c \neq \left(\frac{-1,-D_\mathfrak{p}}{\mathfrak{p}}\right) & \text{if } n = 3, \\ c = \left(\frac{-1,-1}{\mathfrak{p}}\right) \text{ and } D_\mathfrak{p} \in (F_\mathfrak{p}^\times)^2 & \text{if } n = 4, \end{cases}$$

where c is the Hasse invariant of Q at $\mathfrak{p}$. Since the norm residue symbol $\left(\frac{a,b}{\mathfrak{p}}\right)$ depends only on the square classes of a and b over $F_\mathfrak{p}$, we know Q is anisotropic exactly when the form Q'' from the map $\pi_{B''}$ is anisotropic. The form Q' from $\pi_{B'}$ is obtained by multiplying Q by $\pi_\mathfrak{p}$, then changing the $\mathbb{S}_1 \cup \mathbb{S}_2$ coefficients within a square class by dividing by $\pi_\mathfrak{p}^2$. Since multiplication by $\pi_\mathfrak{p}$ doesn't change the anisotropicity of Q, we see that if Q is anisotropic, then so are the Q', Q'' arising from it.

Using $\pi_{B'}$ and $\pi_{B''}$, the Bad-type solutions can be computed recursively in terms of (finitely many) $r^{Good}_{p^k,\widetilde{Q}}(\widetilde{m})$ for some $\widetilde{Q}$ and $\widetilde{m}$. However m is assumed to be highly $\mathfrak{p}$-divisible and the Bad-type depth is bounded independently of m, so each of the $r^{Good}_{p^k,\widetilde{Q}}(\widetilde{m})$ must be zero which guarantees there are no Bad-type solutions. Hence $r_{\mathfrak{p}^k,Q}(m) = r^{Zero}_{\mathfrak{p}^k,Q}(m)$.

($\Leftarrow$) Suppose Q is isotropic at $\mathfrak{p}$, so there is some non-zero vector over $F_\mathfrak{p}$ which represents zero. By clearing denominators appropriately we obtain a primitive vector $\vec{x}_0$ over $\mathfrak{o}_\mathfrak{p}$. Then $\vec{x}_0$ mod $\mathfrak{p}^k$ gives a non-Zero-type solution $\vec{x}_1$ in $R_{\mathfrak{p}^k,Q}(0)$. By the reduction procedure mentioned above, we may reduce $\vec{x}_1$ to a Good-type representation $\vec{x}_1^* \in R^{Good}_{\mathfrak{p}^{k^*},Q^*}(0)$ for some auxilliary form Q^*.

Since m is assumed highly $\mathfrak{p}$-divisible we have $R^{Good}_{\mathfrak{p}^{k^*},Q^*}(0) = R^{Good}_{\mathfrak{p}^{k^*},Q^*}(m^*)$ where m^* is obtained by applying the same reduction to m, Lemma 3.2 guarantees the existence of a Good-type representation $\vec{x}_2$ over $F_\mathfrak{p}$ of m^* for $k >> 1$ with $\vec{x}_2 \equiv \vec{x}_1 \equiv \vec{x}_0$ mod $\mathfrak{p}$. By reversing the reduction procedure with $\vec{x}_2$, we obtain a non-Zero-type representation of m by Q. $\square$

Remark 2.8.1. From (3.2) we see that if Q is anisotropic at $\mathfrak{p}$, then $\mathfrak{p} \mid D$. Since Q is anisotropic at $\mathfrak{p} \iff 2Q$ is anisotropic at $\mathfrak{p}$, Lemma 2.2 tells us that all anisotropic primes divide N. Therefore if $\mathfrak{p} \nmid N$ then $\mathfrak{p}$ is isotropic.

Remark 3.9. Due to the very simple nature of our approach, one could equally well use these methods to understand the number of solutions $r_{P,\mathfrak{p}^k}(m)$ of a diagonalizable homogeneous polynomial $P(\vec{x})$ of degree d in n variables, and the associated local factors $\beta_{P,\mathfrak{p}}(m)$ as in (5.2). In particular, one can describe $r_{P,\mathfrak{p}^k}(m)$ in terms of Good-type, Zero-type, and Bad-type solutions, however the reduction procedure for Bad-type solutions will involve d reduction maps $\pi_B^{(l)}$ corresponding to the d possible divisions of $\vec{x}$ by powers $\pi_\mathfrak{p}^l$ with $1 \leq l \leq d$. However, the definitions of stability can be made exactly as in the quadratic case, and they lead to a simple description of the growth of the local factor $\beta_{P,\mathfrak{p}}(m\pi_\mathfrak{p}^{d\nu})$ when m is $\mathfrak{p}$-stable. Generalizations of Siegel-type results to forms of higher degree have been studied by Igusa [Ig].

§4 Modular forms

Throughout this section we take $F = \mathbb{Q}$ and assume that $n \geq 3$.

Our interest in modular forms stems from the fact that the theta function $\Theta_Q(z)$ is known to be a modular form of weight $n/2$ on $\Gamma_0(N)$ for some quadratic character χ (see [An-Zh, Thrm 2.2, p61]). When $n = 3$ the Shimura lift will play a key role in our analysis, so we make some related definitions before proceeding.

Definition 4.1. Suppose $n \geq 3$ is odd. For $f(z) = \sum_{m=1}^{\infty} a(m)\mathbf{e}(mz) \in S_{n/2}(N,\chi)$ and some fixed square free integer $t > 0$ we define its **Shimura lift** $Shi(f) =$

$Shi(f,t)$ following [Sh, p441] to be the modular form $g(z) = \sum_{m=0}^{\infty} b(m)\boldsymbol{e}(mz) \in M_{n-1}(N/2, \chi^2)$ satisfying

$$\sum_{m_0=1}^{\infty} b(m_0)m_0^{-s} = L(s - \tfrac{n-3}{2}, \Phi_n) \sum_{m_0=1}^{\infty} a(tm_0^2)m_0^{-s}. \tag{4.1}$$

Notice that since n is odd the character Φ_n depends on t, and that χ^2 is the trivial character since χ is quadratic. Additionally, Shimura showed that $Shi(f)$ is actually a cusp form when $n \geq 5$.

Remark. This definition agrees with Shimura's since for odd n we have $\chi(\cdot) = \left(\frac{D}{\cdot}\right)$.

We now describe the extent to which the Shimura lift fails to be cuspidal when $n = 3$. Let $U(N,\chi)$ be the subspace of $S_{3/2}(N,\chi)$ spanned by

$$\left\{ u(z) = \sum_{m\in\mathbb{Z}} \psi(m) m \boldsymbol{e}(hm^2 z) \right\} \tag{4.2}$$

where ψ is a primitive Dirichlet character of conductor R with $\psi(-1) = -1$, $\psi = \Phi_3 = \chi_{(h)}$ on $(\mathbb{Z}/N\mathbb{Z})^\times$, $4hR^2 \mid N$ and $h > 0$. Since the character ψ depends only on the square class $t\mathbb{Z}^2$ containing h, we henceforth denote it by ψ_T for any $T \in t\mathbb{Z}^2$. Notice that there are only finitely many $t\mathbb{Z}^2$ on which the Fourier coefficients of $U(N,\chi)$ are non-zero.

It is known (see [Ci, Cor 4.10, p108]) that $U(N,\chi)$ is the subspace of $S_{3/2}(N,\chi)$ whose Shimura lift (for any t) is not cuspidal. We denote by $U^\perp(N,\chi)$ the subspace of $S_{3/2}(N,\chi)$ perpendicular to $U(N,\chi)$ under the Petersson inner product.

Our approach to understanding $\Theta_Q(z)$ is as follows. When $n \geq 4$ we write

$$\Theta_Q(z) = E(z) + f(z) \tag{4.3}$$

as the sum of an Eisenstein series $E(z) = \sum_{m\geq 0} a_E(m)\boldsymbol{e}(mz)$ and a cusp form $f(z)$, and analyze the growth of the Fourier coefficients separately. However when $n = 3$, the situation is complicated by the existence of cusp forms with non-cuspidal Shimura lift, and we write

$$\Theta_Q(z) = E(z) + H(z) + f(z) \tag{4.4}$$

where $H(z) = \sum_{m>0} a_H(m)\boldsymbol{e}(mz) \in U(N,\chi)$ and $f(z) \in U^\perp(N,\chi)$. In this case, we will also be interested in the form $g = Shi(f) \in S_2(N/2)$.

Definition 4.2. When $n = 3$ we say that $m \in t\mathbb{Z}^2$ is **spinor p-stable** at some prime p if $a_H(mp^{2\nu}) = a_H(m)\psi_t(p^\nu)p^\nu$ for all $\nu \geq 0$ with ψ_t as in (4.2), and **spinor stable** if m is spinor p-stable for all primes p. Notice that $\operatorname{lcm}\{h_j \mid h_j \in t\mathbb{Z}^2\}$ is spinor stable. We also say that m is **very p-stable** if it is both p-stable (in the sense of Definition 3.6) and spinor p-stable, and likewise say that m is **very stable** if it is very p-stable at all primes p.

From the work of [Si], [KuRa1-2], [Ra] and [SP2, Satz 2, p291], we may realize the following Fourier coefficients as weighted averages over $\operatorname{Gen}(Q)$ and $\operatorname{Spn}(Q)$ respectively:

$$a_E(m) = \frac{\sum_{Q'\in\operatorname{Gen}(Q)} \dfrac{r_{Q'}(m)}{|\operatorname{Aut}(Q')|}}{\sum_{Q'\in\operatorname{Gen}(Q)} \dfrac{1}{|\operatorname{Aut}(Q')|}} \geq 0, \tag{4.5}$$

$$a_E(m) + a_H(m) = \frac{\sum_{Q' \in \mathrm{Spn}(Q)} \frac{r_{Q'}(m)}{|\mathrm{Aut}(Q')|}}{\sum_{Q' \in \mathrm{Spn}(Q)} \frac{1}{|\mathrm{Aut}(Q')|}} \geq 0. \tag{4.6}$$

In fact, Kneser [Kn] (when Q is indefinite) and Hsia [Hs] (more generally) have shown that $\mathrm{Gen}(Q)$ splits into two half genera consisting of equal numbers of spinor genera, and that $a_E(m) + a_H(m)$ is the same for all spinor genera in a given half genus. By comparing (4.5) and (4.6), we see that $H(z)$ changes sign as we switch between these half genera.

Definition 4.3. For convenience, if t is square free and there is some $m \in t\mathbb{Z}^2$ with $a_H(m) \neq 0$, then we say that $t\mathbb{Z}^2$ is a **spinor square class** because of its close connection with the spinor genera in the genus of Q.

We also say that a locally represented number m is of **(spinor) exceptional-type** if $a_E(m) = |a_H(m)|$, and **non-exceptional** otherwise. We see that m is of exceptional-type exactly when it is extremal in the sense of Lemma 5.8(a).

Remark. Schulze-Pillot [SP1] has given a complete local characterization of numbers of exceptional-type, extending the sufficient conditions given by Hsia in [Hs].

We will need effective upper bounds for the Fourier coefficients of a normalized newform of weight $\frac{n}{2}$. When n is odd this comes in two parts. Within a square class the Shimura lift gives a good bound, but for square free numbers additional analytic information is needed. Since the state-of-the-art for these square free estimates is constantly changing, we include their precise statement as an assumpton in what follows. When n is even, no assumptions are required.

Assumption 4.4. *Suppose $n \geq 3$ is odd and $f \in S_{n/2}(N, \chi)$ is an eigenform for all Hecke operators T_{p^2} for all $p \nmid N$ and normalized so that $< f, f >= 1$. Then for all square free $t > 0$ we have*

$$|a(t)| < B_{\varepsilon'} t^{\frac{n-1}{4} - \eta + \varepsilon'}$$

for some $\varepsilon' > 0$ and $0 \leq \eta \leq \frac{1}{4}$, and some effective constant $B_{\varepsilon'} > 0$.

As of this writing, the best known exponent is $\eta = \frac{1}{12}$ in [Co-Iw], however the implied constant is probably quite large and has not been made explicit. Even for smaller η, where the constant is probably smaller, the author knows of no results with an explicit constant.

For simplicty, we adopt the following convention for decomposing a cusp form for $\Gamma_0(N)$ as a linear combination of Hecke eigenforms.

If $g(z) = \sum_{m \geq 0} b(m)\mathbf{e}(mz)$ has integral weight k, then we write

$$g(z) = \sum_{i=1}^{r} \gamma_i \, g_i(z) \tag{4.7}$$

where $g_i(z) = \sum_{m=1}^{\infty} b_i(m)\mathbf{e}(mz)$ and the $g_i(z)$ are eigenforms for all T_p with $p \nmid N$ and normalized so that their first non-zero Fourier coefficient is 1. By the theory of newforms [At-Le] and Deligne's bound on Hecke eigenvalues [De] we have $|b_i(m)| \le \tau(m) m^{\frac{k-1}{2}}$, therefore

$$|b(m)| \le \tau(m) m^{\frac{k-1}{2}} \sum_{i=1}^{r} |\gamma_i|. \tag{4.8}$$

If $f(z)$ has half-integral weight $\frac{n}{2}$ with $n \ge 3$ odd, and $f \in U^{\perp}(N,\chi)$ when $n = 3$, then we write $f(z) = \sum_k \delta_k f_k(z)$ where $f_k(z) = \sum_{m=1}^{\infty} a_k(m)\mathbf{e}(mz)$ are Hecke eigenforms for all T_{p^2} with $p \nmid N$ and normalized so that $< f_k, f_k >= 1$. Then $\delta_k Shi(f_k, t) = \gamma_i g_i(z)$ for some i with g_i as in the integral weight case above, so $\gamma_i = \delta_k a_k(t)$. When t is fixed, by Möebuis inversion, this together with Deligne's bound on Hecke eigenvalues and $\tau(m/d) \le \tau(m)$ gives the estimate

$$|a(m)| \le \tau(m_0)^2 m_0^{\frac{n-2}{2}} \sum_{i=1}^{r} |\gamma_i| \tag{4.9}$$

where $m = tm_0^2$. However, as t varies we can use Assumption 4.4 to obtain

$$|a(m)| \le \left(B_{\varepsilon'} \sum_k |\delta_k| \right) t^{\frac{n-1}{4} - \eta + \varepsilon'} \tau(m_0)^2 m_0^{\frac{n-2}{2}}. \tag{4.10}$$

§5 The main term

In this section we establish some exact formulas and precise lower bounds for $a_E(m)$ and $a_E(m) + a_H(m)$ by combining our reduction procedure with Siegel's product formula and results from §4. While we will only need information over $\mathbb{Q}$ for our main results, we initially state and prove a bound for $a_E(m)$ more generally over a totally real number field F, obtaining the lower bound over $\mathbb{Q}$ as a corollary. Precise statements about $a_E(m) + a_H(m)$ over F could be proved similarly by replacing §4 with the analogous facts for Hilbert modular forms.

Following Siegel, for $m \in \mathfrak{o}_F$ and a totally definite integral quadratic form Q defined over F we define the **local representation density** $\beta_v(m)$ at a place v of F by

$$\beta_v(m) = \lim_{U \to \{m\}} \frac{\mathrm{Vol}\,(Q^{-1}(U))}{\mathrm{Vol}(U)}, \tag{5.1}$$

where U is an open neighborhood of $m \in F_v$. (Here we use the usual measure on $\mathbb{R}$, and the Haar measure on $F_\mathfrak{p}$ normalized so that $\mathrm{Vol}(\mathfrak{o}_\mathfrak{p}) = 1$.) The $\beta_v(m)$ give a measure of the number of local solutions of $Q(x) = m$ over F_v. If v is a finite place corresponding to the prime $\mathfrak{p}$ of F, then by reduction mod $\mathfrak{p}^\nu$ we may rewrite $\beta_v(m)$ as

$$\beta_\mathfrak{p}(m) = \lim_{\nu \to \infty} \frac{r_{\mathfrak{p}^\nu}(m)}{q^{(n-1)(\nu-1)}}, \tag{5.2}$$

where $q = N_{F/\mathbb{Q}}(\mathfrak{p})$. When $n \ge 3$, Siegel's product formula ([Si1], [KuRa1-2], [Ra]) states that

$$a_E(m) = \prod_v \beta_v(m) \tag{5.3}$$

where the product runs over all places v of F.

Definition 5.1. For our purposes, it will also be convenient to consider $\beta_{\mathfrak{p}}(m)$ which satisfy certain congruence conditions at $\mathfrak{p}$ (i.e. $\beta_{\mathfrak{p}}^{Good}(m)$, $\beta_{\mathfrak{p}}^{Bad}(m)$, etc.), which are defined by imposing these conditions on $r_{\mathfrak{p}^\nu}(m)$ in (5.2).

Definition 5.2. We say that $m = (m_v)_v \in \mathbb{A}_{\mathfrak{o}_F}$ is **locally represented** by Q when $\beta_v(m_v) \neq 0$ for all places v of F. (This agrees with Definition 3.5 when $m \in \mathfrak{o}_F$.) It is equivalent to saying $a_E(m) = 0$ where $a_E(m)$ is defined by (5.3), and we understand $\beta_v(m)$ to mean $\beta_v(m_v)$. We similarly say that m is **$\mathfrak{p}$-stable** when $m_{\mathfrak{p}}$ is $\mathfrak{p}$-stable, and that m is **stable** if m is $\mathfrak{p}$-stable for all primes $\mathfrak{p}$. We likewise extend our definition for m to be **supported** on some set $\mathbb{S}$ of primes.

Definition 5.3. We say that a representation $\vec{x}$ of m by Q is **$\mathfrak{p}$-primitive** if its image in $R_{Q,\mathfrak{p}^k}(m)$ is not of Zero-type, and we say that $\vec{x}$ is **primitive** if it is $\mathfrak{p}$-primitive for all primes $\mathfrak{p}$. We denote the number of primitive representations of m by Q as $r_Q^*(m)$.

We define $a_E^*(m)$ and $a_E^*(m)+a_H^*(m)$ analogously to (4.5) and (4.6) as weighted averages of $r_Q^*(m)$ over $\mathrm{Gen}(Q)$ and $\mathrm{Spn}(Q)$ respectively. One can similarly prove a primitive product formula

$$a_E^*(m) = \prod_v \beta_v^{Good \,\cup\, Bad}(m) \tag{5.4}$$

using (5.3).

Theorem 5.4. *Let Q be a totally definite integral quadratic form of dimension $n \geq 3$ defined over a totally real number field F. Suppose that $m = T'(m')^2 \in T'{\mathfrak{o}_F}^2$ where T' is $\mathfrak{p}$-stable at all primes $\mathfrak{p} \mid m'$. Then*

$$a_E(m) = a_E(T') \prod_{\substack{\mathfrak{p} \mid m' \\ \mathfrak{p}\ Iso}} \left[C_{\mathfrak{p}}(T') + \frac{1 - C_{\mathfrak{p}}(T')}{q^{(n-2)\nu_{\mathfrak{p}}}} \right] N_{F/\mathbb{Q}}((m')_{Iso})^{n-2},$$

where $\nu_{\mathfrak{p}} = ord_{\mathfrak{p}}(m')$ and $C_{\mathfrak{p}}(T')$ is defined after (5.8) below.

Proof. We proceed by computing the growth of each of the local factors $\beta_v(m)$ separately, and use Siegel's product formula (5.3) to assemble our results.

At a real valuation $v \mid \infty$, Siegel [Si, Hilfssatz 26, pp554–5] has computed

$$\beta_v(m) = \frac{n\,\omega_n\, D^{-\frac{1}{2}}}{2} m^{\frac{n-2}{2}} \tag{5.5}$$

where ω_n is the volume of the n-sphere $\sum_{i=1}^n x_i^2 \leq 1$ in $\mathbb{R}^n$.

At a prime valuation v associated to $\mathfrak{p}$, we give a lower bound for the ratios of local factors within a square class using our reduction formula. In estimating these ratios, we assume $m \in T'{\mathfrak{o}_{\mathfrak{p}}}^2$ for some fixed T', and consider several cases:

m is not $\mathfrak{p}$-stable: In this case, applying the map π_Z for $k >> 1$ gives the weaker inequality

$$\frac{\beta_{\mathfrak{p}}(m\,\pi_{\mathfrak{p}}^2)}{\beta_{\mathfrak{p}}(m)} = \frac{r_{\mathfrak{p}^k}(m\,\pi_{\mathfrak{p}}^2)}{r_{\mathfrak{p}^k}(m)} \geq \frac{r_{\mathfrak{p}^k}^{Zero}(m\,\pi_{\mathfrak{p}}^2)}{r_{\mathfrak{p}^k}(m)} = \frac{1}{q^{n-2}}. \tag{5.6}$$

$\mathfrak{p}$ anisotropic and m is $\mathfrak{p}$-stable: By Lemma 3.8, $\mathfrak{p}$ is anisotropic iff we have equality in (5.6) above.

$\mathfrak{p}$ isotropic and T' is $\mathfrak{p}$-stable: For convenience, we let $\nu = \mathrm{ord}_\mathfrak{p}(m')$ and let $K = K(T') = \beta_\mathfrak{p}^{Good \cup Bad}(\pi_\mathfrak{p}^2 T')$. By our $\mathfrak{p}$-stability assumption and repeated application of the map π_Z, we have

$$\beta_\mathfrak{p}(m) = K + \frac{K}{q^{n-2}} + \cdots + \frac{K}{q^{(n-2)(\nu-1)}} + \frac{\beta_\mathfrak{p}(T')}{q^{(n-2)\nu}}. \tag{5.7}$$

Therefore

$$\begin{aligned} \frac{\beta_\mathfrak{p}(m)}{\beta_\mathfrak{p}(T')} &= \frac{1}{q^{(n-2)\nu}} + \frac{K}{\beta_\mathfrak{p}(T')} \frac{\left(\frac{1}{q^{n-2}}\right)^\nu - 1}{\frac{1}{q^{n-2}} - 1} \\ &= \frac{(1 - C_\mathfrak{p}) + C_\mathfrak{p}\, q^{(n-2)\nu}}{q^{(n-2)\nu}} \end{aligned} \tag{5.8}$$

where $C_\mathfrak{p} = C_\mathfrak{p}(T') = \frac{q^{n-2}}{q^{n-2}-1} \frac{K}{\beta_\mathfrak{p}(T')}$. Lemma 3.8 tells us that $C_\mathfrak{p} > 0$. $\square$

Remark 5.4.1.

(a) From the proof of Theorem 5.4 and (5.4), we can see that if m is locally represented and $\mathfrak{p}$-stable, then

$$\left.\begin{aligned} \frac{a_E(m\,\pi_\mathfrak{p}^{2\nu})}{q^\nu} &\longrightarrow C_\mathfrak{p}(m)\, a_E(m) \\ \frac{a_E^*(m\,\pi_\mathfrak{p}^{2\nu})}{q^\nu} &\longrightarrow a_E^*(m) \end{aligned}\right\} \quad \text{when } \mathfrak{p} \text{ is isotropic,}$$

monotonically as $\nu \to \infty$, and

$$a_E(m\,\pi_\mathfrak{p}^{2\nu}) = a_E(m) \qquad \text{when } \mathfrak{p} \text{ is anisotropic.}$$

(b) When $\mathrm{ord}_\mathfrak{p}(T') \le 1$ we may easily compute $C_\mathfrak{p}(T')$ since there are no Zero-type or Bad-type solutions. Then

$$C_\mathfrak{p}(T') = \frac{q^{n-2}}{q^{n-2}-1} \frac{\beta_\mathfrak{p}^{Good}(T'\pi_\mathfrak{p}^{2\nu})}{\beta_\mathfrak{p}^{Good}(T')} \tag{5.9}$$

and a short computation with Lemma 9.1 gives the table:

Table 2 - Local constants $C_\mathfrak{p}(T')$ for $\mathfrak{p} \nmid N$ appearing in (5.8)

$C_\mathfrak{p}$ for $\mathfrak{p} \nmid N$	n odd	n even
$\mathfrak{p} \nmid T'$	$\frac{q^{n-2} - q^{\frac{n-3}{2}} \Phi_n(\mathfrak{p})}{q^{n-2}-1}$	$\frac{q^{\frac{n-2}{2}}}{q^{\frac{n-2}{2}} - \Phi_n(\mathfrak{p})}$
$\mathrm{ord}_\mathfrak{p}(T') = 1$	$\frac{q^{n-2}}{q^{n-2}-1}$	$\frac{q^{n-2}}{q^{n-2}-1}$

Theorem 5.5. *Let Q be a positive definite integral quadratic form in 3 variables defined over $\mathbb{Q}$, and suppose that $m = \widetilde{T}\widetilde{m}^2 \in \widetilde{T}\mathbb{Z}^2$ where $\widetilde{T}$ is very p-stable at all primes $p \mid \widetilde{m}$. Then*

$$a_E(m) + a_H(m) = \left[a_E(\widetilde{T}) + \psi_{\widetilde{T}}(\widetilde{m})a_H(\widetilde{T})\right](\widetilde{m})_{Iso}$$
$$+ a_E(\widetilde{T})\left(\widetilde{m}_+ \prod_{p\mid\widetilde{m}_-}\left[p^{\nu_p} + 2\sum_{\mu=0}^{\nu_p-1} p^\mu\right]\prod_{p\mid\widetilde{m}_2}\left[C_p(\widetilde{T})(p^{\nu_p}-1)+1\right] - (\widetilde{m})_{Iso}\right),$$

where $\nu_p = ord_p(\widetilde{m})$, $C_p(\widetilde{T})$ is as in (5.8), and $(\widetilde{m})_{Iso} = \widetilde{m}_+\widetilde{m}_-\widetilde{m}_2$ with $\widetilde{m}_+ = (\widetilde{m})_{\mathbb{S}_+}$, $\widetilde{m}_- = (\widetilde{m})_{\mathbb{S}_-}$, $\widetilde{m}_2 = (\widetilde{m})_{\mathbb{S}_2}$, and

$$\mathbb{S}_+ = \{p \in VStable(\widetilde{T}) \cap Iso \mid \psi_{\widetilde{T}}(p) = 1 \text{ and } p \nmid N\widetilde{T}\},$$
$$\mathbb{S}_- = \{p \in VStable(\widetilde{T}) \cap Iso \mid \psi_{\widetilde{T}}(p) = -1 \text{ and } p \nmid N\widetilde{T}\},$$
$$\mathbb{S}_2 = \{p \in VStable(\widetilde{T}) \cap Iso \mid p \mid N \text{ or } ord_p(\widetilde{T}) \geq 2\}.$$

Proof. To see $\mathrm{VStable}(\widetilde{T}) \cap Iso = \mathbb{S}_+ \sqcup \mathbb{S}_- \sqcup \mathbb{S}_2$, notice that $\psi_{\widetilde{T}}(p) = 0 \implies p \mid N\widetilde{T}$ and also if $\mathrm{ord}_p(\widetilde{T}) = 1$ then $p \mid t$ so $p \mid N$. Thus $(\widetilde{m})_{Iso} = \widetilde{m}_+\widetilde{m}_-\widetilde{m}_2$. By taking $T' = \widetilde{T}$, Theorem 5.4 gives an exact formula for $a_E(m)$. When $n = 3$, Table 2 yields the explicit formulas

(5.10)
$$C_p(\widetilde{T}) + \frac{1 - C_p(\widetilde{T})}{p^\nu} = \frac{1}{p^\nu}\begin{cases} p^\nu & \text{if } p \nmid \widetilde{T} \text{ and } \psi_{\widetilde{T}}(p) = 1, \\ p^\nu + 2\sum_{\mu=0}^{\nu-1} p^\mu & \text{if } p \nmid \widetilde{T} \text{ and } \psi_{\widetilde{T}}(p) = -1, \\ \sum_{\mu=0}^{\nu} p^\mu & \text{if } \mathrm{ord}_p(\widetilde{T}) = 1. \end{cases}$$

Since $\widetilde{T}$ is very p-stable at all $p \mid \widetilde{m}$, we also have $a_H(\widetilde{m}) = \psi_{\widetilde{T}}(\widetilde{m})\, a_H(\widetilde{T})(\widetilde{m})_{Iso}$. Combining these proves the theorem. □

To obtain precise lower bounds for $a_E(m)$, it is useful to notice that

$$\frac{\beta_{\mathfrak{p}}(T'\pi_{\mathfrak{p}}^{2\nu})}{\beta_{\mathfrak{p}}(T')} \geq C'_{\mathfrak{p}}(T') \quad \text{for all } \nu \geq 0, \tag{5.11}$$

where $C'_{\mathfrak{p}}(T') = \min\{1, C_{\mathfrak{p}}(T')\}$. This follows since the ratio is 1 when $\nu = 0$, and approaches $C_{\mathfrak{p}}(T')$ monotonically as $\nu \to \infty$ by Remark 5.4.1(a).

From Table 2 we see that for $n \geq 3$ and $\mathfrak{p} \nmid N$, we have

$$C'_{\mathfrak{p}}(T') = 1 \iff \begin{cases} n = 3, \text{ or} \\ n \geq 4,\ \mathfrak{p} \nmid T',\ \text{and } \Phi_n(\mathfrak{p}) = (-1)^{n-1}. \end{cases} \tag{5.12}$$

Definition 5.6. When $n \geq 4$, for each $T \in \mathfrak{o}_F$ we let **Stable(T)** be the set of all prime ideals $\mathfrak{p}$ in $\mathfrak{o}_F$ such that T is $\mathfrak{p}$-stable. When $n = 3$ and $F = \mathbb{Q}$, for each $T \in \mathbb{Z}$ we let **VStable(T)** be the set of all primes $p \in \mathbb{Z}$ such that T is very p-stable.

Let $\mathcal{T}$ be a finite union of square classes $t(\mathbb{A}_{\mathfrak{o}_F})^2$ with $t \in \mathbb{A}_{\mathfrak{o}_F}$ and $\mathrm{ord}_{\mathfrak{p}}(t) \leq 1$ at all primes $\mathfrak{p}$. By Remark 3.6.1 and Definition 4.2, there is some ideal $\mathfrak{s} \subseteq \mathfrak{o}_F$

such that any locally represented m is stable (resp. very stable when $n = 3$ and $F = \mathbb{Q}$) when $m_\mathfrak{p} \in \mathfrak{s}_\mathfrak{p}$ for all primes $\mathfrak{p}$. By choosing representatives of $\mathcal{T}$ which generate the ideals dividing $\mathfrak{s}$, we can find a minimal (finite) subset $\mathcal{B}_\mathcal{T} \subset \mathcal{T}$ such that any locally represented $m \in \mathcal{T}$ can be written as $m = T'(m')^2$ with $T' \in \mathcal{B}_\mathcal{T}$ and $m' \in \mathbb{A}_{\mathfrak{o}_F}$ supported on Stable(T') (resp. VStable(T')). Without any difficulty, we may also assume that $\prod_v |T'|_v = 1$ for all $T' \in \mathcal{B}_\mathcal{T}$.

Since the ratios of local factors in (5.8) are all non-zero numbers, we know that m is locally represented $\iff$ T' is locally represented. Therefore all $T' \in \mathcal{B}_\mathcal{T}$ are locally represented.

Theorem 5.7. *Let Q be a totally positive definite integral quadratic form of dimension $n \geq 3$ defined over a totally real number field F.*

Also, let $C'_\mathfrak{p}(T') = \min\{1, C_\mathfrak{p}(T')\}$ and let $\mathcal{T} = \bigcup_{t\in\mathbb{T}} t(\mathbb{A}_{\mathfrak{o}_F})^2$ where $\mathbb{T} \subset \mathbb{A}_{\mathfrak{o}_F}$ is a (finite) set of representatives for the locally represented square classes in $\prod_{\mathfrak{p}|N} \mathfrak{o}_\mathfrak{p}$.

a) When $n = 3$, m is locally represented by Q, and $m = T'(m')^2$ for some T' not contained in a spinor square class with m' supported on $\mathbb{S} \subseteq$ Stable(T'), we have the explicit lower bound

$$a_E(m) \geq \Lambda_3(T') N_{F/\mathbb{Q}}((m')_{Iso}),$$

where

$$\Lambda_3(T') = a_E(T') \prod_{\substack{\mathfrak{p}\in\mathbb{S},\, \mathfrak{p}|N \\ \mathfrak{p}\, Iso}} C'_\mathfrak{p}(T')$$

with $C'_\mathfrak{p}(T')$ defined as in (5.11).

Moreover, if we have an effective estimate $L_F(1,\psi_t) \geq C_\varepsilon N_{F/\mathbb{Q}}(t)^{-\varepsilon}$ for some $\varepsilon > 0$ with $C_\varepsilon > 0$ as t runs over square free $t \in \mathfrak{o}_F > 0$, then we have

$$a_E(m) \geq \widehat{\Lambda}_3\, N_{F/\mathbb{Q}}(t)^{\frac{1}{2}-\varepsilon} N_{F/\mathbb{Q}}((m_0)_{Iso}) \qquad \textit{for all } m \in \mathfrak{o}_F,$$

where $m = tm_0^2$ and

$$\widehat{\Lambda}_3 = \frac{C_\varepsilon \left(2\pi D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]}}{\zeta_F(2)} \min_{T'\in\mathcal{B}_\mathcal{T}} \left\{ N_{F/\mathbb{Q}}((T'/t)_{Aniso})^{\frac{1}{2}} \prod_{\substack{\mathfrak{p}\in\mathrm{Stable}(T') \\ \mathfrak{p}|N,\, \mathfrak{p}\, Iso}} C'_\mathfrak{p}(T') \prod_{\mathfrak{p}|N} \frac{\beta_\mathfrak{p}(T')}{1+q} \right\}.$$

b) When $n = 4$ and m is locally represented by Q, we have the lower bound:

$$a_E(m) \geq \widehat{\Lambda}_4\, N_{F/\mathbb{Q}}((m)_{Iso}) \prod_{\substack{\mathfrak{p}|m,\, \mathfrak{p}\nmid N \\ \chi(\mathfrak{p})=-1}} \frac{q-1}{q+1} \qquad \textit{for all } m \in \mathfrak{o}_F > 0,$$

where

$$\widehat{\Lambda}_4 = \min_{T'\in\mathcal{B}_\mathcal{T}} \left\{ \frac{\left(2\omega_4 D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]}}{N_{F/\mathbb{Q}}((T')_{Aniso})\, L_F(2,\chi)} \prod_{\mathfrak{p}|N} \frac{\beta_\mathfrak{p}(T')}{\left(1 - \frac{\chi(\mathfrak{p})}{q^2}\right)} \prod_{\substack{\mathfrak{p}\in\mathrm{Stable}(T') \\ \mathfrak{p}|N,\, \mathfrak{p}\, Iso}} C'_\mathfrak{p}(T') \right\}.$$

c) When $n \geq 5$ and m is locally represented by Q, we have the lower bound:

$$a_E(m) \geq \widehat{\Lambda}_n \, N_{F/\mathbb{Q}}(m)^{\frac{n-2}{2}} \qquad \text{for all } m \in \mathfrak{o}_F > 0,$$

where the constants $\widehat{\Lambda}_n$ for $n \geq 5$ are given by

$$\widehat{\Lambda}_n = \left(\frac{n\,\omega_n\, D^{-\frac{1}{2}}}{2} \right)^{[F:\mathbb{Q}]} \begin{cases} \frac{\zeta_F(n-2) E_n(X)}{\zeta_F(n-1)\zeta_F(\frac{n-1}{2})} \min_{T' \in \mathcal{B}_T} \{\widehat{B}_n(T')\} & \text{if } n \text{ is odd,} \\ \frac{\zeta_F(n-2)}{L_F(\frac{n}{2}, \Phi_n)\zeta_F(\frac{n-2}{2})^2} \min_{T' \in \mathcal{B}_T} \{\widehat{B}_n(T')\} & \text{if } n \text{ is even,} \end{cases}$$

with

$$\widehat{B}_n(T') = \begin{cases} \prod_{\mathfrak{p} \mid N} \frac{\beta_v(T')}{1+q^{(n-1)/2}} & \text{if } n \text{ is odd,} \\ \prod_{\mathfrak{p} \mid N} \frac{\beta_v(T')}{\left(1 - \frac{\Phi_n(\mathfrak{p})}{q^{n/2}}\right)\left(1 - \frac{1}{q^{(n-2)/2}}\right)} & \text{if } n \text{ is even,} \end{cases}$$

and

$$E_n(X) = \frac{\prod_{p<X} \left(\frac{1}{1+\frac{1}{p^s}} \right)^{[F:\mathbb{Q}]}}{\prod_{N\mathfrak{p} \leq X} \left(1 + \frac{1}{N\mathfrak{p}^s}\right)} \left(\frac{\zeta_{\mathbb{Q}}(2s)}{\zeta_{\mathbb{Q}}(s)} \right)^{[F:\mathbb{Q}]},$$

for any X.

Proof. Fix some $T' \in \mathbb{A}_{\mathfrak{o}_F}$ with $\mathrm{ord}_{\mathfrak{p}}(T') \leq 1$ at all $\mathfrak{p} \nmid N$ and satisfying the product formula $\prod_v |T'|_v = 1$, and consider $m = T'(m')^2 \in T'(\mathbb{A}_{\mathfrak{o}_F})^2$ with m' supported on $\mathrm{Stable}(T')$. Combining (5.5) and our estimates $\beta_{\mathfrak{p}}(m) \geq C'_{\mathfrak{p}}(T')\beta_{\mathfrak{p}}(T')$ from (5.11), we see that

$$a_E(m) \geq a_E(T')\, N_{F/\mathbb{Q}}((m')_{Iso})^{n-2} \prod_{\substack{\mathfrak{p} \in \mathrm{Stable}(T') \\ \mathfrak{p}\, Iso}} C'_{\mathfrak{p}}(T'). \tag{5.13}$$

The first part of (a) follows from (5.12) since $C'_{\mathfrak{p}}(T') = 1$ for all $\mathfrak{p} \nmid N$ when $n = 3$.

For the remaining cases, we must establish a bound over all square classes $t(\mathbb{A}_{\mathfrak{o}_F})^2$. This is related to the generic behavior of the local factors as t varies, and depends on the parity of n. After accounting for the local factors at $\mathfrak{p} \nmid N$ we will be left with finitely many lower bounds for $a_E(m)$, and taking their minimum proves the theorem. This generic behavior was first investigated by Siegel [Si, Hilfssatz 12, pp539–42], who showed that it is related to certain special values of L-functions.

Suppose n is even: When n is even, the quadratic character Φ_n associated to Q is independent of m, and the generic part of $\prod_v \beta_v(m)$ here is essentially $L(\frac{n}{2}, \Phi_n)$. Explicitly, since $\mathrm{ord}_{\mathfrak{p}}(T') \leq 1$ at all $\mathfrak{p} \nmid N$, we can use Table 1 to compute

$$\begin{aligned} \prod_{\mathfrak{p} \nmid N} \beta_{\mathfrak{p}}(T') &= \prod_{\mathfrak{p} \nmid NT'} \left(1 - \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n}{2}}}\right) \prod_{\mathfrak{p} \mid T',\, \mathfrak{p} \nmid N} \frac{\left(q^{\frac{n-2}{2}} + \Phi_n(\mathfrak{p})\right)\left(q^{\frac{n}{2}} - \Phi_n(\mathfrak{p})\right)}{q^{n-1}} \\ &= \prod_{\mathfrak{p} \nmid N} \left(1 - \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n}{2}}}\right) \prod_{\mathfrak{p} \mid T',\, \mathfrak{p} \nmid N} \frac{\left(q^{\frac{n-2}{2}} + \Phi_n(\mathfrak{p})\right)\left(q^{\frac{n}{2}} - \Phi_n(\mathfrak{p})\right)}{q^{\frac{n-2}{2}}\left(q^{\frac{n}{2}} - \Phi_n(\mathfrak{p})\right)} \\ &\geq \prod_{\mathfrak{p} \nmid N} \left(1 - \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n}{2}}}\right) \prod_{\substack{\mathfrak{p} \mid T',\, \mathfrak{p} \nmid N \\ \Phi_n(\mathfrak{p}) = -1}} \left(1 - \frac{1}{q^{\frac{n-2}{2}}}\right). \end{aligned}$$

When $n \geq 6$ we can estimate this directly, getting

$$a_E(T') \geq \frac{N_{F/\mathbb{Q}}(T')^{\frac{n-2}{2}}}{L_F(\frac{n}{2}, \Phi_n)\zeta_F(\frac{n-2}{2})} \prod_{\mathfrak{p}|N} \frac{\beta_{\mathfrak{p}}(T')}{\left(1 - \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n}{2}}}\right)\left(1 - \frac{1}{q^{\frac{n-2}{2}}}\right)} \prod_{v|\infty} \beta_v(1),$$

while for $n = 4$ we have

$$a_E(T') \geq \frac{N_{F/\mathbb{Q}}(T')}{L_F(2, \chi)} \prod_{\mathfrak{p}|N} \frac{\beta_{\mathfrak{p}}(T')}{\left(1 - \frac{\chi(\mathfrak{p})}{q^2}\right)} \prod_{v|\infty} \beta_v(1) \prod_{\substack{\mathfrak{p}|T',\, \mathfrak{p}\nmid N \\ \chi(\mathfrak{p})=-1}} \left(1 - \frac{1}{q}\right).$$

From Table 2 we see that $C'_{\mathfrak{p}}(T') = 1$ unless $\mathfrak{p} \nmid T'$ and $\Phi_n(\mathfrak{p}) = -1$, in which case $C'_{\mathfrak{p}}(T')$ is the local factor at $\mathfrak{p}$ of $\zeta_F(n-2)/\zeta_F(\frac{n-2}{2})$. When $n \geq 6$, this together with (5.13) and (5.5) gives

$$a_E(m) \geq N_{F/\mathbb{Q}}(m)^{\frac{n-2}{2}} \frac{\zeta_F(n-2)\left(\frac{n}{2}\omega_n D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]}}{L_F(\frac{n}{2}, \Phi_n)\zeta_F(\frac{n-2}{2})^2} \prod_{\mathfrak{p}|N} \frac{\beta_{\mathfrak{p}}(T')}{\left(1 - \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n}{2}}}\right)\left(1 - \frac{1}{q^{\frac{n-2}{2}}}\right)},$$

and when $n = 4$ this gives

$$a_E(m) \geq \frac{N_{F/\mathbb{Q}}((m)_{Iso})\left(2\omega_4 D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]}}{N_{F/\mathbb{Q}}((T')_{Aniso})\, L_F(2, \chi)} \prod_{\mathfrak{p}|N} \frac{\beta_{\mathfrak{p}}(T')}{\left(1 - \frac{\chi(\mathfrak{p})}{q^2}\right)} \prod_{\substack{\mathfrak{p}\in\mathrm{Stable}(T') \\ \mathfrak{p}|N,\, \mathfrak{p}\ Iso}} C'_{\mathfrak{p}}(T')$$
$$\prod_{\substack{\mathfrak{p}|T',\, \mathfrak{p}\nmid N \\ \chi(\mathfrak{p})=-1}} \left(1 - \frac{1}{q}\right) \prod_{\substack{\mathfrak{p}|m',\, \mathfrak{p}\nmid N \\ \chi(\mathfrak{p})=-1}} \left(1 + \frac{1}{q}\right)^{-1}.$$

Taking the minimum over all $T' \in \mathcal{B}_{\mathcal{T}}$ as above gives (b) for $n = 4$ and (c) when $n \geq 6$ and even.

Suppose n is odd: When n is odd, then the generic factor is more complicated since the quadratic character Φ_n depends on m (or more precisely, its square free part t). Since $ord_{\mathfrak{p}}(T') \leq 1$ at all $\mathfrak{p} \nmid N$, we have

$$\begin{aligned}\prod_{\mathfrak{p}\nmid N} \beta_{\mathfrak{p}}(T') &= \prod_{\mathfrak{p}\nmid NT'} \left(1 + \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n-1}{2}}}\right) \prod_{p\nmid N,\, \mathfrak{p}|T'} \left(1 - \frac{1}{q^{n-1}}\right) \\ &= \frac{L_F(\frac{n-1}{2}, \Phi_n)}{\zeta_F(n-1)} \prod_{\mathfrak{p}|N} \frac{1 - \frac{\Phi_n(\mathfrak{p})}{q^{\frac{n-1}{2}}}}{1 - \frac{1}{q^{n-1}}},\end{aligned}$$

since $\Phi_n(\mathfrak{p}) = 0$ for all $\mathfrak{p} \mid T'$ where $\mathfrak{p} \nmid N$. From this we have

$$a_E(T') \geq \frac{L_F(\frac{n-1}{2}, \Phi_n)}{\zeta_F(n-1)} N_{F/\mathbb{Q}}(T')^{\frac{n-2}{2}} \prod_{\mathfrak{p}|N} \frac{\beta_{\mathfrak{p}}(T')}{1 + q^{\frac{n-1}{2}}} \prod_{v|\infty} \beta_v(1).$$

From Table 2 we see that when n is odd, $C'_p(T') = 1$ unless $n \geq 5$ and $\Phi_n(\mathfrak{p}) = 1$, in which case $C'_\mathfrak{p}(T')$ is the local factor at $\mathfrak{p}$ of $\zeta_F(n-2)/\zeta_F(\frac{n-1}{2})$. Combining this with (5.13) and (5.5) gives

$$a_E(m) \geq N_{F/\mathbb{Q}}(m)^{\frac{n-2}{2}} \frac{L_F(\frac{n-1}{2}, \Phi_n)\zeta_F(n-2)}{\zeta_F(n-1)\zeta_F(\frac{n-1}{2})} \left(\frac{n}{2}\omega_n D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]} \prod_{\mathfrak{p}|N} \frac{\beta_\mathfrak{p}(T')}{1+q^{\frac{n-1}{2}}}$$

when $n \geq 5$.

To find a lower bound for $L_F(1, \Phi_n)$ when $s \in \mathbb{R} > 1$, we write

$$L_F(s, \Phi_n) \geq \prod_{N\mathfrak{p} \leq X} \left(1 + \frac{1}{N\mathfrak{p}^s}\right)^{-1} \prod_{N\mathfrak{p} > X} \left(1 + \frac{1}{N\mathfrak{p}^s}\right)^{-1}$$

for some parameter X, and estimate

$$\prod_{N\mathfrak{p} > X} \left(1 + \frac{1}{N\mathfrak{p}^s}\right) \leq \prod_{p > X} \left(1 + \frac{1}{p^s}\right)^d = \left(\frac{\zeta_\mathbb{Q}(s)}{\zeta_\mathbb{Q}(2s)}\right)^d \prod_{p < X} \left(\frac{1}{1 + \frac{1}{p^s}}\right)^d$$

where $d = [F : \mathbb{Q}]$, by taking all primes $\mathfrak{p} \mid p$ to split completely. This shows

$$L_F(s, \Phi_n) \geq \frac{\prod_{p<X} \left(\frac{1}{1+\frac{1}{p^s}}\right)^d}{\prod_{N\mathfrak{p} \leq X} \left(1 + \frac{1}{N\mathfrak{p}^s}\right)} \left(\frac{\zeta_\mathbb{Q}(2s)}{\zeta_\mathbb{Q}(s)}\right)^d$$

which becomes optimal as $X \to \infty$, and gives (c) by taking the minimum of the $\beta_\mathfrak{p}(T')$ at $\mathfrak{p} \mid N$ over all T' in the lower bound for $a_E(m)$ above.

When $n = 3$ we have $C'_\mathfrak{p}(T') = 1$ for all $\mathfrak{p} \nmid N$, so

$$a_E(m) \geq \frac{N_{F/\mathbb{Q}}(t(m_0)^2_{Iso})^{\frac{1}{2}}}{N_{F/\mathbb{Q}}((T'/t)_{Aniso})^{-\frac{1}{2}}} L_F(1, \psi) \frac{\left(2\pi D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]}}{\zeta_F(2)} \prod_{\mathfrak{p}|N} \frac{\beta_\mathfrak{p}(T')}{1+q} \prod_{\substack{\mathfrak{p} \in \mathrm{Stable}(T') \\ \mathfrak{p}|N,\, \mathfrak{p}\ Iso}} C'_\mathfrak{p}(T').$$

If we know $L_F(1, \psi) = L_F(1, \chi_{(t)}) \geq C_\varepsilon N_{F/\mathbb{Q}}(t)^{-\varepsilon}$, then we have

$$a_E(m) \geq \frac{N_{F/\mathbb{Q}}(t(m_0)^2_{Iso})^{\frac{1}{2}}}{N_{F/\mathbb{Q}}(t)^\varepsilon} \frac{C_\varepsilon \left(2\pi D^{-\frac{1}{2}}\right)^{[F:\mathbb{Q}]}}{\zeta_F(2)\, N_{F/\mathbb{Q}}((T'/t)_{Aniso})^{-\frac{1}{2}}} \prod_{\mathfrak{p}|N} \frac{\beta_\mathfrak{p}(T')}{1+q} \prod_{\substack{\mathfrak{p} \in \mathrm{Stable}(T') \\ \mathfrak{p}|N,\, \mathfrak{p}\ Iso}} C'_\mathfrak{p}(T'),$$

which similarly gives the second part of (a). $\square$

Remark 5.7.1. When the class number of F is 1, it is unnecessary to consider the adelic square classes $t(\mathbb{A}_{\mathfrak{o}_F})^2$ in Theorem 5.7, and we can freely replace them by the more conventional square classes $t{\mathfrak{o}_F}^2$. In particular, when $F = \mathbb{Q}$ we are dealing with the square classes $t\mathbb{Z}^2$.

Lemma 5.8. *Suppose $n = 3$ and $F = \mathbb{Q}$.*

a) We have the general inequality

$$|a_H(m)| \leq a_E(m).$$

b) Given any set $\mathbb{T} \subseteq VStable(m)$, we have the refined inequality

$$|a_H(m)| \leq \left(\prod_{\substack{p \in \mathbb{T}, \\ \psi(p) \neq 0}} C'_p(m) \right) a_E(m),$$

with equality iff m is of exceptional-type (in which case $|a_H(m)| = a_E(m)$).

Suppose $H(z) \neq 0$, $t\mathbb{Z}^2$ is a spinor square class, and ψ_t is its associated quadratic character. Then $t \mid N$ and

c) $\psi_t(p) = 0$ for all anisotropic primes p.

d) If m is of exceptional-type (so $m \in t\mathbb{Z}^2$), then $C'_p(m) = 1$ for all primes $p \in VStable(m)$ with $\psi_t(p) \neq 0$.

Proof. To see (a), by the discussion after (4.6), if $|a_H(m)| > a_E(m)$ then $a_H(m) > a_E(m)$ for some spinor genus in $\mathrm{Gen}(Q)$, contradicting (4.6) ≥ 0.

For (b), we let $\mathbb{S} = \{p \in \mathbb{T} \mid \psi(p) \neq 0 \text{ and } C_p(m) < 1\}$ and let $m_1 \to \infty_{\mathbb{S}}$ mean that $m_1 \in \mathbb{N}$ is divisible only by primes $p \in \mathbb{S}$ and that $m_1 \to \infty$ in such a way that $\mathrm{ord}_p(m_1) \to \infty$ for all $p \in \mathbb{S}$.

From Remark 5.4.1(a), we see that

$$\lim_{m_1 \to \infty_{\mathbb{S}}} \frac{a_E(m m_1^2)}{m_1} = a_E(m) \prod_{p \in \mathbb{S}} C_p(m)$$

and

$$\lim_{m_1 \to \infty_{\mathbb{S}}} \frac{|a_H(m m_1^2)|}{m_1} = |a_H(m)|,$$

hence the inequality in (b) follows from (a).

Now suppose we have equality in (b). Then we wish to show

$$\lim_{m_1 \to \infty_{\mathbb{S}}} \frac{a_E^*(m m_1^2) + a_H^*(m m_1^2)}{a_E^*(m m_1^2)} = 0$$

which contradicts [SP3, Korollar 2, pp130-131] unless m is of exceptional-type. By Remark 5.4.1(a) we see that $\lim_{m_1 \to \infty_{\mathbb{S}}} \frac{a_E^*(m m_1^2)}{m_1} \neq 0$ since all $p \in \mathbb{S}$ are isotropic, thus we are reduced to showing

$$\lim_{m_1 \to \infty_{\mathbb{S}}} \frac{a_E^*(m m_1^2) + a_H^*(m m_1^2)}{m_1} = 0.$$

However, this follows from our assumption by evaluating the limit inside the defining divisor sum (which has finitely many terms since $\mathbb{S}$ is a finite set).

Finally, if m is of exceptional-type then we have equality in (a), hence (a) and (b) coincide and $C_p(m) \geq 1$ for all $p \in \mathrm{VStable}(m)$ with $\psi(p) \neq 0$, proving (d). □

Remark 5.8.1. Since the character $\psi_t(\cdot) = \Phi_3(\cdot) = \left(\frac{-tD}{\cdot}\right)$ is associated to the pair $(Q, t\mathbb{Z}^2)$ while the anisotropic primes are related only to Q, we do not expect a general relationship between the anisotropic primes and those primes with $\psi_t(p) = 0$. However, for a spinor square class $t\mathbb{Z}^2$, Lemma 5.8(c) and (d) gives that $\{p \in \mathrm{VStable}(T') \mid C'_p(T') = 1\} \subseteq \{p \mid \psi_t(p) \neq 0\} \subseteq Iso$ when $T' \in t\mathbb{Z}^2$ is of exceptional-type.

Theorem 5.9. *Let Q be a positive definite integral quadratic form in 3 variables defined over $\mathbb{Q}$, and suppose that $m = \widetilde{T}\widetilde{m}^2$ is locally represented by Q and contained in a spinor square class, and that $\widetilde{m}$ is supported on VStable$(\widetilde{T})$. Then we have the following lower bounds for $a_E(m) + a_H(m)$:*

a) If $\widetilde{T}$ is non-exceptional, then

(i) *When $a_H(m) = 0$, we may apply Theorem 8.3(a) to obtain*

$$a_E(m) + a_H(m) \geq \Lambda_3(\widetilde{T})(\widetilde{m})_{Iso}.$$

(ii) *When $a_H(m) \neq 0$, we have the lower bound*

$$a_E(m) + a_H(m) \geq K_0(\widetilde{T})(\widetilde{m})_{Iso}$$

where

$$K_0(\widetilde{T}) = a_E(\widetilde{T}) \prod_{\substack{p \in \mathrm{VStable}(\widetilde{T}) \\ p \mid N,\, \psi_{\widetilde{T}}(p) \neq 0}} C'_p(\widetilde{T}) - |a_H(\widetilde{T})| > 0.$$

b) If $\widetilde{T}$ is of exceptional-type and m is non-exceptional, then

(i) *When $a_H(m) \geq 0$, we may apply Theorem 5.7(a) to obtain*

$$a_E(m) + a_H(m) \geq \Lambda_3(\widetilde{T})(\widetilde{m})_{Iso}.$$

(ii) *When $a_H(m) < 0$, we have the lower bound*

$$a_E(m) + a_H(m) \geq a_E(\widetilde{T})\, \widetilde{m}_+\, 2^{\epsilon} \left(\sigma(\widetilde{m}_-) - \widetilde{m}_-\right) \widetilde{m}_2 \prod_{p \mid \widetilde{m}_2} \left[\frac{(C_p(\widetilde{T}) - 1)(p-1)}{p}\right],$$

where $(\widetilde{m})_{Iso} = \widetilde{m}_+\widetilde{m}_-\widetilde{m}_2$ is as in Theorem 5.5 and ϵ is defined to be 0 if $\widetilde{m}_- = 1$ and 1 if $\widetilde{m}_- > 1$. Moreover, this lower bound is an equality when for some prime p either $\widetilde{m}_- = p^\nu$ and $\widetilde{m}_2 = 1$, or $\widetilde{m}_- = 1$ and $\widetilde{m}_2 = p$.

Proof. Part (i) of (a) and (b) follows directly from Theorem 5.7(a).

Part (ii) of (a): Since $a_H(m) \neq 0$, both $a_H(\widetilde{T})$ and $\psi_{\widetilde{T}}(\widetilde{m}) \neq 0$. By Lemma 5.8($c$), this implies that all $p \mid \widetilde{m}$ are isotropic. Using Theorem 5.7(a) with $T' = \widetilde{T}$ and $\mathbb{S} = \{p \in \mathrm{VStable}(\widetilde{T}) \mid \psi_{\widetilde{T}}(p) \neq 0\}$, we see

$$a_E(m) + a_H(m) \geq \left[a_E(\widetilde{T}) \prod_{p \in \mathbb{S}} C'_p(\widetilde{T}) - |a_H(\widetilde{T})|\right] (\widetilde{m})_{Iso},$$

which is > 0 by Lemma 5.8(b) since $\widetilde{T}$ is not of exceptional-type.

Part (ii) of (b): Theorem 5.5 gives an exact formula for $a_E(m) + a_H(m)$, and our conditions imply that its first term vanishes. Since m is non-exceptional, from the remaining term we see that $\widetilde{m}_-\widetilde{m}_2 > 1$.

We obtain our estimate by applying Theorem 5.5 in stages (going from $\widetilde{T}_0 = \widetilde{T}\widetilde{m}_+^2$, to $\widetilde{T}_1 = \widetilde{T}_0\widetilde{m}_-^2$, to $m = \widetilde{T}_1\widetilde{m}_2^2$), and rounding off by assuming $|a_H(\widetilde{T}_i)| = a_E(\widetilde{T}_i)$ at each stage.

For each $p \mid \widetilde{m}_2$, we have

$$\begin{aligned} a_E(\widetilde{T}_i p^{2\nu}) + a_H(\widetilde{T}_i p^{2\nu}) &\geq a_E(\widetilde{T}_i)(1 + C_p(\widetilde{T}_i)(p^\nu - 1)) - |a_H(\widetilde{T}_i)|p^\nu \\ &= a_E(\widetilde{T}_i)(C_p(\widetilde{T}_i) - 1)(p^\nu - 1) \\ &\geq a_E(\widetilde{T}_i)\left[\frac{(C_p(\widetilde{T}_i) - 1)(p-1)}{p}\right] p^\nu, \end{aligned}$$

where $\widetilde{T}_i \in \widetilde{T}_1\mathbb{Z}^2$ and $p \nmid \widetilde{T}_i$. By choosing $\widetilde{T}_{i+1} = \widetilde{T}_i p^{2\nu_p}$ and inducting on all $p \mid \widetilde{m}_2$, we have

$$a_E(m) + a_H(m) \geq \left[a_E(\widetilde{T}_1) - |a_H(\widetilde{T}_1)|\right] \prod_{p \mid \widetilde{m}_2} \left[\frac{(C_p(\widetilde{T}) - 1)(p-1)}{p}\right],$$

(Since as we vary $\widetilde{T}_i$ the $\mathrm{ord}_p(\widetilde{T}_i)$ are the same whenever $p \mid \widetilde{T}_i$, we see that $C_p(\widetilde{T}_i) = C_p(\widetilde{T})$.) From Theorem 5.5, we also have that

$$a_E(\widetilde{T}_1) - a_H(\widetilde{T}_1) \geq \left[a_E(\widetilde{T}_0) - |a_H(\widetilde{T}_0)|\right] 2^\epsilon \left[\sigma(\widetilde{m}_-) - \widetilde{m}_-\right],$$

and

$$a_E(\widetilde{T}_0) - |a_H(\widetilde{T}_0)| = a_E(\widetilde{T})\,\widetilde{m}_+,$$

which combine to prove the theorem. $\square$

§6 Main Results

We now state some effective lower bounds which are sufficient to ensure that a number m is represented by a positive definite quadratic form Q in $n \geq 3$ variables.

Theorem 6.1. *Suppose Q is a positive definite quadratic form in 3 variables and t is square free. Then any sufficiently large $m = \widetilde{T}\widetilde{m}^2 \in t\mathbb{Z}^2$ locally represented by Spn(Q) with $\widetilde{m}$ supported on VStable($\widetilde{T}$) and having a priori bounded divisibility at the anisotropic primes is represented by Q, except possibly when $\widetilde{T}$ is anti-exceptional and $m = \widetilde{T}p^2$ for some prime $p \nmid N$ with $\psi_{\widetilde{T}}(p) = -1$.*

If either $\widetilde{T}$ is non-exceptional or $a_H(m) \geq 0$, we see that m is represented when

$$\frac{\sqrt{(m_0)_{Iso}}}{\tau((m_0)_{Iso})^2} > M_3\,\tau((m_0)_{Aniso})^2\sqrt{(m_0)_{Aniso}},$$

where $m = t(m_0)^2$, $M_3 = M_3(\widetilde{T}) = \sum_i |\gamma_i|/[(\widetilde{T}/t)_{Iso}^{\frac{1}{2}} \min\{\Lambda_3(\widetilde{T}), K_0(\widetilde{T})\}] > 0$ with Λ_3 and K_0 as in Theorem 5.7(a) and Theorem 5.9(a)(ii) respectively, and the γ_i are as in (4.7) with $g = Shi(f,t)$.

If $\widetilde{T}$ is of exceptional-type and m is non-exceptional, then m is represented when

$$2^\epsilon \frac{\sqrt{\widetilde{m}_+ \widetilde{m}_2}}{\tau((m_0)_{Iso})^2} \frac{\sigma(\widetilde{m}_-) - \widetilde{m}_-}{\sqrt{\widetilde{m}_-}} > \frac{\sum_{i=1}^r |\gamma_i|}{a_E(\widetilde{T})} \frac{\tau((m_0)_{Aniso})^2 \sqrt{(m_0)_{Aniso}}}{\prod_{p|\widetilde{m}_2} \left[\frac{(C_p(\widetilde{T})-1)(p-1)}{p}\right]},$$

where $m = t(m_0)^2$, $(\widetilde{m})_{Iso} = \widetilde{m}_+ \widetilde{m}_- \widetilde{m}_2$ with $\widetilde{m}_{\pm,2}$ as defined in Theorem 5.5, $\epsilon = 1$ when $\widetilde{m}_2 > 1$ and zero otherwise, and the γ_i are as in (4.7) with $g = Shi(f,t)$.

Proof. The general statement follows from the following two cases, noting that when $m = \widetilde{T}p^2$ as above our bound is no better than for $m = \widetilde{T}$. Thus, if $\widetilde{T}$ is not represented, we can say nothing about the representability of $\widetilde{T}p^2$.

Case 1: If either $\widetilde{T}$ is non-exceptional or $a_H(m) > 0$, then by Theorem 5.9 we have

$$a_E(m) \geq \min\{\Lambda_3(\widetilde{T}), K_0(\widetilde{T})\}(\widetilde{m})_{Iso} > 0.$$

Combining this with (4.9) and solving to ensure $a_E(m) > |a_H(m)|$ gives the desired bound.

Case 2: If $\widetilde{T}$ is of exceptional-type and m is non-exceptional, then the result follows from combining Theorem 5.9$(b)(ii)$ and (4.9) to ensure $a_E(m) > |a_H(m)|$. $\square$

Theorem 6.2. *Let Q be a positive definite integral quadratic form in 3 variables, and suppose $L(1, \psi_t) \geq C_\varepsilon t^{-\varepsilon}$ for some $\varepsilon > 0$ with $C_\varepsilon > 0$ as t runs over all positive square free numbers. Then any sufficiently large locally represented $m \in \mathbb{N}$ not contained in a spinor square class is represented by Q. In fact, m is represented when*

$$\frac{t^{\eta-(\varepsilon+\varepsilon')}(m_0)_{Iso}^{\frac{1}{2}}}{\tau((m_0)_{Iso})^2} \geq \frac{B_{\varepsilon'} \sum_k |\delta_k|}{\widehat{\Lambda}_3} \tau((m_0)_{Aniso})^2 (m_0)_{Aniso}^{\frac{1}{2}},$$

where $m = tm_0^2$, $\widehat{\Lambda}_3$ is defined in Theorem 5.7(a), the δ_k are defined after (4.8), and η, ε', and $B_{\varepsilon'}$ are as in Assumption 4.4.

Proof. This follows by using Theorem 5.7(a) and (4.10) with $n = 3$, and solving to ensure $a_E(m) > |a(m)|$. $\square$

From Theorem 6.1, we have a good understanding of which numbers are represented by Q within any given square class $t\mathbb{Z}^2$, though our information is only complete if $t\mathbb{Z}^2$ is not one of the finitely many (spinor) exceptional-type square classes. Assuming the Riemann hypothesis for Dirichlet L-functions (or at least that they have no Siegel zeros) gives the effective lower bound $L(1, \chi_{(t)}) \geq C_\varepsilon t^{-\varepsilon}$ necessary for Theorem 6.2, and allows us to uniformly understand the representation behavior across all but finitely many square classes. Obtaining complete information about the representation behavior within the (spinor) exceptional-type square classes is more subtle and depends on understanding the behavior of the Fourier coefficients of the cusp form $f(z)$ in (4.4). We take up this issue in [Ha2].

Theorem 6.3. *Let Q be a positive definite integral quadratic form in 4 variables. Then any sufficiently large locally represented m with a priori bounded divisibility at the anisotropic primes is represented by Q. In fact, m is represented when*

$$\frac{\sqrt{(m)_{Iso}}}{\tau((m)_{Iso})} \prod_{\substack{p \nmid N,\, p|m \\ \chi(p)=-1}} \frac{p-1}{p+1} > \frac{\sum_{i=1}^r |\gamma_i|}{\widehat{\Lambda}_4} \tau((m)_{Aniso}) \sqrt{(m)_{Aniso}}$$

where $\widehat{\Lambda}_4 > 0$ is as in Theorem 5.7(b), and the γ_i are as in (4.7).

Proof. This follows by combining Theorem 5.7(b) and (4.8) with $k = \frac{n}{2} = 4$ to ensure $a_E(m) > |a(m)|$. $\square$

Remark. Schulze-Pillot [SP3] has given an explicit lower bound for representability when $n = 4$, though his bound is a bit coarser since it depends only on the level N of Q, not Q itself, thus is not very practical for computations.

For completeness, we state an explicit bound for the case $n \geq 5$ as well, though there are already many such bounds available in the literature. (See [Wa] and [Hs-Ic] for example.)

Theorem 6.4. *Suppose Q be a positive definite integral quadratic form in $n \geq 5$ variables. Then any sufficiently large locally represented number m is represented by Q. In fact, m is represented when*

$$\frac{m^{\frac{n-2}{4}}}{\tau(m)} \geq \frac{\sum_{i=1}^{r} |\gamma_i|}{\widehat{\Lambda}_n} \qquad \text{if } n \text{ is even,}$$

and under Assumption 1 when

$$\frac{t^{\frac{n-3}{4}+\eta-\varepsilon'}(m_0)^{\frac{n-2}{2}}}{\tau(m_0)^2} \geq \frac{B_{\varepsilon'} \sum_k |\delta_k|}{\widehat{\Lambda}_n} \qquad \text{if } n \text{ is odd,}$$

with $m = tm_0^2$, the γ_i and δ_k as defined at the end of §3, and $\widehat{\Lambda}_n$ as in Theorem 5.7(c).

Proof. This follows by combining Theorem 5.7(c), (4.8), and (4.10) with $k = \frac{n}{2}$ to ensure $a_E(m) > |a(m)|$. $\square$

Theorem 6.5. *Suppose p is anisotropic and m is p-stable. Then*

$$r_Q(mp^{2\nu}) = r_Q(m) \qquad \text{for all } \nu \geq 0.$$

Proof. It suffices to prove this for $\nu = 1$, since the theorem follows by repeated application of this result. Notice that since every representation $Q(\vec{x}) = m$ gives rise to a representation $Q(p\vec{x}) = mp^2$, we have the general inequality $r_Q(mp^2) \geq r_Q(m)$.

Suppose p is anisotropic. Then by Remark 5.4.1(a) we have $a_E(mp^2) = a_E(m)$. However (4.5) expresses $a_E(m)$ as an average of $r_{Q'}(m)$ over all $Q' \in \text{Gen}(Q)$, so $a_E(mp^2) = a_E(m)$ implies $r_{Q'}(mp^2) = r_{Q'}(m)$ for all $Q' \in \text{Gen}(Q)$. $\square$

Theorems 6.3 and 6.4 allow us to determine a finite set of numbers to check for representability, assuming bounded growth at anisotropic primes. Once this is done, for each m which is not represented we may use Theorem 6.5 to determine the representation behavior allowing anisotropic factors. While this does not guarantee the existence of only finitely many numbers which are not represented (given local representability), it does provide a practical procedure for determining the numbers represented by a positive definite integral quadratic form in 4 variables, and also in 3 variables aside from the sequences $\widetilde{T}p^2$ mentioned in Theorem 6.1.

For computational purposes, we now state some useful inequalities.

Lemma 6.6. *For some fixed $N \in \mathbb{N}$ and quadratic Dirichlet character χ, let*

$$F_4(m) = \frac{\sqrt{m}}{\tau(m)} \prod_{\substack{p \nmid N,\, p \mid m \\ \chi(p)=-1}} \frac{p-1}{p+1}.$$

Then $F_4(m)$ is a multiplicative function and for any prime p, we have

$$F_4(mp^\nu) \geq F_4(m)$$

when either $p \geq 11$ and $\nu \geq 1$, $p = 7$ or 5 and $\nu \geq 2$, $p = 3$ and $\nu \geq 5$, or $p = 2$ and $\nu \geq 11$.

Proof. Clearly $F_4(ab) = F_4(a)F_4(b)$ when $\gcd(a,b) = 1$, so $F_4(m)$ is multiplicative. For the second part, we write $m = m_1 p^{\nu_1}$ where $p \nmid m_1$. Then

$$\begin{aligned} F_4(mp^\nu) &= \frac{p^{\nu/2}\sqrt{m_1 p^{\nu_1}}}{(1+\nu_1+\nu)\tau(m_1)} \prod_{\substack{p' \nmid N,\, p' \mid mp \\ \chi(p')=-1}} \frac{p'-1}{p'+1} \\ &\geq \frac{p^{\nu/2}(p-1)}{p+1} \frac{1+\nu_1}{1+\nu_1+\nu} F_4(m), \end{aligned}$$

and we are interested in when $\frac{p^{\nu/2}(p-1)}{p+1}\frac{1+\nu_1}{1+\nu_1+\nu} \geq 1$. The most restrictive case is when $\nu_1 = 0$, and we can see that this is true when either p or ν is sufficiently large. For $p \geq 11$, we see that any $\nu \geq 1$ will do, while for $p = 2, 3, 5,$ or 7 we must have $\nu \geq 11, 5, 2,$ or 2 respectively. □

Remark 6.6.1. The function $F_4(m)$ in Lemma 6.6 is just the right side of the expression in Theorem 6.3 when $m = (m)_{Iso}$ and N is the level of Q.

§7.1 Asymptotics

While it is not our main goal, the methods of the previous sections allow us to describe the asymptotic behavior of $r_Q(m)$ as $m \to \infty$. This is especially interesting when $n = 3$, though the exact nature of the main term depends on how $m \to \infty$.

Suppose $n = 3$ and $F = \mathbb{Q}$, fix a square class $t\mathbb{Z}^2$, and suppose $m \to \infty$ is evenutally in $\widetilde{T}\mathbb{Z}^2$ for some $\mathbb{S}$-stable $\widetilde{T}$, where $m = \widetilde{T}\widetilde{m}^2$ and $\widetilde{m}$ is supported on VStable$(\widetilde{T})$. (If $m \to \infty$ by becoming increasingly divisible by square factors, for example, then Remark 3.6.1 guarantees that m is eventually in some such $\widetilde{T}\mathbb{Z}^2$.) To make sensible estimates we require that $sign(a_H(m)) \to \{0, \pm 1\}$, and for simplicity we also assume $\widetilde{m} = (\widetilde{m})_{Iso}$. Then using (4.9), Theorem 5.5, and estimating as in Theorem 5.9$(b)(ii)$, we have

$$r_Q(m) = a_E(m) + a_H(m) + O(\widetilde{m}^{\frac{1}{2}+\varepsilon})$$

where $a_H(m) = \pm' |a_H(m)|$ and

$$LL(\widetilde{m}) \leq \Big[a_E(m) \pm' |a_H(m)|\Big] - \Big[a_E(\widetilde{T}) \pm' |a_H(\widetilde{T})|\Big]\, \widetilde{m} \leq UU(\widetilde{m}),$$

with

$$LL(\widetilde{m}) = \widetilde{m}_+ \widetilde{m}_2 2^{\epsilon} (\sigma(\widetilde{m}_-) - \widetilde{m}_-) \prod_{p \mid \widetilde{m}_2} \frac{(C_p(\widetilde{T}) \pm' 1)(p-1)}{p}$$

and

$$UU(\widetilde{m}) = \widetilde{m}_+ \widetilde{m}_2 2^{\#\{p \mid \widetilde{m}_-\}} (\sigma(\widetilde{m}_-) - \widetilde{m}_-) \prod_{p \mid \widetilde{m}_2} (C_p(\widetilde{T}) \pm' 1).$$

To produce a well-defined constant, we fix a set of isotropic primes $\mathbb{S}$ such that $\sum_{\mathbb{S}'} \frac{1}{p} < \infty$ where $\mathbb{S}' = \{p \in \mathbb{S} \mid \psi_t(p) = -1\}$, and suppose $\widetilde{m} \to \infty_{\mathbb{S}}$. In this case, we have the simpler estimate

$$a_E(m) \pm' |a_H(m)| \sim \left(C_{3,\mathbb{S}} \pm' |a_H(\widetilde{T})| \right) \widetilde{m},$$

where $C_{3,\mathbb{S}}$ is defined by the (finite) product $C_{3,\mathbb{S}} = a_E(\widetilde{T}) \prod_{p \in \mathbb{S}} C_p(\widetilde{T})$.

§7.2 Quadratic Polynomials

While our original intention was to describe (compute) the numbers represented by a positive definite integral quadratic form Q, these results can be easily modified to describe the numbers represented by an integer-valued quadratic polynomial P whose homogeneous degree 2 part is positive definite.

By completing the square, this is equivalent to asking which numbers are represented by $Q(\vec{x} + \vec{b}) + c$ for some $\vec{b} \in \mathbb{Q}^n$ and $c \in \mathbb{Q}$, where Q is the degree 2 part of P. Now clearing deminators by multiplying through by some $d \in \mathbb{N}$, the question becomes which $m \in d\mathfrak{o}_F$ are represented by $Q(\vec{x} + \vec{b}') + c'$ with $\vec{b}' \in \mathbb{Z}^n$ and $c' \in \mathbb{Z}$. However this question can be answered by considering the congruence theta function, whose m^{th} coefficient counts $\vec{x} \in R_Q(m)$ with $\vec{x} \equiv \vec{b}' \pmod{d}$. The same results for the usual theta function apply to the congruence theta function, which gives the same results for them as for $\Theta_Q(z)$, though the constants involved will be different. The modifications necessary to include congruence conditions are described in §2 of [Du-SP]. Roughly speaking, there is an analogue of the Siegel product formula due to Van der Blij [VB] whose local factors count solutions satisfying the desired congruence, and the theta functions are modular forms with the same weight (though they may have a different level N' and be modular only for the group $\Gamma_1(N')$). Since our reduction procedure will respect these congruences, and our error term bound depends only on general properites of cusp forms, the only change is to modify the local constants C_p at those primes $p \mid d$ to account for the additional congruence condition.

§8 An Example

We now describe the numbers represented by the form $Q = x^2 + 3y^2 + 5z^2 + 7w^2$. This form has level $N = 420$, $\chi = \left(\frac{105}{\cdot}\right)$, and its only anisotropic place is $v = \infty$. Checking locally at $p = 2, 3, 5, 7$, we see that there are no congruence obstructions since all congruence classes (mod 8,3,5,7 respectively) have Good-type solutions. It was conjectured in 1982 by Kneser that Q represents all natural numbers except for 2 and 22, and he checked that this was true for all numbers $< 40,000$. This conjecture was later popularized by Kaplansky, and has been the positive definite form in 4 variables with smallest discriminant whose representation behavior was unknown. (The smaller forms in 4 variables can be handled by various arithmetic tricks.)

Using the QFlib package for Pari/GP [Ha1], we see that the relevant constants for Theorem 6.3 are $\sum_{i=1}^{r} |\gamma_i| \approx 39.34$ and $\widehat{\Lambda}_4 = 2/9$. Since Q has no anisotropic primes, it suffices to simply check the representability of all m with

$$F_4(m) < 177.03,$$

where F_4 is as in Lemma 6.6.

To implement this, we first check all square free numbers less than this bound. We do this by first computing the primes involved in such a computation, and then forming the list of square free numbers divisible only by these primes which again satisfy our bound. With the bound 177.03 above, we find that the first 11,765 primes are involved in our search. This leads to 68,776 square free numbers to check, and the largest of these is $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots 31 \approx 2 \times 10^{11}$. Using Magma on a Celeron (Coppermine) 1GHz, it takes ≈ 17 hours to compute the first 10^6 Fourier coefficients of $\Theta_Q(z)$, which makes a direct computation up to 2×10^{11} infeasible.

For quadratic forms in $n \geq 3$ variables, one approach is to reconstruct the Θ-function Fourier coefficients for each number m we're interested in by computing $a_E(m)$ locally using Siegel's product formula, and reconstructing $a(m)$ form the constants γ_i and the Hecke eigenvalues $\omega_i(p^2)$ (or $\omega_i(p)$ for $p \mid N$) of f_i for all $p \mid m$.

For quadratic forms Q in $n \geq 4$ variables, there is a convenient trick due to Bhargava we can use. Suppose we can write $Q = Q_1 + cw^2$ for some form Q_1 in ≥ 3 variables, and suppose m is represented by Q for some large $w = w_0$. Then $m - cw_0^2$ is much smaller than m (at best it's $\leq 2c\sqrt{m}$) and is represented by Q_1. However Q_1 has fewer variables than Q, so one can compute its theta coefficients more quickly and look for these representations. (In fact, to compute all coefficients $\leq X$ of Θ_Q, it takes $\approx cX^{\frac{n}{2}}$ time.) By repeating this for several large values of w_0, one can quickly reduce the size of the list of possibly non-represented numbers.

Applying this strategy of $Q = x^2 + 3y^2 + 5z^2 + 7w^2$ with $Q_1 = x^2 + 3y^2 + 7z^2$, we can compute the first 10^7 coefficients of $\Theta_{Q_1}(z)$ in ≈ 65 minutes, and easily check that the only possibly not represented numbers are 2 and 22. Since they are not represented, we see that Q represents all integers ≥ 0 except for 2 and 22.

§9 Appendix

It will be useful to have on hand the following straighforward Gauss sum computations (originally due to Siegel) to compute the local densities $\beta_{\mathfrak{p}}(m)$ when $\mathfrak{p} \nmid 2$.

Lemma 9.1. *Let $Q(\vec{x}) = \sum_{i=1}^{n} a_i x_i^2$ be an integral quadratic form defined over a number field F with $\mathfrak{p} \nmid a_i$, and let $r_{\mathfrak{p}}(m)$ denote the number of solutions $Q(\vec{x}) \equiv m \pmod{\mathfrak{p}}$. Then*

$$r_{\mathfrak{p}}(0) = \begin{cases} q^{n-1} & \text{if } n \text{ is odd,} \\ q^{n-1} + (q-1)q^{\frac{n-2}{2}} \left(\frac{(-1)^{\frac{n}{2}} a_1 \cdots a_n}{\mathfrak{p}}\right) & \text{if } n \text{ is even,} \end{cases}$$

$$r_{\mathfrak{p}}(u) = \begin{cases} q^{n-1} + q^{\frac{n-1}{2}} \left(\frac{(-1)^{\frac{n-1}{2}} a_1 \cdots a_n\, u}{\mathfrak{p}}\right) & \text{if } n \text{ is odd,} \\ q^{n-1} - q^{\frac{n-2}{2}} \left(\frac{(-1)^{\frac{n}{2}} a_1 \cdots a_n}{\mathfrak{p}}\right) & \text{if } n \text{ is even,} \end{cases}$$

where $u \in (\mathfrak{o}_F/\mathfrak{p})^\times = \mathbb{F}_q^\times$.

Proof. We let $r_\mathfrak{p}^n(m) = r_\mathfrak{p}(m)$ above and proceed by induction on n.

When $n = 1$ we check by hand that

$$r_\mathfrak{p}^1(0) = 1, \qquad r_\mathfrak{p}^1(u) = 1 + \left(\frac{au}{\mathfrak{p}}\right).$$

When $n \geq 1$ we assume by induction that

$$r_\mathfrak{p}^{n+1}(u) = C_{n+1} + D_{n+1}\left(\frac{u}{\mathfrak{p}}\right) \tag{9.1}$$

for all $u \in \mathbb{F}_q^\times$ where C_{n+1}, D_{n+1} are independent of u, and that $r_\mathfrak{p}^{n+1}(0) = C_{n+1}$ when $D_n = 0$.

We begin with the solutions $Q(\vec{x}) \equiv 0$. By allowing all but the last variable to be freely chosen, we have

$$r_\mathfrak{p}^{n+1}(0) = \sum_{\substack{m,z\in\mathbb{F}_q\\ m+a_{n+1}z=0}} r_\mathfrak{p}^n(m)\left(1 + \left(\frac{z}{\mathfrak{p}}\right)\right).$$

Rewriting the relationship between m and z as $m = -a_{n+1}z$ gives

$$\sum_{z\in\mathbb{F}_q} r_\mathfrak{p}^n(-a_{n+1}z) + \sum_{z\in\mathbb{F}_q} r_\mathfrak{p}^n(-a_{n+1}z)\left(\frac{z}{\mathfrak{p}}\right).$$

Since $z \mapsto -a_{n+1}z$ is a permutation of $\mathbb{F}_q$ we are summing over all possible values of Q, so the first term is just q^n. To analyze the other term, we substitute (9.1) which gives the preliminary formula

$$r_\mathfrak{p}^{n+1}(0) = q^n + (q-1)D_n\left(\frac{-a_{n+1}}{\mathfrak{p}}\right).$$

We now compute $r_\mathfrak{p}^n(u)$, and justify our inductive assumption (9.1). Suppose $r_\mathfrak{p}^n(u)$ is independent of u (i.e., $D_n = 0$), then by a similar argument to the previous computation, we have

$$\begin{aligned}
r_\mathfrak{p}^{n+1}(u) &= \sum_{\substack{m,z\in\mathbb{F}_q\\ m+a_{n+1}z=u}} r_\mathfrak{p}^n(m)\left(1 + \left(\frac{z}{\mathfrak{p}}\right)\right)\\
&= \sum_{m\in\mathbb{F}_q} r_\mathfrak{p}^n(m) + \sum_{m\in\mathbb{F}_q} r_\mathfrak{p}^n(m)\left(\frac{(u-m)\,a_{n+1}}{\mathfrak{p}}\right)\\
&= q^n + \left(r_\mathfrak{p}^n(0) - C_n\right)\left(\frac{u\,a_{n+1}}{\mathfrak{p}}\right) + \sum_{m\neq u} C_n\left(\frac{(u-m)\,a_{n+1}}{\mathfrak{p}}\right)\\
&= q^n + \left(r_\mathfrak{p}^n(0) - C_n\right)\left(\frac{u\,a_{n+1}}{\mathfrak{p}}\right).
\end{aligned}$$

Therefore $r_{\mathfrak{p}}^{n+1}(u)$ has the form $C_{n+1} + D_{n+1}\left(\frac{u}{\mathfrak{p}}\right)$ where

$$C_{n+1} = q^n, \qquad D_{n+1} = \left(r_{\mathfrak{p}}^n(0) - C_n\right)\left(\frac{a_{n+1}}{\mathfrak{p}}\right). \tag{9.2}$$

Comparing this with our previous result about $r_{\mathfrak{p}}^n(0)$ we see that in fact (9.1) holds for all $m \in \mathbb{F}_q$ when $D_n = 0$.

Now suppose $r_{\mathfrak{p}}^n(u)$ depends on u (i.e., $D_n \neq 0$). By induction we assume

$$r_{\mathfrak{p}}^n(m) = C_n + D_n\left(\frac{m}{\mathfrak{p}}\right) \tag{9.3}$$

for all $m \in \mathbb{F}_q$. Therefore

$$\begin{aligned} r_{\mathfrak{p}}^{n+1}(\alpha u) &= \sum_{\substack{m,z\in\mathbb{F}_q \\ m+a_{n+1}z=\alpha u}} \left(C_n + D_n\left(\frac{m}{\mathfrak{p}}\right)\right)\left(1+\left(\frac{z}{\mathfrak{p}}\right)\right) \\ &= \sum_{\substack{m,z\in\mathbb{F}_q \\ \alpha m+\alpha a_{n+1}z=\alpha u}} \left(C_n + D_n\left(\frac{\alpha m}{\mathfrak{p}}\right)\right)\left(1+\left(\frac{\alpha z}{\mathfrak{p}}\right)\right) \\ &= \sum_{z\in\mathbb{F}_q} C_n + \sum_{z\in\mathbb{F}_q} C_n\left(\frac{\alpha z}{\mathfrak{p}}\right) + \sum_{m\in\mathbb{F}_q} D_n\left(\frac{\alpha m}{\mathfrak{p}}\right) + \sum_{\substack{m,z\in\mathbb{F}_q \\ m+a_{n+1}z=u}} D_n\left(\frac{\alpha m}{\mathfrak{p}}\right)\left(\frac{\alpha z}{\mathfrak{p}}\right). \end{aligned}$$

By reparameterizing, we see that each of the terms is independent of α. So when $D_n \neq 0$, (9.1) holds and $D_{n+1} = 0$. To compute C_n in this case, we use the formula

$$r_{\mathfrak{p}}^{n+1}(u) = \frac{q^{n+1} - r_{\mathfrak{p}}^{n+1}(0)}{q-1} = q^n - D_n\left(\frac{-a_{n+1}}{\mathfrak{p}}\right). \tag{9.4}$$

All that remains is to determine D_n. Since $D_1 = 1$, we see that $D_{2n} = 0$. When n is odd, substituting (9.4) into (9.2) we obtain the relation $D_{n+1} = q\left(\frac{-a_n a_{n+1}}{\mathfrak{p}}\right)D_{n-1}$, therefore

$$D_{2n+1} = q^n\left(\frac{(-1)^n a_1\cdots a_n}{\mathfrak{p}}\right). \quad \square$$

References

[An-Zh] Andrianov, A. N. and Zhuravlëv, V. G., *Modular forms and Hecke operators*, American Mathematical Society, Providence, RI, 1995, pp. viii+334.

[At-Le] Atkin, A. O. L. and Lehner, J., *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[Ca] Cassels, J. W. S., *Rational quadratic forms*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1978, pp. xvi+413.

[Ci] Cipra, B. A., *On the Niwa-Shintani theta-kernel lifting of modular forms*, Nagoya Math. J. **91** (1983), 49–117.

[Co-Iw] Conrey, J. B. and Iwaniec, H., *The cubic moment of central values of automorphic L-functions*, Ann. of Math. **151** (2000), no. 3, 1175–1216.

[C-S] Conway, J. H. and Sloane, N. J. A., *Sphere packings, lattices and groups, 3rd ed.*, Springer-Verlag, New York, 1999, pp. preface+703.

[De] Deligne, P., *La conjecture de Weil. I.*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307. (French)

[Du-SP] Duke, W. and Schulze-Pillot, R., *Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids*, Invent. Math. **99** (1990), 49–57.

[Ha1] Hanke, J., *QFLib package for Pari/GP.*

[Ha2] ———, *On a local-global principle for quadratic forms* (to appear).

[Hs] Hsia, J. S., *Representations by spinor genera*, Pacific J. Math **63** (1976), no. 1, 147–152.

[Hs-Ic] Hsia, J. S. and Icaza M. I., *Effective version of Tartakowski's theorem*, Acta Arith. **89** (1999), no. 3, 235–253.

[Ig] Igusa, J., *Forms of higher degree*, Tata Institute of Fundamental Research, Bombay, 1978, pp. iv+175.

[Kn] Kneser, M., *Darstellungmaße indefiniter quadratischer Formen*, Math Z. **77** (1961), 188–194.

[Ku-Ra1] Kudla, S. and Rallis, S., *On the Siegel-Weil formula*, J. Reine Angew. **387** (1988), 1–68.

[Ku-Ra2] ———, *On the Siegel-Weil formula II: the isotropic convergent case*, J. Reine Angew. **391** (1988), 65–84.

[M-H] Milnor, J. and Husemoller, D., *Symmetric bilinear forms*, Springer-Verlag, New York, 1973, pp. viii+147.

[OM] O'Meara O. T., *Introduction to Quadratic Forms*, Springer-Verlag, Berlin, 2000, pp. xiv+342.

[O-S] Ono, K. and Soundararajan, K., *Ramanujan's ternary quadratic form*, Invent. Math. **130** (1997), no. 3, 415–454.

[Ra] Rallis, S, *L-functions and the Oscillator Representation*, Lecture Notes in Math., vol. 1254, Springer-Verlag, New York, 1987.

[SP1] R. Schulze-Pillot, *Darstellung durch Spinorgeschlechter ternärer quadratischer Formen*, J. Number Theory **12** (1980), no. 4, 529–540. (German)

[SP2] ———, *Thetareihen positiv definiter quadratischer Formen*, Invent. Math. **75** (1984), no. 2, 283–299. (German)

[SP3] ———, *On explicit versions of Tartakovski's Theorem*, Arch. Math. **77** (2001), 129–137.

[Si] C. L. Siegel, *Über die Analytische Theorie der Quadratischen Formen*, Ann. of Math. **36** (1935), no. 3, 527–606. (German)

[Sh] G. Shimura, *On modular forms of half-integral weight*, Ann. of Math. **97** (1973), 440–481.

[VB] Van der Blij, F., *On the theory of quadratic forms*, Ann. of Math. **50** (1949), 875–899.

[Wa] Watson, G. L., *Quadratic Diophantine equations*, Philos. Trans. Roy. Soc. London Ser. A **253** (1960/1961), 227–254.