On the Number of Representations of Integers by Quadratic Forms

Hunter Liu

1 Introduction and Background

There is a deep field of mathematics that's centred on the study of quadratic forms, and perhaps the simplest is the question of which integers are representable as the sum of two squares? Or, if one wishes to add more flavour, which squares and which primes are sums of two squares? More generally, which numbers are expressible as the sum of n squares?

Most generally, this type of question can be extended to quadratic forms. For the purposes of this paper,

Definition: *A quadratic form in n variables is a function of the form*

$$Q(x) = Q(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j,$$

where $x = (x_1, \ldots, x_n)$ and a_{ij} are integers. Q is said to be positive-definite if $Q(x) > 0$ whenever each $x_i \neq 0$, negative-definite if $Q(x) < 0$ whenever each $x_i \neq 0$, and indefinite otherwise.

Here, we shall note that the theory we shall be developing is not confined to reals, rationals, and integers; this definition can be carried over to any field, and the analogous question of solutions in the ring of algebraic integers of that field is similarly rich and interesting. Special care and psychological caution must be taken in characteristic 2. [7] gives a thorough treatment of quadratic forms in the general setting, though we will not stray far from $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$.

The question now becomes, given a positive definite quadratic form Q and an integer k, does $Q(x) = k$ for $x \in \mathbb{Z}^n$ have a solution? If such a solution exists, we say Q represents k.

To such a quadratic form one often associates the symmetric matrix B whose diagonal entries are $b_{ii} = a_{ii}$ and whose off-diagonals are $b_{ij} = b_{ji} = \frac{1}{2}a_{ij}$. This way, $Q(x) = x^\top Bx$. Often, we will abuse notation and use Q to refer to both the quadratic form and the matrix associated to Q; in other words, we shall identify Q with its matrix B.

Inklings of a local-global principle for this problem arises when one realises that if $Q(x) = k$ has an integer solution, then $Q(x) \equiv k \bmod m$ has a solution for all m. Equivalently, $Q(x) = k$ has a solution in the local fields $\mathbb{Z}_p$ and in $\mathbb{R}$ if $Q(x) = k$ has an integer solution. One would very, very much like the converse to hold, but $Q(x, y) = 5x^2 + 11y^2$ is a common counterexample. Nevertheless, there is a slightly less satisfying yet still astounding local-to-global principle.

Definition: *Let Q and Q' be two quadratic forms. Q and Q' are said to be equivalent (over the integers) if there exists an orthonormal integer matrix S such that $S^\top Q' S = Q$. The set of all matrices equivalent to Q is called the class of Q, denoted* $\mathrm{cl}\left(Q\right)$.

Q and Q' are equivalent over $\mathbb{Z}_p$ if there exists an orthonormal matrix S with entries in $\mathbb{Z}_p$ such that $S^\top Q' S = Q$. Q and Q' are said to lie in the same genus if they are equivalent over $\mathbb{Z}_p$ for all p; the genus of Q is the set of all matrices lying in the same genus as Q, denoted $\mathrm{gen}\left(Q\right)$.

The question of representations $Q\left(x\right) = k$ really only depends on the class of Q, and there are local-to-global results involving the genus of Q.

Theorem (The Hasse-Minkowski Principle)**:** *Two forms Q and Q' are equivalent over $\mathbb{Z}$ if and only if they lie in the same genus and they are equivalent over $\mathbb{R}$.*

Theorem: *Suppose $Q\left(x\right) = k$ has a solution over $\mathbb{Z}_p$ for all p. Then, there exists some $Q' \in \mathrm{gen}\left(Q\right)$ such that $Q'\left(x\right) = k$ has an integer solution.*

This more or less answers the question of the existence of an integral representation $Q\left(x\right) = k$. A natural extension of this question, and the main topic of our discussion, is the question of *how many* different solutions to $Q\left(x\right) = k$ there are. For some equations, such as $x^2 + y^2 = 0$, the answer is obvious, but answering this question in its full generality was not achieved until the 1900's.

To formalise the problem, we are interested in computing

$$r_Q\left(k\right) := \left|\left\{x \in \mathbb{Z}^n : Q\left(x\right) = k\right\}\right|,$$

where Q is a positive-definite quadratic form in n variables and k is an integer.

2 A "Classical" Approach

We'll consider first the number of representations of an integer k by the sum of n squares. The quadratic form in question is $Q\left(x\right) = \sum_{i=1}^{n} x_i^2$, and the corresponding matrix is the $n \times n$ identity matrix. We write $r_n\left(k\right)$ for the number of representations of k rather than $r_Q\left(k\right)$ to highlight later dependences on n.

A common approach to such a problem is to use the famous circle method. Let $\theta\left(z\right) = \sum_{k\in\mathbb{Z}} z^{k^2}$; then, this forms a generating series

$$\left(\theta\left(z\right)\right)^n = \sum_{k_1,\ldots,k_n\in\mathbb{Z}} z^{k_1^2+\cdots+k_n^2} = \sum_{k=0}^{\infty} r_n\left(k\right) z^k,$$

and the representation numbers $r_n(k)$ can be extracted by integrating

$$r_n(k) = \frac{1}{2\pi i} \oint \left(\theta(z)\right)^n z^{-k-1} \,\mathrm{d}z$$

around a circle centred at the origin for $k \geq 1$; note that $r_n(0) = 1$ for all n. Of course, $r_n(k)$ is bounded by a polynomial in k, and so $\theta(z)$ converges whenever $|z| < 1$. We let the contour get close to the unit circle, which will allow us to directly evaluate the integral in arcs centred at rational angles. We shall sketch the process but omit some details and computations for brevity; a nearly complete treatment is available in [5].

One may rewrite the integral with $z = Re(-kt)$ for a real parameter t so that

$$r_n(k) = \int_0^1 \left(\theta\left(Re(t)\right)\right)^n R^{-k} e(-kt)\,\mathrm{d}t;$$

for some fixed positive real number $R < 1$, to be made arbitrarily close to 1. Here, $e(x) = e^{2\pi i x}$, per usual. Then, one approximates the integral near rational points $0 \leq \frac{a}{b} < 1$ with a, b coprime. This transforms the integral to the form

$$r_n(k) = \frac{1}{2\pi i} \sum_{a,b} R^{-k} \int \left(\theta\left(Re\left(\frac{a}{b} + \phi\right)\right)\right)^n e\left(-k\left(\frac{a}{b} + \phi\right)\right) \mathrm{d}\phi.$$

This argument (given first by Hardy) differs slightly from the "usual" circle method in that the integrals around the rationals completely cover the unit circle. Specifically, if ϕ_1 and ϕ_2 are consecutive rational points in the approximation, then the arcs centred at ϕ_1 and ϕ_2 meet at the midpoint $\frac{1}{2}(\phi_1 + \phi_2)$. By increasing the number of rational points, the arc length is decreased, and this turns out to be good enough for our purposes. Thus, we need not worry about any errors from the nonexistent "minor arcs".

A factor of $e\left(-\frac{ka}{b}\right)$ may be brought out of the integral, and one expands

$$\theta\left(Re\left(\frac{a}{b} + \phi\right)\right) = \sum_{k\in\mathbb{Z}} R^{k^2} e\left(\frac{ak^2}{b} + k^2\phi\right).$$

The $e\left(\frac{ak^2}{b}\right)$ is nearly reminiscent of a Gauss sum, whose precise value is actually known, were it not for k being summed over all integers. The trick is to reorder the sum by writing $k = lb + m$, where l ranges over all integers and m ranges over $0, \ldots, b-1$. Summing over l first, applying the Poisson summation formula, and rewriting $Re(\phi) = e^{2\pi(-\delta + i\phi)}$ for some $\delta > 0$ small yields

$$\theta\left(Re\left(\frac{a}{b} + \phi\right)\right) = \frac{1}{b\sqrt{2\tau}}\left(G(a,b) + H(a,b;\tau)\right),$$

where $\tau = -\delta + i\phi$, $G(a,b) = \sum_{m=0}^{b-1} e\left(\frac{ak^2}{b}\right)$ is the Gauss sum, and

$$H(a,b;\tau) = \sum_{l\neq 0} \exp\left(\frac{-\pi l^2}{2b^2\tau}\right) \sum_{m=0}^{b-1} e\left(\frac{am^2+lm}{b}\right).$$

Upon expanding θ^n, one gets a term involving $\frac{G^n}{b^n(2\tau)^{n/2}}$, and many terms mixing powers of G and H. For an optimal choice of R or δ, which only depends on the number of major arcs, one is able to approximate

$$r_n(k) = \frac{1}{2\pi i}\sum_{a,b} e\left(-\frac{ak}{b}\right)\int\left(\frac{G(a,b)}{b\sqrt{2\tau}}\right)^n e^{2\pi k\tau}\,\mathrm{d}\phi + O\left(k^{\frac{n}{4}}\right).$$

Note that $G(a,b)$ does not depend on ϕ. What remains to be unpacked is the integral $\int \tau^{-\frac{n}{2}} e^{2\pi k\tau}\,\mathrm{d}\phi$ along the major arcs, and using the optimal choice of R or δ with sufficiently many arcs, these integrals may be approximated with an error of $O\left(k^{\frac{n}{4}}\right)$ as well. The techniques and computations are covered in full detail in [5]. The result is as follows:

Theorem: *For $n \geq 5$,*

$$r_n(k) = \frac{\pi^{\frac{n}{2}} k^{\frac{n}{2}-1}}{\Gamma\left(\frac{n}{2}\right)} \sum_{q=1}^{\infty} A_q(k,n) + O\left(k^{\frac{n}{4}}\right),$$

where

$$A_q(k,n) = q^{-n} \sum_{\substack{a \bmod q \\ \gcd(a,q)=1}} G(a,q)^n\, e\left(\frac{ak}{q}\right).$$

The sum over q is known as the "singular series". For $n = 1, 2$, a technical issue in approximating the integral $\int \tau^{-\frac{n}{2}} e^{2\pi k\tau}\,\mathrm{d}\phi$ arises and invalidates the proof.

Since $\left|G(a,q)\right| = \sqrt{q}$, we see that $\left|A_q\right| \leq q^{1-\frac{n}{2}}$. This is a rather crude upper bound, but it demonstrates that care is needed when handling the series when $n < 5$ due to convergence issues. In addition, when $n < 5$ the error term becomes comparable to the main term; the result $r_4(k) = O(k)$ is rather underwhelming, for instance.

Surprisingly, for $3 \leq n \leq 8$ one can show an *exact* result as follows:

Theorem: *If $3 \leq n \leq 8$,*

$$r_n(k) = \frac{\pi^{\frac{n}{2}} k^{\frac{n}{2}-1}}{\Gamma\left(\frac{n}{2}\right)} \sum_{q=1}^{\infty} A_q(k,n).$$

For $5 \leq n \leq 8$, Estermann [4] provided a proof by constructing a cusp form whose coefficients were related to both sides of the above equation. He then applied a dimensionality argument to equate the two sides. For $n = 3, 4$, the problem amounts to verifying equations; special care is needed due to covergence issues with the singular series, and [1] gives a thorough overview of these arguments. For $n = 2$, the formula is off by a factor of 2, and for $n = 1$ the formula is rather trivial. For $n > 8$, the error term is sometimes nonzero, making the exact formula fail.

3 The Singular Series and Obstacles to Generalisations

Although the singular series looks intractible, it is in fact possible to evaluate it with some work. In the following discussion, we shall fix n and k, abbreviate $A_q = A_q(k, n)$, and $\mathscr{S} = \sum_{q=1}^{\infty} A_q$ for the singular series.

Proposition: *If q_1 and q_2 are coprime, then $A_{q_1q_2} = A_{q_1}A_{q_2}$. In other words, A_q is multiplicative.*

Proof. Substitute and expand:

$$A_{q_1}A_{q_2} = (q_1q_2)^{-n} \sum_{\substack{a_1 \bmod q_1 \\ (a_1,q_1)=1}} \sum_{\substack{a_2 \bmod q_2 \\ (a_2,q_2)=1}} G(a_1, q_1)^n \, G(a_2, q_2)^n \, e\left(-k \cdot \frac{a_1q_2 + a_2q_1}{q_1q_2}\right).$$

Writing $a = a_1q_2 + a_2q_1$, it's easily seen that a ranges over all residues mod q_1q_2 coprime to q_1q_2 by coprimality of q_1 and q_2. Expanding the Gauss sums lets us rewrite

$$\begin{aligned} &= (q_1q_2)^{-n} \sum_{\substack{a \bmod q_1q_2 \\ (a,q_1q_2)=1}} G(a, q_1q_2)^n \, e\left(-\frac{ak}{q_1q_2}\right) \\ &= A_{q_1q_2}. \end{aligned}$$

□

Corollary: *Let $\mathscr{S}_p = \sum_{j=0}^{\infty} A_{p^j}$. Then, $\mathscr{S} = \prod_p \mathscr{S}_p$, where the product ranges over all primes p.*

This already suggests a local-global correspondence, and we shall now explore more of what $\mathscr{S}_p$ represents.

Consider any fixed prime p. Let us now analyse A_p by directly expanding the Gauss sums in the definition. We have

$$\begin{aligned} A_p &= p^{-n} \sum_{a=1}^{p-1} \left(\sum_{x=0}^{p-1} e\left(\frac{ax^2}{p} \right) \right)^n e\left(-\frac{ak}{p} \right) \\ &= p^{-n} \sum_{a=1}^{p-1} \sum_{x_1,\ldots,x_n=0}^{p-1} e\left(\frac{a}{p} \left(x_1^2 + \cdots + x_n^2 \right) \right) e\left(-\frac{ak}{p} \right) \\ &= p^{-n} \sum_{x_1,\ldots,x_n=0}^{p-1} \sum_{a=1}^{p-1} e\left(\frac{a}{p} \left(x_1^2 + \cdots + x_n^2 - k \right) \right) \end{aligned}$$

Notice that the inner sum is just 0 if $p \nmid x_1^2 + \cdots + x_n^2 - k$ and that it's $p-1$ otherwise. Hence, A_p is detecting the number of solutions to $x_1^2 + \cdots + x_n^2 \equiv k \bmod p$! Written another way, this becomes

$$= p^{-n} (p-1) \left| \left\{ (x_1, \ldots, x_n) \in \left(\mathbb{Z}/p\mathbb{Z} \right)^n : x_1^2 + \cdots + x_n^2 \equiv k \bmod p \right\} \right|$$

This analysis generalises to prime powers (and any integer in fact). It can be shown with some effort that the number of solutions modulo p^j eventually stabilises for sufficiently large j, and so the sum $\sum_{j=0}^{\infty} A_{p^j}$ telescopes towards the tail and truly does converge. In a sense, $\mathscr{S}_p$ can be thought of detecting the number of *local* solutions in $\mathbb{Z}_p$, weighted against some normalising factors of p^{-nj}. Rewriting the earlier result, we see

$$r_n(k) = \frac{\pi^{\frac{n}{2}} k^{\frac{n}{2}-1}}{\Gamma\left(\frac{n}{2}\right)} \prod_p \mathscr{S}_p(k,n) + O\left(k^{\frac{n}{4}}\right)$$

provides a *quantitative* local-to-global relationship for the representation of k as a sum of n squares.

It's natural to worder if this quantitative relationship can be extended to $r_Q(k)$ for a general quadratic form Q in n variables, but we run into significant obstructions when attempting to adapt the above techniques to a more general setting. Our generating function now becomes

$$\theta_Q(z) = \sum_{x \in \mathbb{Z}^n} z^{Q(x)} = \sum_{k \geq 0} r_Q(k) z^k.$$

But analysing and integrating this function is significantly more difficult than analysing θ^n from the previous section.

Another significant limitation is that the local data of $\mathscr{S}_p(k,n)$ gives information about the representations of k by the *genus* of $x_1^2 + \cdots + x_n^2$ while $r_n(k)$ only depends on the *class* of this form. Yet the genus and the class are very rarely the same; the number of equivalence classes occupying a form is seldom equal to 1. Indeed, Watson [12] showed that any positive-definite quadratic form in more than 10 variables has more than one class in its genus.

It is, in fact, true that a *precise* local-to-global quantitative relationship does hold, so long as one takes into consideration the dependence of the local data on the genus rather than the class. This is one interpretation of the Smith-Minkowski-Siegel mass formula, which we shall explore next.

4 The Smith-Minkowski-Siegel Mass Formula

We will eventually state this formula, but the proof is extraordinarily elaborate and is well beyond the scope of the author's IQ. Siegel [10] provides a complete proof of the theorem, and he additionally provides generalisations to the indefinite case and to arbitrary number fields. In addition, [9] contains a more rigourous discussion and thorough proof of the indefinite case. [2] provides a more practical statement of the theorem, alongside some interesting history and commentary that is worth reading.

First, we shall define and consider a genus-invariant version of $r_Q(k)$.

Definition: *Let Q be a positive-definite quadatric form in n variables. Then define* $\mathrm{Aut}(Q) = \left\{X \in GL(n, \mathbb{Z}) : X^\top Q X = Q\right\}$*. The weight or mass of Q is defined as*

$$w(Q) = \sum_{Q' \in \mathrm{gen}(Q)} \frac{1}{\left|\mathrm{Aut}(Q)\right|}.$$

Note that this definition is well-defined: on one hand, $\mathrm{gen}(Q)$ is finite, for one may observe that the discriminant of any two matrices in the same genus are equal. Second, $\left|\mathrm{Aut}(Q)\right|$ is finite for any (positive definite) Q.

The idea is as follows: provide a generalisation of the singular series $\mathscr{S} = \prod_p \mathscr{S}_p$ to arbitrary positive definite quadratic forms. These $\mathscr{S}_p$'s should loosely measure the solvability of $Q(x) = k$ in $\mathbb{Z}_p$. As seen before, solvability over $\mathbb{Z}_p$ for all p and in $\mathbb{R}$ corresponds to a solution $\mathbb{Z}$ for some $Q' \in \mathrm{gen}\, Q$, so $\prod_p \mathscr{S}_p$ should estimate the "average" number of representations among quadratic forms in the genus.

To this end, define the "local densities" as follows: let

$$d_\infty(Q, k) = \lim_{U \to \{k\}} \frac{\mathrm{Vol}\left(Q^{-1}(U)\right)}{\mathrm{Vol}(U)},$$

where we are treating Q as a function $\mathbb{R}^n \to \mathbb{R}$, the limit is taken on open sets (relative to the Euclidean topology) converging to $\{k\}$, and Vol is the standard Lebesgue volume.

The number of representations of k by Q is equal to the number of integer lattice points lying on $Q^{-1}(U)$, which is the surface of an ellipsoid. d_∞, loosely speaking, approximates the "density" of such lattice points by comparing volumes. This limit is not difficult to compute, and it turns out to be

$$d_\infty (Q,k) = \frac{\pi^{\frac{n}{2}} k^{\frac{n}{2}-1}}{\Gamma\left(\frac{n}{2}\right)\sqrt{\det Q}}.$$

The exact same definition can be adapted to define the p-adic densities d_p, where the limit is instead taken over the p-adic topology and Vol is defined using the Haar measure on $\mathbb{Z}_p$ and $\mathbb{Z}_p^n$. Fortunately, this bulky definition is re-expressible as

$$d_p (Q,k) = \lim_{j\to\infty} p^{-nj} \left| \left\{ x \in \mathbb{Z}^n \bmod p^j : Q(x) \equiv k \bmod p^j \right\} \right|.$$

This is quite literally a measurement of the p-adic density of representations: there are p^{nj} possible values of $x \in \mathbb{Z}^n \bmod p^j$, and the numerator is the exact number of solutions. Note that d_2 is a special case and needs an additional factor of $\frac{1}{2}$ in its definition. This reflects the fact that $1 \equiv -1 \bmod 2$, and so there is some degree of "overcounting" to be attenuated.

The p-adic density is well-defined: for sufficiently large powers of p, the ratio actually stabilises, as each solution mod p^j will lift to p^n solutions mod p^{j+1}. In fact, the $\mathscr{S}_p$'s from earlier are precisely the p-adic densities as defined above!

Theorem: *Let Q be a positive-definite quadratic form in n variables and k an integer. Then,*

$$w(Q)^{-1} \sum_{Q' \in \mathrm{gen}(Q)} \frac{r_{Q'}(k)}{\left|\mathrm{Aut}(Q')\right|} = \epsilon_n d_\infty (Q,k) \prod_{p \text{ prime}} d_p (Q,k),$$

where $\epsilon_n = \frac{1}{2}$ if $n = 1,2$ and $\epsilon_n = 1$ otherwise.

The corrective factor of ϵ_n reflects special structure of certain matrix groups, and it is connected to their Tamagawa numbers. A better and more detailed discussion of this is well beyond the intellectual capacity of the author.

If a quadratic form Q satisfies $\mathrm{cl}\, Q = \mathrm{gen}\, Q$, i.e. its genus consists of a single class, then the left hand side reduces to just $r_Q(k)$. This allows us to recover some formulae that were known before this formula by computing d_p directly, such as:

Theorem (Jacobi)**:** *Let k be a nonnegative integer. Then*

$$r_4(k) = \begin{cases} 8\sum_{m|k} m & 2 \nmid k \\ 24\sum_{m|k} m & 2 \mid k. \end{cases}$$

Theorem: *For every odd prime $p \equiv 1 \bmod 4$, there exist unique nonnegative integers x, y such that $x^2 + y^2 = p$.*

More general explicit formula for $r_n(k)$ are available with some additional work; we refer the reader to [10] and [5] for the details.

Here, we will say that the mass formula generalises beyond representations of integers by quadratic forms. If Q and P are quadratic forms in n and m variables, repsectively, we say that Q represents P if there exists some $n \times m$ integer matrix X such that $X^\top QX = P$; when $m = 1$, this degenerates to the representation of integers again. Then $r_Q(P)$ and the local densities are defined analogously in this setting, and we have:

Theorem (The Smith-Minkowski-Siegel Mass Formula)**:**

$$w(Q)^{-1} \sum_{Q' \in \text{gen}(Q)} \frac{r_{Q'}(P)}{|\text{Aut}(Q')|} = \epsilon_{n,m} d_\infty(Q,P) \prod_{p \text{ prime}} d_p(Q,P),$$

where $\epsilon_{n,m} = \begin{cases} \frac{1}{2} & n = m, m+1 \\ 1 & \textit{otherwise.} \end{cases}$

5 Reinterpretations in Terms of Lattices

In this section, we briefly cover a reinterpretation of the theory in terms of lattices rather than quadratic forms. The two lie in a close correspondence, and many of the results can be restated in terms of lattices; within this language, however, other connections and applications become clearer. We shall present the material in far less detail, however. We refer the reader to [6] for an expository overview of this connection and [7] for a fuller discussion and development of the theory from the lattice-centric perspective.

As with quadratic forms, the definitions can easily be generalised to arbitrary rings and fields (except in characteristic 2, where extra care is needed). And continuing the theme here, we will only really develop the theory in characteristic 0, particularly over $\mathbb{Z}$ and $\mathbb{Q}$.

Definition: *Let $M \cong \mathbb{Z}^n$ be a free $\mathbb{Z}$-module. A quadratic form on M is a map $q : M \to \mathbb{Z}$ such that (i) $q(cx) = c^2 q(x)$ for all $c \in \mathbb{Z}$ and $x \in M$, and (ii) $b(x,y) = q(x+y) - q(x) - q(y)$ is a symmetric bilinear form. The pair (M,q) is called a quadratic module.*

If (M,q_1) and (N,q_2) are quadratic modules, an injective $\mathbb{Z}$-module homomorphism $\varphi : M \hookrightarrow N$ is called an isometry if $q_1(x) = q_2 \circ \varphi(x)$ for all $x \in M$. If such an isometry exists, we say M is represented by N. In addition, if φ is surjective (and thus an isomorphism), we say M and N are isometric.

Replacing $\mathbb{Z}$ with $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Q}_p$, etc. in the above definition gives a more complete definition of a quadratic module. This definition has no immediate issues with characteristic 2, but some properties and results about quadratic forms need to be revised to fit characteristic 2.

Note that there is a natural way to extend a quadratic module over $\mathbb{Z}$ to a quadratic module over $\mathbb{Q}$ by taking the fraction field; this can further be extended to quadratic modules over $\mathbb{R}$ or $\mathbb{Q}_p$ via completions and extensions of scalars.

To make sure that the notion representation is consistent with what we have been doing, consider the quadratic module $(\mathbb{Z}, q_k)$, where $q_k(x) = kx^2$ for any $x \in \mathbb{Z}$, and also $(\mathbb{Z}^n, q)$, where $q\left(x_1, \ldots, x_n\right) = \sum x_i^2$. By the above definition, q_k is represented by q if there exists some embedding $\varphi : \mathbb{Z} \to \mathbb{Z}^n$ such that $q_k = q \circ \varphi$; evaluating at $x = 1$ indicates that there must be some $x_1, \ldots, x_n \in \mathbb{Z}^n$ such that $k = q_k\left(1\right) = q\left(x_1, \ldots, x_n\right) = \sum x_i^2$. This coincides with our previous definition of "k is represented by the sum of n squares", and likewise for more general quadratic forms of more than one variable.

Of course, the notion of "isometric quadratic modules" corresponds to the notion of "equivalent quadratic forms": an isomorphism of quadratic modules is a $\mathbb{Z}$-linear automorphism of $\mathbb{Z}^n$, which is just a linear change of variables. After reframing local densities in the language of quadratic modules, one can create a one-to-one translation of the Smith-Minkowski-Siegel mass formula.

We now turn to a related and more concrete geometric idea:

Definition: *A lattice in $\mathbb{R}^n$ is a free $\mathbb{Z}$-submodule of $\mathbb{R}^n$ of rank n.*

We may define the volume of a lattice as the usual volume of a fundamental domain; this is equivalently the determinant of a matrix whose columns form a basis of the lattice (up to a sign).

In addition, each lattice can be endowed with the structure of a quadratic module. Let $\Lambda \subset \mathbb{R}^n$ be a lattice, and pick a $\mathbb{Z}$-basis $v_1, \ldots, v_n$. This induces an isomorphism $\Lambda \cong \mathbb{Z}^n$. For any $\left(x_1, \ldots, x_n\right) \in \mathbb{Z}^n$, the function

$$q\left(x_1, \ldots, x_n\right) = \sum_{1 \leq i,j \leq n} x_i x_j \left(v_i \cdot v_j\right)$$

defines a quadratic form on $\mathbb{Z}^n$, where $\cdot$ is the usual dot product. It is positive definite because it is $\mathbb{R}$-equivalent to the sum of n squares: one can "move" the basis to be orthogonal.

Dirichlet's analytic class number formula is often presented via a correspondence between ideal classes and quadratic forms; however, this can obscure a geometric shade to the proof. We present the following correspondence:

$$\left\{\begin{matrix}\text{Ideal Classes}\\ \text{in } \mathbb{Q}\left(\sqrt{-D}\right)\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{Lattices of}\\ \text{“Volume } D\text{”}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{Quadratic forms of}\\ \text{“Discriminant } D\text{”}\end{matrix}\right\}$$

(Some corrective factors may be needed for the volume and discriminant, hence the quotations.)

For some actual discussion and applications of the formula in such a context, please see [8], who produces a general class number formula for certain algebraic extensions of $\mathbb{Q}$ beyond just quadratic imaginary extensions.

In addition, the formula has seen extensive use in geometric applications; see [3] for a very comprehensive overview, wherein chapters 15 and 16 develop our above discussion with a geometric focus. Venkatesh [11] later found an application of the formula to finding highly symmetric high-dimensional lattices, and this led to significant progress in the sphere packing problem.

6 Conclusion

With this, we conclude our cursory survey of the Smith-Minkowski-Siegel mass formula. Although we have only dealt with positive-definite quadratic forms, a generalisation to the indefinite case was also provided by Siegel [9]. No one source seems to consolidate every case and statement of the theorem.

The formula could perhaps appear, at first glance, to be highly specific and niche, yet as we have seen in the above discussion, it sees a surprising amount of flexibility, generality, and applicability. We hope this has demonstrated at least a shade of the incredible depth of the formula.

References

[1] Paul T. Bateman. "On the Representations of a Number as the Sum of Three Squares". In: *Transactions of the American Mathematical Society* 71.1 (1951), pp. 70 –101.

[2] J. H. Conway and N. J. A. Sloane. "Low-Dimensional Lattices. IV. The Mass Formula". In: *Proceedings of the Royal Society of London* 419.1857 (1988), pp. 259 –286.

[3] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices, and Groups.* 3rd ed. Springer-Verlag, 1999.

[4] T. Estermann. "On the Representations of a Number as a Sum of Squares". In: *Proceedings of the London Mathematical Society* s3-9 (4 Oct. 1959), pp. 575 –594.

[5] Emil Grosswald. *Representations of Integers as Sums of Squares.* Springer-Verlag, 1985.

[6] Jonathan Hanke. *Notes on "Quadratic Forms and Automorphic Forms" from the 2009 Arizona Winter School.* 2012.

[7] Yoshiyuki Kitaoka. *Arithmetic of Quadratic Forms.* Cambridge Tracts in Mathematics. Cambridge University Press, 1993.

[8] Goro Shimura. "Quadratic Diophantine Equations, the Class Number, and the Mass Formula". In: *Bulletin of the American Mathematical Society* 43.3 (July 2006), pp. 285 –304.

[9] C. L. Siegel and K. G. Ramanathan. *Lectures on Quadratic Forms.* Tata Institute of Fundamental Research, Bombay, 1957.

[10] C. L. Siegel and Morgan Ward. *Lectures on the Analytical Theory of Quadratic Forms: Second Term, 1934/35.* Institute for Advanced Study and Princeton University. R. Peppmüller, 1963.

[11] Akshay Venkatesh. "A Note on Sphere Packings in High Dimension". In: *International Mathematics Research Notices* 2013 (7 2013), pp. 1628 –1642.

[12] G. L. Watson. "The Class-Number of a Positive Definite Quadratic Form". In: *Proceedings of the London Mathematical Society* s3-13 (1 1963), pp. 549–576.