ON THE ANALYTIC THEORY OF ISOTROPIC TERNARY QUADRATIC FORMS

By

WILLIAM DUKE

WITH AN APPENDIX BY RAINER SCHULZE-PILLOT

To Peter Sarnak, on the occasion of his seventieth birthday

Abstract. A new local-global result about the primitive representations of zero by integral ternary quadratic forms is proven. By an extension of a result of Kneser (given in the Appendix), it yields a quantitative supplement to the Hasse principle on the number of automorphic orbits of primitive zeros of a genus of forms. One ingredient in its proof is an asymptotic formula for a count of the zeros of a given form in such an orbit.

1 Introduction

Let S be a symmetric 3×3 matrix with integral entries and with $\det S = D > 0$. Associated to S is the nonsingular ternary quadratic form

$$S(x) := xSx^t,$$

where $x = (x_1, x_2, x_3)$. All ternary quadratic forms we consider here are assumed to arise this way. We will sometimes refer to them simply as forms. Two forms S, S' are said to be in the same **class** if there is an $A \in \mathrm{GL}_3(\mathbb{Z})$ such that

$$S[A] := A^t SA = S'. \tag{1.1}$$

They are in the same **genus** if, for any prime p or $p = \infty$, there is an $A \in \mathrm{GL}_3(\mathbb{Z}_p)$ such that (1.1) holds. Here $\mathbb{Z}_\infty = \mathbb{R}$. The genus G of S consists of finitely many, say h, classes. Forms in the same genus have the same determinant.

The form S is **isotropic** if and only if $S(x) = 0$ has primitive solutions $x \in \mathbb{Z}^3$. Hasse's principle applied to S says that S is isotropic if and only if $S(x) = 0$ is non-trivially solvable over $\mathbb{Z}_p$ for all primes p and $p = \infty$. This result is equivalent to Legendre's theorem, which states that for abc square-free the equation

$$ax_1^2 + bx_2^2 + cx_3^2 = 0 \tag{1.2}$$

JOURNAL D'ANALYSE MATHÉMATIQUE, Vol. 151 (2023)
DOI 10.1007/s11854-023-0324-x

has primitive solutions if and only if a, b, c are not all of the same sign and $-bc$, $-ac$, $-ab$ are quadratic residues modulo $|a|$, $|b|$, $|c|$, respectively.[1] The Hasse principle implies that isotropy is a property of the genus of S.

A **primitive representation of zero** by an isotropic form S is a pair (x, S), with $x \in \mathbb{Z}^3$ primitive such that $S(x) = 0$. Two such (x, S) and (x', S') are **equivalent over** $\mathbb{Z}$ if there exists $A \in \mathrm{GL}_3(\mathbb{Z})$ so that

$$S'[A] = S \quad \text{and} \quad xA^t = x'. \tag{1.3}$$

They are **equivalent over** $\mathbb{Z}_p$ for a prime p (including $p = \infty$) if (1.3) holds with $A \in \mathrm{GL}_3(\mathbb{Z}_p)$. The first goal of this paper is to prove the following supplement to the Hasse principle for isotropic ternary forms.

Theorem 1. *Two primitive representations of zero by ternary quadratic forms are equivalent over $\mathbb{Z}$ if and only if they are equivalent over $\mathbb{Z}_p$ for all p, including ∞.*

Theorem 1, together with Corollary 2 of the Appendix, yields a quantitative result about the orbits of primitive zeros of a genus of ternary forms. Say primitive $x, x' \in \mathbb{Z}^3$ with $S(x) = S(x') = 0$ are in the same $\mathbb{Z}$-orbit if (x, S) and (x', S) are equivalent over $\mathbb{Z}$. Clearly this happens precisely when there is an integral automorph A of S (see (2.1) below) such that $xA^t = x'$. There are at most finitely many, say $c(S)$, such orbits. For a prime p or $p = \infty$ say that these x, x' are in the same $\mathbb{Z}_p$-orbit if (x, S) and (x', S) are equivalent over $\mathbb{Z}_p$. Let $c_p(S)$ denote the number of $\mathbb{Z}_p$-orbits. Here $c_p(S) \neq 1$ for at most finitely many p.

Theorem 2. *For S as above we have*

$$\sum_{S' \in G} c(S') = \prod_p c_p(S), \tag{1.4}$$

where G is the genus containing S.

Theorem 2 is a quantitative version of the Hasse principle for ternary quadratic forms. However, our proof assumes that the form is isotropic; we are using the original Hasse principle and not giving an independent proof of that. Although it has a similar form, Theorem 2 differs from Siegel's main theorem [25] applied to the representation of an integer by an indefinite ternary quadratic form. In (1.4) orbits are counted without the measures of representations or p-adic densities that

[1] Proofs of Legendre's theorem were given by Legendre [20, pp. 509–513], Gauss [11, Art. 294] and Dedekind [5, §156]. See Weil's book [28, Chap. 4.] for a discussion of the early history of Legendre's theorem and for a treatment of its relation to the Hasse principle in the general ternary case (App. I, pp. 339–345).

occur in Siegel's identity. Siegel's main theorem, in any of the forms given in [25] or [26], does not apply to the representation of zero by a ternary isotropic form (see also [17]).

Unlike in the definite case, an indefinite ternary quadratic form often has one class in its genus, that is $h = 1$. In this case it follows from Theorem 1 that two primitive zeros of S are in the same $\mathbb{Z}$-orbit if and only if they are in the same $\mathbb{Z}_p$-orbit for all p. Theorem 2 now implies that

$$c(S) = \prod_p c_p(S).$$

In general, we have that $h = 2^\nu$ for some ν (see [16, Satz 4]). In the following examples, where $h = 1$, it is not difficult to compute $c_p(S)$ directly.

Examples.

(i) When S is an isotropic Legendre equation (1.2) with abc odd and square-free, we have that $c_p(S) = 1$ for each p and hence $h = 1$ and $c(S) = 1$. In particular, there is only one orbit of Pythagorean triples, which is known [1] (see also [4]).

(ii) The Legendre equation

$$S(x) = q^2x_1^2 - qx_2^2 - x_3^2 = 0$$

has the nontrivial solution $(1, 0, q)$. If q is a product of distinct primes each $\equiv 3 \pmod 4$, then for each such p we have $c_p(S) = \frac{p-1}{2}$, with $c_p(S) = 1$ otherwise. Also, it is shown in [22] that $h = 1$ so

$$c(S) = \prod_{p|q} \frac{p-1}{2}.$$

Outline of the Proofs. The result needed to deduce Theorem 2 from Theorem 1 is Corollary 2 in the Appendix. This corollary translates to the language of matrices and forms (an extension of) a theorem of Kneser, which is formulated in terms of lattices and quadratic spaces.

Our proof of Theorem 1 uses an analytic method that compares two asymptotic formulas. These formulas count primitive zeros of an individual form in terms of the size of the zero. The first asymptotic, which follows from one that is well-known, counts all zeros. It is stated in the form we need in §3, as Theorem 4. The second, which is new and of independent interest, restricts the count to an orbit of zeros. It is stated in §3 as Theorem 5. The constants in the leading terms in both are determined in terms of certain local densities. Summing over orbits and the

genus leads to an identity between constants, which is given in Theorem 6. In the derivation of Theorem 6 from Theorems 4 and 5, essential use is also made of the Siegel mass formula, which is recalled in the required form in §2 and applied to an associated Fuchsian group.

That Theorem 6 implies Theorem 1 is shown in §4. Here we also need to invoke Theorem 7 of the appendix.

The proofs of Theorems 4 and 5 occupy the remainder of the paper. In §5 the problem of counting within an orbit is attacked using the theory of Eisenstein series for the associated Fuchsian group. The main result here is Proposition 1. Using some of the machinery set up in §5, in §6 we prove Theorem 4. Then in §7, which contains the most delicate arguments, we compute the local densities needed to complete the proof of Theorem 5. It is noteworthy that, although we must compute the 2-adic density of a certain isotropy subgroup of the orthogonal group of S, we do not need to compute explicitly the 2-adic density of the full orthogonal group of S itself, which is notoriously troublesome. This is due to our use of the orbit-stabilizer theorem in the proof of Theorem 6.

Remarks. The proof we give of Theorem 1 is similar in spirit to the novel approach to Siegel's main theorem given by Eskin, Rudnick and Sarnak in [8], which compares counts in an orbit, obtained more generally in [7], to the full count (see also [2] and [3]). The constant for the full count is a product of local densities, usually obtained by the Hardy-Littlewood circle method, except that in the ternary quadratic case serious convergence problems occur. The circle method is made to work in the homogeneous ternary case (with weights) in [12]. Related methods were introduced in [13] and [6]. The refined circle method can be used to give an alternative proof of Theorem 4.

Acknowledgements. I want to thank Peter Sarnak for sharing valuable insights on the general subject of this paper and also for some helpful specific comments. In addition, I am very grateful to the referee for carefully reading the paper and for suggesting numerous improvements.

2 The associated Fuchsian group and Siegel's mass formula

Suppose that S is indefinite and nonsingular. Let O be the group of **integral automorphs of** S given by

$$O = O(S) = \{A \in \mathrm{GL}_3(\mathbb{Z});\ S[A] = S\}. \tag{2.1}$$

Let $O^+(S)$ be the subgroup of O consisting of those $A \in \mathrm{SL}_3(\mathbb{Z}) \cap O(S)$ that are contained in the connected component of the identity $SO^+(S, \mathbb{R})$ of the special orthogonal group of S. Then $O^+(S)$ is isomorphic to $\Gamma(S) \subset \mathrm{PSL}_2(\mathbb{R})$, a Fuchsian group of the first kind acting on the upper half-plane $\mathcal{H}$. Also, Γ has cusps if and only if S is isotropic. This well-known isomorphism arises by a construction of Fricke–Klein [10]. Another useful reference for this construction is [21].

To summarize, let

$$S_0 = \begin{pmatrix} 0 & 0 & \frac{1}{2} \\ 0 & -1 & 0 \\ \frac{1}{2} & 0 & 0 \end{pmatrix}$$

and for $g = \pm\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ let

$$A_g = \begin{pmatrix} \alpha^2 & 2\alpha\beta & \beta^2 \\ \alpha\gamma & \alpha\delta + \beta\gamma & \beta\delta \\ \gamma^2 & 2\gamma\delta & \delta^2 \end{pmatrix}. \tag{2.2}$$

We have that $\det A_g = (\det g)^3$ and $\operatorname{tr} A_g = (\operatorname{tr} g)^2 - \det g$. Also, for $g, h \in \mathrm{PSL}_2(\mathbb{R})$

$$A_{gh} = A_g A_h \quad \text{and} \quad S_0[A_g] = S_0.$$

Choose B so that $S_0[B] = S$ and for

$$C_g = B^{-1} A_g B \tag{2.3}$$

we have that $\det C_g = (\det g)^3$ and $\operatorname{tr} C_g = (\operatorname{tr} g)^2 - \det g$ as well as

$$C_{gh} = C_g C_h \quad \text{and} \quad S[C_g] = S$$

for $g, h \in \mathrm{PSL}_2(\mathbb{R})$. The map $g \mapsto C_g$ gives a Lie group isomorphism from $\mathrm{PSL}_2(\mathbb{R})$ to $SO^+(S, \mathbb{R})$. Define

$$\Gamma = \Gamma(S) = \{ g \in \mathrm{PSL}_2(\mathbb{R});\ C_g \in \mathrm{Mat}_3(\mathbb{Z}) \}. \tag{2.4}$$

Then Γ is isomorphic to $O^+(S)$.

The co-volume of $\Gamma(S)$ with respect to the usual hyperbolic measure on $\mathcal{H}$

$$v\ (S) = \mathrm{vol}\,(\Gamma(S) \backslash \mathcal{H})$$

is finite. For a prime p let

$$O_p = O_p(S) = \{ A \in \mathrm{GL}_3(\mathbb{Z}_p);\ S[A] = S \} \tag{2.5}$$

and set

$$\delta_p = \delta_p(S) = \lim_{m\to\infty} \frac{1}{2} p^{-3m} \#\{ O_p \,(\mathrm{mod}\, p^m)\} \quad \text{and} \quad \delta_\infty = \frac{\pi}{4D^2}, \tag{2.6}$$

where $D = \det S$. Siegel's mass formula identifies the sum of co-volumes over the genus with the product of these local densities.

Theorem 3 ([25, p. 412 in G.A.])**.**[2] *Let S be indefinite. Then*

$$\sum_{S'\in G} \upsilon\ (S') = 2\delta_\infty^{-1} \prod_p \delta_p^{-1}, \tag{2.7}$$

where the product is over all primes p and the sum is over a complete set of representatives of the genus G.

Using well-known calculations of the local densities from [24] we can express the RHS of (2.7) as a finite product

$$2\delta_\infty^{-1} \prod_p \delta_p^{-1} = \frac{4\pi D^2}{3} \prod_{p|2D} (1 - p^{-2}) \delta_p^{-1}. \tag{2.8}$$

Remark. As noted in [25, p. 413 in G.A.], a version of the mass formula in the indefinite ternary case was found by Humbert [14].

3 Asymptotic formulas

Turning now to the statements of the asymptotic results, let $\mathcal{C}(S)$ be the set of all primitive $x \in \mathbb{Z}^3$ with $S(x) = 0$. Let $S^* = DS^{-1}$ where $D = \det S$ is the **adjugate** of S. Choose $y \in \mathbb{R}^3$ such that $S^*(y) = 4D$. Since the plane determined by $xy^t = T$ for $T > 0$ intersects the cone given by $\{x \in \mathbb{R}^3; S(x) = 0\}$ in an ellipse, there are at most finitely many $x \in \mathcal{C}(S)$ with

$$0 < xy^t \le T.$$

For an illustration see Figure 1.

For a prime p let $\mathcal{C}_p(S)$ be the set of all $x \in \mathbb{Z}_p^3$ with $p \nmid x$ and $S(x) = 0$. Define the **p-adic density** of $\mathcal{C}(S)$ by

$$\sigma_p = \lim_{m\to\infty} p^{-2m} \#\{ \mathcal{C}_p(S) \,(\mathrm{mod}\, p^m)\}. \tag{3.1}$$

A similar definition for the density at infinity σ_∞ yields the value, derived below in §6,

$$\sigma_\infty = \frac{\pi}{2\sqrt{D}}. \tag{3.2}$$

The following asymptotic formula is a consequence of well-known results of [9] and [23]. Details are given in §6.

[2] Our definition of the volume differs from Siegel's by a factor of two.

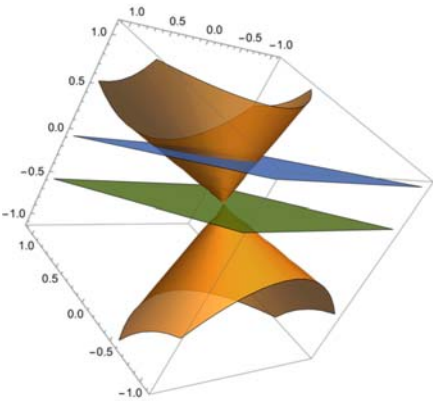

Figure 1.

Theorem 4. *Suppose that S is isotropic. Fix $y \in \mathbb{R}^3$ with $S^*(y) = 4D$. Then, as $T \to \infty$,*

$$\#\{x \in \mathcal{C}(S);\ 0 < xy^t \leq T\} \sim \left(\frac{1}{2}\sigma_\infty \prod_p \sigma_p\right) T. \tag{3.3}$$

Using again [24] and (3.2), the constant in the RHS of (3.3) can be written as

$$\frac{3}{2\pi\sqrt{D}} \prod_{p|2D} (1 - p^{-2})^{-1} \sigma_p. \tag{3.4}$$

Theorem 4 counts rational points of bounded height on the conic $S(x) = 0$. A natural refinement of Theorem 4, whose nature is intrinsically integral rather than rational, counts asymptotically the elements in an orbit under automorphs. For $x \in \mathcal{C}(S)$, its orbit is defined by

$$\mathcal{C}(S, x) = \{x' \in \mathcal{C}(S); x' = xA^t \text{ for some } A \in O(S)\}.$$

Given $x \in \mathcal{C}_p$, the **isotropy subgroup** of $O_p(S)$ from (2.5) that fixes x is given by

$$O_p(S, x) = \{A \in O_p(S);\ xA^t = x\}.$$

Define the **p-adic density**

$$\delta_p(S, x) = \lim_{m \to \infty} \frac{1}{2} p^{-m} \#\{\, O_p(S, x) \pmod{p^m}\}. \tag{3.5}$$

We have the following asymptotic formula.

Theorem 5. *Suppose that S is isotropic with $\det S = D$. Fix $y \in \mathbb{R}^3$ with $S^*(y) = 4D$ and $x \in \mathcal{C}(S)$. Then as $T \to \infty$, we have*

$$\#\{x' \in \mathcal{C}(S,x);\ 0 < x'y^t \le T\} \sim \left(\frac{2D^{\frac{3}{2}}}{v\ (S)} \prod_{p|2D} \delta_p^{-1}(S,x)\right) T. \tag{3.6}$$

By Theorems 4, 5 and (3.4) we get a local identity for the volume by summing over orbits, but not over the genus, of S.

Corollary 1. *For isotropic S*

$$v\ (S) = \frac{4\pi D^2}{3} \sum_x \prod_{p|2D} (1-p^{-2}) \delta_p^{-1}(S,x) \sigma_p^{-1}, \tag{3.7}$$

where x runs over a complete set of representatives of the orbits of $\mathcal{C}(S)$.

The $\mathbb{Z}_p$**-orbit of** $x \in \mathcal{C}_p(S)$ is given by

$$\mathcal{C}_p(S,x) = \{x' \in \mathcal{C}_p(S);\ x' = xA^t \ \text{ for some } \ A \in O_p(S)\}.$$

Define the p**-adic density of the orbit of** x by

$$\sigma_p(S,x) = \lim_{m\to\infty} p^{-2m} \#\{\mathcal{C}_p(S,x) \,(\mathrm{mod}\, p^m)\}. \tag{3.8}$$

By the orbit-stabilizer theorem for all $p|2D$ we have

$$\sigma_p(S,x) = \frac{\delta_p}{\delta_p(S,x)}. \tag{3.9}$$

Let $S = S_1, \dots, S_h$ be a complete set of representatives of the genus G and suppose that $x_{i,j}$ for $i = 1, \dots, c(S_j)$ runs over a complete set of representatives of orbits of $\mathcal{C}(S_j)$, for each j. By Corollary 1, (2.8) from Siegel's mass formula in Theorem 3 and (3.9), we will have the following result once Theorems 4 and 5 are proven.

Theorem 6. *For isotropic S*

$$\prod_{p|2D} \sigma_p = \sum_{j=1}^{h} \sum_{i=1}^{c(S_j)} \prod_{p|2D} \sigma_p(S_j, x_{i,j}). \tag{3.10}$$

4 Classes and genera of primitive representations of zero

This section reduces the proof of Theorem 1 to that of Theorem 6, hence to Theorems 4 and 5. Application is made of Theorem 7, which is given in the

Appendix. I will change slightly the notation there by using x in place of X, to conform with ours. This should not cause confusion. Also, to use the terminology there, say two primitive representations of zero (x, S) and (x', S') are in the same class if they are equivalent over $\mathbb{Z}$ and in the same genus if they are equivalent over $\mathbb{Z}_p$ for all primes p (including $p = \infty$). Thus to prove Theorem 1 it is equivalent to show that a genus of primitive representations of zero by ternary forms contains exactly one class.

For the purpose of counting, it is convenient to express p-adic products in terms of congruences. For $q \in \mathbb{Z}^+$ say that $x \in (\mathbb{Z}/q\mathbb{Z})^3$ is primitive if $\gcd(x, q) = 1$. Let $\mathcal{O}_q(S)$ be the set of primitive $x \in (\mathbb{Z}/q\mathbb{Z})^3$ with $S(x) \equiv 0 \pmod q$. Then $\mathcal{O}_q(S)$ splits into orbits under the group of automorphs modulo q:

$$\{A \in \mathrm{GL}_3(\mathbb{Z}/q\mathbb{Z});\ S[A] \equiv S \,(\mathrm{mod}\, q)\}.$$

For $x \in \mathcal{O}_q(S)$ let $\mathcal{O}_q(S, x)$ denote the orbit of x. For q divisible by a sufficiently high power of each prime dividing $2D$, we have that

$$\#\mathcal{O}_q(S, x) = q^2 \prod_{p|2D} \sigma_p(S, x) \quad \text{and} \quad \#\mathcal{O}_q(S) = q^2 \prod_{p|2D} \sigma_p. \tag{4.1}$$

Here $\sigma_p(S, x)$ and σ_p were defined in (3.8) and (3.1), respectively.

Let $S = S_1, \ldots, S_h$ be a complete set of representatives of the genus G. The classes of primitive representations of zero by forms in G are uniquely represented by $(x_{i,j}, S_j)$ where, as before, $x_{i,j} \in \mathbb{Z}^3$ for $i = 1, \ldots, c(S_j)$ runs over a complete set of representatives of orbits of $\mathcal{C}(S_j)$.

Lemma 1. *Let q be as above. For each j choose $A_j \in \mathrm{GL}_3(\mathbb{Z}/q\mathbb{Z})$ with $S[A_j] \equiv S_j$ and set $x'_{i,j} \equiv x_{i,j}A_j^t$ with $x_{i,j}$ as above. The map*

$$(x_{i,j}, S_j) \mapsto \mathcal{O}_q(S, x'_{i,j})$$

is well-defined and induces a bijection from the genera of primitive representations of zero by forms in G to the orbits in $\mathcal{O}_q(S)$. The orbit $\mathcal{O}_q(S, x'_{i,j})$ has the same cardinality as $\mathcal{O}_q(S_j, x_{i,j})$.

Proof. Clearly $x'_{i,j} \in \mathcal{O}_q(S)$ and the orbit $\mathcal{O}_q(S, x'_{i,j}) \subset \mathcal{O}_q(S)$ is independent of the choice of A_j. Also, two primitive representations of zero map to the same orbit if and only if they are in the same genus of representations. That the map is surjective follows from the bijection given in (c) of Theorem 7 of the Appendix, translated into equivalent matrix terminology using Lemma 6. The final statement follows by conjugation. □

By Theorem 6, (4.1) and the last statement of Lemma 1, we have

$$\sum_{j=1}^{h}\sum_{i=1}^{c(S_j)} \#\mathcal{O}_q(S, x'_{i,j}) = \#\mathcal{O}_q(S). \tag{4.2}$$

Theorem 1 follows from (4.2) and the bijection of Lemma 1 since having two classes in a genus of representations would imply that the LHS of (4.2) is greater than the RHS.

Therefore we are left with proving Theorems 4 and 5.

5 Eisenstein series

Suppose that S is isotropic with $D = \det S > 0$. Choose any primitive $x \in \mathbb{Z}^3$ with $S(x) = 0$. Completing x^t to a matrix $M_1 \in \mathrm{SL}_3(\mathbb{Z})$ we have

$$S[M_1] = \begin{pmatrix} 0 & s_1 & s_2 \\ s_1 & * & * \\ s_2 & * & * \end{pmatrix}. \tag{5.1}$$

Suppose $a = \gcd(s_1, s_2)$. Choose $u, v \in \mathbb{Z}$ with $us_1 + vs_2 = a$. Define

$$M_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{s_2}{a} & u \\ 0 & -\frac{s_1}{a} & v \end{pmatrix} \in \mathrm{SL}_3(\mathbb{Z})$$

so that M_1M_2 still has x^t as its first column and

$$S_1 = S[M_1M_2] = \begin{pmatrix} 0 & 0 & a \\ 0 & -b & c \\ a & c & d \end{pmatrix}. \tag{5.2}$$

This shows that we may find an equivalent S_1 of the form (5.2) whose associated orbit of primitive zeros contains $(1, 0, 0)$. We have that $a, b > 0$ are uniquely determined and c is determined modulo $\gcd(a, b)$ by the orbit of the solution.

Let $\Gamma(S_1) \subset \mathrm{PSL}_2(\mathbb{R})$ be the Fuchsian group from §2 that is isomorphic to the subgroup $O^+(S_1)$ of proper automorphs of S_1. Clearly $\Gamma(S_1)$ is conjugate to $\Gamma(S)$ in $\mathrm{PSL}_2(\mathbb{R})$. In effect, it is the conjugation that moves the cusp associated to x to infinity. For S_1 we take, as above (2.3), $B = B_0$ where

$$B_0 = \begin{pmatrix} 1 & \frac{c}{a} & \frac{d}{2a} \\ 0 & \sqrt{b} & 0 \\ 0 & 0 & 2a \end{pmatrix}.$$

Then $S_0[B_0] = S_1$ and we let

$$C_g = B_0^{-1} A_g B_0, \tag{5.3}$$

which may now be explicitly computed. In particular,

$$C_{\pm\left(\begin{smallmatrix}1 & \kappa\\ 0 & 1\end{smallmatrix}\right)} = \begin{pmatrix} 1 & 2\kappa\sqrt{b} & 2a\kappa^2 - \frac{2c\kappa}{\sqrt{b}} \\ 0 & 1 & \frac{2a\kappa}{\sqrt{b}} \\ 0 & 0 & 1 \end{pmatrix} \tag{5.4}$$

for $\kappa > 0$. Let f be the smallest positive integer so that

$$\Big(\frac{2a}{f}, \frac{2b}{f}, \frac{2c}{f} - \frac{2ab}{f^2}\Big) \in \mathbb{Z}^3. \tag{5.5}$$

Thus $\kappa = \frac{\sqrt{b}}{f}$ with f given in (5.5) is the minimal positive value so that the entries of the matrix C in (5.4) are integers. Hence, according to (2.4), for this κ the translation $\pm\left(\begin{smallmatrix}1 & \kappa\\ 0 & 1\end{smallmatrix}\right)$ generates the parabolic subgroup of $\Gamma(S_1)$ with cusp at $i\infty$. This f is well-defined for the orbit of solutions but can vary over different orbits. It is easily checked that

$$f = 2^\delta \gcd(a, b, c)$$

for some $\delta \in \{0, 1, 2\}$.

Next we will use the Eisenstein series for $\Gamma(S_1)$ with cusp at $i\infty$ to count solutions within the orbit. For any $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ define for $z \in \mathcal{H}$

$$N(x; z) = (2a \operatorname{Im} z)^{-1}(2ax_1 + (2c - 4a\sqrt{b} \operatorname{Re} x)x_2 + (d + 4a^2|z|^2)x_3). \tag{5.6}$$

In particular,

$$N(x; i) = x_1 + \frac{c}{a} x_2 + \Big(2a + \frac{d}{2a}\Big)x_3.$$

A calculation shows that for

$$y = (\operatorname{Im} z)^{-1}\Big(1, \frac{c - 2a\sqrt{b}\, x}{a}, \frac{d + 4a^2|z|^2}{2a}\Big) \tag{5.7}$$

we have $S_1^*(y) = 4D$ and

$$N(x; z) = xy^t. \tag{5.8}$$

Observe that the condition $xy^t > 0$ restricts x to a connected component of the cone given by $S_1(x) = 0$. This component is left stable by $O^+(S_1)$. For S_1 from (5.2) and $x_0 = (1, 0, 0)$, any $x \in \mathcal{C}(S_1, x_0)$ that satisfies $xy^t > 0$ will be contained in the $O^+(S_1)$ orbit of x_0.

Proposition 1. *For y from (5.7) with $z \in \mathcal{H}$ and f given in (5.5)*

$$\#\{x \in \mathcal{C}(S_1, x_0);\ 0 < xy^t \le T\} \sim \frac{\sqrt{b}}{f v\ (S_1)}\, T$$

as $T \to \infty$.

Proof. The Eisenstein series for the cusp $i\infty$ is defined by

$$E(z, s) = \sum_{g \in \Gamma_\infty^{(\kappa)} \backslash \Gamma} (\operatorname{Im} \sigma^{-1} g z)^s, \tag{5.9}$$

convergent for $\operatorname{Re} s > 1$. Here $\Gamma_\infty^{(\kappa)} \subset \Gamma = \Gamma(S_1)$ is generated by $\pm\left(\begin{smallmatrix} 1 & \kappa \\ 0 & 1 \end{smallmatrix}\right)$ and the scaling matrix is

$$\sigma = \begin{pmatrix} \kappa^{\frac{1}{2}} & 0 \\ 0 & \kappa^{-\frac{1}{2}} \end{pmatrix}. \tag{5.10}$$

Lemma 2. *Let $N(x; z)$ be given in (5.6) and f above* (5.5)*. For $z \in \mathcal{H}$ and* $\operatorname{Re}(s) > 1$ *we have*

$$E(z, s) = \left(\frac{f}{\sqrt{b}}\right)^s \sum_{\substack{x \in \mathcal{C}(S_1, x_0) \\ N(x;z) > 0}} N(x; z)^{-s}. \tag{5.11}$$

Proof. Corresponding to $g = \pm\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \Gamma_\infty^{(\kappa)} \backslash \Gamma$, we have

$$x = C_{g^{-1}}(1, 0, 0)^t = \Big(\delta^2 + \frac{\delta\gamma c}{a\sqrt{b}} - \frac{\gamma^2 d}{4a^2}, -\frac{\delta\gamma}{\sqrt{b}}, \frac{\gamma^2}{2a}\Big).$$

Note that, using y from (5.7), we have the identity

$$\Big(\delta^2 + \frac{\delta\gamma c}{a\sqrt{b}} - \frac{\gamma^2 d}{4a^2}, -\frac{\delta\gamma}{\sqrt{b}}, \frac{\gamma^2}{2a}\Big) y^t = (\operatorname{Im} z)^{-1} |\gamma z + \delta|^2. \tag{5.12}$$

By (5.10) we get

$$\operatorname{Im}(\sigma^{-1} g z) = \operatorname{Im} z\, \kappa^{-1} |\gamma z + \delta|^{-2} = \frac{f \operatorname{Im} z}{\sqrt{b}} |\gamma z + \delta|^{-2},$$

since $\kappa = \frac{\sqrt{b}}{f}$. The formula (5.11) is now derived using (5.9), (5.6) and (5.12). □

Now $E(z, s)$ has a continuation in s to a meromorphic function which is holomorphic for $\operatorname{Re}(s) \ge 1$ except for a simple pole at $s = 1$ and

$$\operatorname{res}_{s=1} E(z, s) = \frac{1}{v\ (S_1)}. \tag{5.13}$$

For a proof see the book of Iwaniec [15]. In view of (5.8), Proposition 1 follows from Lemma 2 by a standard application of the Ikehara theorem. □

6 Counting all zeros of bounded norm

This section contains the proof of Theorem 4. We may assume that $S = S_1$ from (5.2). Note that the asymptotic constants for the counts of S and of S_1 are equal since when we transform the y chosen for S, which satisfies $S^*(y) = 4D$, to y' for S_1 with $S_1^*(y') = 4D$, the counts are unchanged and the constants are independent of y and y'.

For fixed $c_0 > 0$ and $x \in \mathbb{R}^3$ let

$$\|x\| = \max(c_0\|x\|_\infty, |xy^t|),$$

where y was defined in (5.7) and $\|(x_1, x_2, x_3)\|_\infty = \max(|x_1|, |x_2|, |x_3|)$. Then $\|x\|$ gives a norm on $\mathbb{R}^3$. By (5.8) we have the formula from (5.6):

$$|xy^t| = (2a \operatorname{Im} z)^{-1}|2ax_1 + (2c - 4a\sqrt{b}\operatorname{Re} x)x_2 + (d + 4a^2|z|^2)x_3| \tag{6.1}$$

for some $z \in \mathcal{H}$. It is now easy to see that for a fixed z there exists $c_0 > 0$ so that for all $T \geq 1$ and $0 \leq \epsilon < 1$

$$\{x \in \mathbb{R}^3;\ |xy^t| \leq T \text{ and } |S_1(x)| \leq \epsilon\} = \{x \in \mathbb{R}^3;\ \|x\| \leq T \text{ and } |S_1(x)| \leq \epsilon\}.$$

Lemma 3. *The Hardy–Littlewood singular integral for S_1 and $\|\cdot\|$ is given by*

$$\lim_{\epsilon \to 0} \frac{1}{2\epsilon} \int_{\substack{|S_1(x)| \leq \epsilon \\ \|x\| \leq 1}} dx = \frac{\pi}{a\sqrt{b}}.$$

Proof. By solving for x_1 in $xy^t = r$ in (6.1) and substituting in $S_1(x) = \epsilon$ the area of the resulting ellipse is

$$\operatorname{Area}(r) = \frac{\pi(r^2 - 4\epsilon)}{8\sqrt{D}},$$

after taking into account the Jacobian of the transformation. By integrating $\operatorname{Area}(r)$ over $-1 \leq r \leq 1$, the volume between the hyperboloid given by $S_1(x) = \epsilon$ and the planes $xy^t = \pm 1$ is found to be

$$\frac{\pi}{12\sqrt{D}} - \frac{\pi\epsilon}{\sqrt{D}}.$$

The result follows since the volume between the planes and $|S_1(x)| = \epsilon$ is $\frac{2\pi\epsilon}{\sqrt{D}}$. See Figure 2 for an illustration when $S_1(x) = 2x_1x_3 - x_2^2$ and $\epsilon = .03$.

Theorem 4 is therefore a consequence of the next well-known result (see also [27]):

Proposition 2 ([9], [23])**.** *For σ_p defined in* (3.1)*, as $T \to \infty$, we have*

$$\#\{x \in \mathbb{Z}^3;\ x \text{ primitive}, \|x\| \leq T \text{ and } S_1(x) = 0\} \sim \left(\frac{\pi}{2\sqrt{D}} \prod_p \sigma_p\right) T.$$

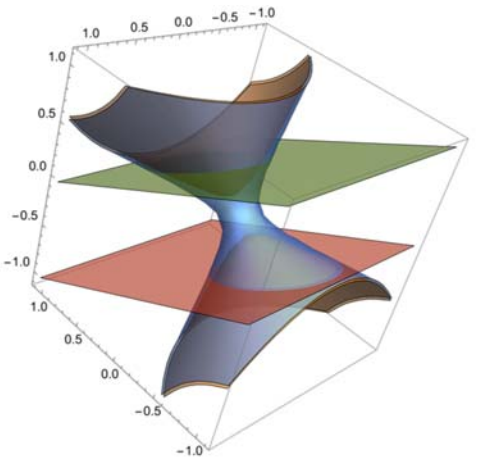

Figure 2.

7 The size of isotropy groups $(\mathrm{mod}\, p^m)$

Now we complete the proof of Theorem 5. We may assume that $\mathcal{C}(S, x) = \mathcal{C}(S_1, x_0)$ where $S = S_1$ is from (5.2) and $x_0 = (1, 0, 0)$. We must evaluate f from Lemma 1 in terms of $\delta_p(S_1, x_0)$ as defined in (3.5).

Proposition 3. *Let a, b, c be given in* (5.2) *and f be from* (5.5)*. Then*

$$2a^3bf = \prod_{p|2D} \delta_p(S_1, x_0).$$

This proposition follows from the next two lemmas. We may assume that the matrices in $O_p(S_1, x_0)$ $(\mathrm{mod}\, p^m)$ we are counting are in $\mathrm{SL}_3(\mathbb{Z}/p^m\mathbb{Z})$ and are reduced to evaluating

$$\alpha(p^m) := \#\left\{ A \in \mathrm{SL}_3(\mathbb{Z}/p^m\mathbb{Z});\ S_1[A] \equiv S_1 \text{ and } A \equiv \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix} (\mathrm{mod}\, p^m) \right\}$$

for sufficiently large m.

Lemma 4. *Let a, b, c be from* (5.2) *and f from* (5.5)*, For any prime $p > 2$ and $\delta_p(S_1, x_0)$ from* (3.5)

$$\delta_p(S_1, x_0) = p^{3\mathrm{ord}_p(a)+\mathrm{ord}_p(b)+\mathrm{ord}_p(f)}.$$

Proof. There are two essentially different cases: $c = 0$ and $c \neq 0$.

Suppose that $c = 0$. For

$$A = \begin{pmatrix} 1 & r_1 & r_2 \\ 0 & s_1 & s_2 \\ 0 & t_1 & t_2 \end{pmatrix} \quad \text{and} \quad S_1 = \begin{pmatrix} 0 & 0 & d_1 p^i \\ 0 & -d_2 p^j & 0 \\ d_1 p^i & 0 & d_3 \end{pmatrix} \tag{7.1}$$

we will count integers $x_1, r_2, s_1, s_2, t_1, t_2 \pmod{p^m}$ with $\det A \equiv 1$ and

$$S_1[A] \equiv S_1 \pmod{p^m}.$$

Suppose that $p \nmid d_1 d_2$. We can take m as large as we please. By a comparison with (5.5), we need to prove that

$$\alpha(p^m) = p^{m+3i+j+\min(i,j)}, \tag{7.2}$$

since from (5.5) we see that $f = \min(i, j)$.

After expanding $S_1[A] - S_1$ we see that it is necessary and sufficient that $t_1 = t_3 p^{m-i}$ and $t_2 = 1 + t_4 p^{m-i}$ for any t_3, t_4 taken modulo p^i. Given that, a calculation of the determinant of A, which we are assuming is $\equiv 1 \pmod{p^m}$, shows that

$$s_1 = 1 + s_3 p^{m-j}$$

with s_3 taken modulo p^j. Here we ignore terms with a factor of $p^{2m-\text{constant}}$, which do not matter when m is large enough. These lead to the congruences

$$\begin{aligned} d_1 r_1 p^i - d_2 s_2 p^j + d_3 p^{m-i} t_3 &\equiv 0 \pmod{p^m}, \\ 2 d_1 r_2 p^i - d_2 s_2^2 p^j + 2 d_3 p^{m-i} t_4 &\equiv 0 \pmod{p^m}. \end{aligned} \tag{7.3}$$

If $i \geq j$ we set $s_2 = s_4 p^{i-j}$ for s_4 modulo p^{m-i+j}, giving p^i choices of r_1 and p^i choices of r_2, for each choice of s_4. If $i < j$ let s_2 be free. This leads to p^i choices of r_1 and r_2. In each case we have (7.2) since the solutions obtained are distinct.

Note that the terms $d_3 p^{m-i} t_3$ and $2 d_3 p^{m-i} t_4$ could have been ignored since they involve only the variables t_3, t_4, which may be considered to be already chosen, and for m sufficiently large each is divisible by any fixed power of p. In the arguments that follow we will indicate such terms by using dots.

Suppose that $c \neq 0$ and consider

$$S_1 = \begin{pmatrix} 0 & 0 & d_1 p^i \\ 0 & -d_2 p^j & d_4 p^k \\ d_1 p^i & d_4 p^k & d_3 \end{pmatrix} \tag{7.4}$$

where $p \nmid d_4$. We now need to show that

$$\alpha(p^m) = p^{m+3i+j+\min(i,j,k)}. \tag{7.5}$$

Again $t_1 = t_3 p^{m-i}$ and $t_2 = 1 + t_4 p^{m-i}$ for any t_3, t_4 taken modulo p^i. We are led to solve the quadratic congruence

$$d_2 p^j s_1^2 - 2d_4 p^{m+k-i} t_3 s_1 - d_2 p^j \equiv 0.$$

There will be a d_5 with $d_4 \equiv d_2 d_5$ and $p \nmid d_5$ so that

$$s_1 = \pm 1 + d_5 p^{m-i-j+k} t_3 + s_3 p^{m-j}. \tag{7.6}$$

To have $\det A \equiv 1$ we must have the plus sign. Then we must solve

$$\begin{aligned} d_1 r_1 p^i - d_2 s_2 p^j + \cdots &\equiv 0 \pmod{p^m}, \\ 2d_1 r_2 p^i - d_2 s_2^2 p^j + 2d_4 s_2 p^k + \cdots &\equiv 0 \pmod{p^m}. \end{aligned} \tag{7.7}$$

As was already mentioned, the dots signify terms that may be ignored as above, only now they might involve s_3 as well as t_3, t_4.

If $k \geq \min(i, j)$ we can follow the arguments used when $c = 0$. Assume now that $k < \min(i, j)$ so (7.5) becomes

$$\alpha(p^m) = p^{m+3i+j+k}. \tag{7.8}$$

If $i \geq j$ take $s_2 = s_4 p^{i-k}$ for s_4 modulo p^{m-i+k} leading to p^i choices of r_1 and r_2, giving (7.8). If $i < j$ let r_2 be free giving p^k choices of s_2 and p^i choices of r_1, also leading to (7.8). Here we apply an easily proven lemma that gives the number of solutions of a degenerate quadratic congruence. □

The case when $p = 2$ is, as is to be expected, more intricate, but the arguments are similar. Differences arise from the two's that occur in the congruences and the fact that a quadratic congruence modulo 2^m can have four solutions. However, we may still assume that the matrices $A \in O_2(S_1, x_0)$ are in $\mathrm{SL}_3(\mathbb{Z}/2^m\mathbb{Z})$ since a calculation shows that a general A must have $\det A \equiv \pm 1$.

Lemma 5. *Let a, b, c be from (5.2) and f be from (5.5). Then*

$$\delta_2(S_1, x_0) = 2^{1+3\,\mathrm{ord}_2(a)+\mathrm{ord}_2(b)+\mathrm{ord}_2(f)}.$$

Proof. We will follow the proof when $p > 2$ as closely as possible. First assume that $c = 0$ and refer to (7.1) with $p = 2$. Again by a comparison with (5.5), if $i = j$ we need to show that

$$\alpha(2^m) = 2^{1+m+5i} \tag{7.9}$$

and otherwise

$$\alpha(2^m) = 2^{2+m+3i+j+\min(i,j)}. \tag{7.10}$$

Set $t_1 = t_3 2^{m-i}$ and $t_2 = 1 + t_4 2^{m-i}$ for any t_3, t_4 taken modulo 2^i. Now the quadratic congruence $2^j d_2(s_1^2 - 1) \equiv 0$ has $4 \cdot 2^j$ solutions:

$$s_1 = \pm 1 + s_3 2^{m-j} \quad \text{and} \quad s_1 = \pm 1 + 2^{m-j-1} + s_3 2^{m-j}.$$

Again we must have the plus signs to get $\det A \equiv 1$. The first pair gives (7.3) with $p = 2$ while the second gives

$$\begin{aligned} d_1 r_1 2^i - d_2 s_2 2^j - d_2 s_2 2^{m-1} + \cdots &\equiv 0 \pmod{2^m}, \\ d_1 r_2 2^{i+1} - d_2 s_2^2 2^j + \cdots &\equiv 0, \end{aligned}$$

where the dots convention is as before. For either pair if $i > j$ we set $s_2 = s_4 p^{i-j}$ for s_4 modulo 2^{m-i+j}, giving 2^i choices of r_1 and 2^{i+1} choices of r_2, for each choice of s_4, hence giving (7.10). If $i < j$ let s_2 be free. This leads to p^i choices of r_1 and r_2, again giving (7.10). If $i = j$ set $s_2 = 2s_4$ for $s_4 \pmod{2^{m-1}}$ leading to 2^i choices of r_1 and 2^{i+1} choices of r_2. Therefore in this case (7.9) holds.

Suppose now that $c \neq 0$ and refer to (7.4) with $p = 2$. If $k \geq \min(i, j)$ and $i = j$ we need to show (7.9), while if $k \geq \min(i, j)$ and $i \neq j$ we need (7.10). If $i = j \geq 1$ and $k = i - 1$ we need

$$\alpha(2^m) = 2^{2+m+5i}. \tag{7.11}$$

Otherwise, we need to show that

$$\alpha(2^m) = 2^{2+m+3i+j+k}. \tag{7.12}$$

Once again, $t_1 = t_3 2^{m-i}$ and $t_2 = 1 + t_4 2^{m-i}$ for any t_3, t_4 taken modulo 2^i. We are now led to solve the quadratic congruence

$$d_2 2^j s_1^2 - 2 d_4 2^{m+k-i} t_3 s_1 - d_2 2^j \equiv 0.$$

Choose d_5 with $d_4 \equiv d_2 d_5$ and $2 \nmid d_5$. We get $2 \cdot 2^j$ solutions in terms of $s_3 \pmod{2^j}$ that give $\det A \equiv 1$. They are

$$s_1 = 1 + d_5 2^{m-i-j+k} t_3 + s_3 2^{m-j} \quad \text{or} \quad s_1 = 1 + d_5 2^{m-i-j+k} t_3 + 2^{m-j-1} + s_3 2^{m-j}.$$

We now record the needed congruences for each of these. For the first we have

$$\begin{aligned} d_1 r_1 2^i - d_2 s_2 2^j + \cdots &\equiv 0 \pmod{2^m}, \\ d_1 r_2 2^{i+1} - d_2 s_2^2 2^j + d_4 s_2 2^{k+1}(1 + t_4 2^{m-i}) + \cdots &\equiv 0. \end{aligned} \tag{7.13}$$

For the second we have

$$\begin{aligned} d_1 r_1 2^i - d_2 s_2 2^j - d_2 s_2 2^{m-1} + \cdots &\equiv 0 \pmod{2^m}, \\ d_1 r_2 2^{i+1} - d_2 s_2^2 2^j + d_4 s_2 2^{k+1}(1 + t_4 2^{m-i}) + \cdots &\equiv 0. \end{aligned} \tag{7.14}$$

If $k \geq \min(i,j)$ proceed as when $c = 0$ to get (7.9) and (7.10). If $i = j \geq 1$ and $k = i - 1$ let s_2 be free to get 2^i values of r_1. If s_2 is even we get 2^{i+1} values of r_2. If s_2 is odd,

$$-d_2 s_2 + d_4(1 + t_4 2^{m-i})$$

is even so again we get 2^{i+1} values of r_2, hence (7.11) holds, after treating both (7.13) and (7.14).

Suppose that $k < \min(i,j)$ and either $i \neq j$ or $i = j$ and $k < i - 1$. If $i > j$ take $s_2 = s_4 2^{i-k}$ for s_4 modulo p^{m-i+k}, leading to 2^i choices for r_1 and 2^{i+1} choices for r_2, giving (7.12). If $i < j$ let r_2 be free giving 2^{k+1} choices of s_2 (since $j > k+1$) and 2^i choices of r_1, also leading to (7.12). Finally, if $i = j$ and $k < i - 1$, again let r_2 be free giving 2^{k+1} choices of s_2 and 2^i choices of r_1, once more giving (7.12). Again we must treat both (7.13) and (7.14). As before, in the last two cases where r_2 is free we are counting solutions of a degenerate quadratic congruence. This finishes the proof of Lemma 5 and hence of Proposition 3. □

Theorem 5 now follows from Propositions 1 and 3. This also completes the proof of Theorems 1 and 2. □

Appendix by Rainer Schulze-Pillot

In this appendix we want to relate the statements of Theorems 1 and 2 to the notions of genus and class of representations of lattices with quadratic form used in [18, 19]; for that we have to recall some terminology.

Let (V, Q) be a finite-dimensional rational quadratic space, i.e., a vector space over $\mathbb{Q}$ equipped with a quadratic form $Q : V \to \mathbb{Q}$ and associated symmetric bilinear form

$$B(x,y) = Q(x+y) - Q(x) - Q(y)$$

and $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ a $\mathbb{Z}$-lattice on V, where $\{v_1, \ldots, v_n\}$ is a basis of V. We will assume that (V, Q) is non-degenerate, i.e., the Gram matrix $(B(v_i, v_j)) \in \mathrm{Mat}_n(\mathbb{Q})$ of B with respect to the basis is nonsingular. The determinant of this matrix is called the determinant $\det(L)$ of $L = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$. If K is another such lattice on a (not necessarily nondegenerate) rational quadratic space $(U, \widetilde{Q})$ we call an injective linear map $\phi : U \to V$ with $\phi(K) \subseteq L$ a representation of K by L if ϕ is an isometry, i.e., if $Q(\phi(u)) = \widetilde{Q}(u)$ for all $u \in U$. The representation is primitive if

$$\phi(U) \cap L = \phi(K)$$

holds, equivalently if $\phi(K)$ is a direct summand in L. A representation ϕ of K by L and another representation ψ of K by a lattice L' in a quadratic space (V', Q')

are in the same class if there exists an isometric linear isomorphism (an isometry) $\rho : V \to V'$ with $\rho \circ \phi = \psi$. The number of classes of primitive representations of K by lattices L of fixed determinant and dimension is finite, see Satz 30.2 and the last sentence of Bemerkung 30.3 of [19].

In the same way, $\mathbb{Z}_p$-classes of representations of the p-adic completions $K_p \subseteq U_p, L_p \subseteq V_p$ are defined, and with essentially the same proof one sees that the number of $\mathbb{Z}_p$-classes of primitive representations of K_p by lattices L_p of fixed determinant and dimension is finite. Representations ϕ of K by L and ψ of K by L' are in the same genus if their p-adic completions ϕ_p, ψ_p are in the same p-adic class for all primes p, including $p = \infty$ with $K_\infty = U_\infty$ etc. Obviously, in that case L and L' have to be in the same genus, i.e., all p-adic completions are isometric, and by the Minkowski–Hasse local-global principle the spaces (V, Q), (V', Q') (but in general not the lattices L, L') are isometric; we may hence assume $(V, Q) = (V', Q')$.

Lemma 6. *Let $\phi : K \to L$, $\psi : K \to L'$ be representations, let $T = (B(u_i, u_j))$ be the Gram matrix of K with respect to the $\mathbb{Z}$-basis $\{u_1, \dots, u_m\}$ and S, S' the Gram matrices of L, L' with respect to the bases $\{v_1, \dots, v_n\}$, $\{v_1', \dots, v_n'\}$; write $\phi(u_j) = \sum_i x_{ij} v_i$, $\psi(u_j) = \sum_i x'_{ij} v_i'$, $X = (x_{ij})$, $X' = (x'_{ij}) \in \mathrm{Mat}_{n,r}(\mathbb{Z})$.*

(a) *One has $T = X^t S X = (X')^t S' X'$.*

(b) *ϕ is primitive if and only if X can be completed to a matrix in $\mathrm{GL}_n(\mathbb{Z})$.*

(c) *ϕ, ψ are in the same class if and only if there exists $A \in \mathrm{GL}_n(\mathbb{Z})$ with $S' = A^t S A$, $X = AX'$.*

(d) *ϕ, ψ are in the same genus if and only if there exist for all primes p (including $p = \infty$) matrices $A_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ with $S' = A_p^t S A_p$, $X = A_p X'$.*

(e) *There exists $q \in \mathbb{Z}$ such that the matrices A_p above exist for all p if and only if there exists $A_q \in \mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$ with $S' \equiv A_q^t S A_q \bmod q$, $X \equiv A_q X' \bmod q$.*

Proof. This is well known and easily checked. □

Definition 1. For symmetric matrices $S \in \mathrm{Mat}_n(\mathbb{Z})$, $T \in \mathrm{Mat}_r(\mathbb{Z})$ with $r \le n$ and $X \in \mathrm{Mat}_{n,r}(\mathbb{Z})$ of rank r with $T = X^t S X$ we say that (X, S) is a **representation** of T. The representation is called **primitive** if X can be completed to a matrix in $\mathrm{GL}_n(\mathbb{Z})$.

(i) Two representations (X, S), (X', S') (primitive or not) are **in the same class** if there exists $A \in \mathrm{GL}_n(\mathbb{Z})$ with $S' = A^t S A$, $X = AX'$.

(ii) Two representations (X, S), (X', S') (primitive or not) are **in the same genus** if there exist for all primes p (including $p = \infty$) matrices $A_p \in \mathrm{GL}_n(\mathbb{Z}_p)$ with $S' = A_p^t S A_p$, $X = A_p X'$.

Remarks.

(a) Since primitivity is a local property, two representations (X, S), (X', S') in the same genus are either both primitive or both imprimitive.

(b) For $S = S'$ the representations (X, S), (X', S) are in the same class if and only if X, X' are in the same orbit under the action of the group of automorphisms of S.

(c) The notion of a genus of representations has apparently not been treated in matrix terminology so far. The definition given above is the natural translation into matrix terminology of the same notion from the lattice terminology.

Theorem 7 (Kneser)**.** *Let K, L be $\mathbb{Z}$-lattices on quadratic spaces U, V as before, assume that V is non-degenerate and that U is represented by V.*

(a) *For almost all primes all primitive representations of K_p by L_p are in the same $\mathbb{Z}_p$-class.*

(b) *Let $\phi : K \to L'$ be a representation of K by a lattice L' in the genus of L. Then for all primes p, there is a representation $\psi_p : K_p \to L_p$ in the same $\mathbb{Z}_p$-class as $\phi_p : K_p \to L'_p$.*

(c) *The map associating to the genus of the primitive representation $\phi : K \to L'$ of K by a lattice L' in the genus of L the family $(\overline{\psi_p})_p$ of the $\mathbb{Z}_p$-classes $\overline{\psi_p}$ of the ψ_p from (b), defines a bijection from*

(i) *the set of genera of primitive representations of K by a lattice L' in the genus of L to*

(ii) *the product over all primes of the sets of $\mathbb{Z}_p$-classes of primitive representations of K_p by L_p.*

(d) *Let $c_p(K_p, L_p)$ denote the number of $\mathbb{Z}_p$-classes of primitive representations of K_p by L_p. Then the number of genera of primitive representations of K by a lattice L' in the genus of L equals $\prod_p c_p(K_p, L_p)$.*

Proof. Without the primitivity condition and with the additional requirement that $\mathbb{Q}K = U$ is nondegenerate this is proven in [19, Hilfssatz 30.7, Satz 30.9]. We check that the proof goes through with only small modifications in our situation.

For almost all primes L_p is regular in the sense of [19]. For such a prime p let ϕ_p, ψ_p be primitive representations of K_p in L_p. By the argument in the paragraph after Definition 2.17 of [19], the primitive submodules $\phi_p(K_p)$, $\psi_p(K_p)$ of L_p are "scharf primitiv" in the sense of that definition. Folgerung 4.4 of [19], a strong version of Witt's extension theorem, then shows that

$$\psi_p \circ \phi_p^{-1} : \phi_p(K_p) \to \psi_p(K_p)$$

can be extended to an automorphism of L_p, hence ϕ_p and ψ_p are in the same $\mathbb{Z}_p$-class of representations, which shows (a).

Let now $\phi : K \to L$ be a representation; replacing K by $\phi(K)$ we may assume $K \subseteq L$. If $\psi : K \to L''$ is a representation of K by a lattice L'' in the genus of L the space $\mathbb{Q}L''$ is isometric to $V = \mathbb{Q}L$ by the Hasse–Minkowski theorem and we may assume $\mathbb{Q}L'' = V$. Since (V, Q) is nondegenerate, hence regular, and any subspace, being a direct summand, is primitive, we obtain as above using [19, Folgerung 4.4] an extension of

$$\psi : U \to \psi(U) \subseteq V$$

to an isometry $\widetilde{\psi} : V \to V$. Setting $L' := \widetilde{\psi}^{-1}(L'')$ we see that the inclusion $K \to L'$ is in the class of the representation ψ. For each class of representations of K by a lattice in the genus of L we can therefore choose a lattice L' on V such that the inclusion $i_{L'} : K \to L'$ is a representative of that class. For such an L' we choose isometries $\tau_p : L_p \to L'_p$ for all primes p and have that

$$\rho_p := \tau_p^{-1} \circ i_{L'} : K_p \to L_p$$

is a representation of K_p by L_p in the $\mathbb{Z}_p$-class of i'_L, which proves (b).

By Satz 21.5 of [19] one has $L'_p = L_p$ for almost all primes p, we can thus choose $\tau_p = \mathrm{id}_{V_p}$ for almost all p. The family $(\overline{\rho_p})_p$ of the $\mathbb{Z}_p$-classes of the representations ρ_p depends only on the genus of the representation $i_{L'}$, and the map sending $i_{L'}$ to that family is injective by the definition of a genus of representations. Conversely, let any family $(\overline{\rho_p})_p$ of classes of representations ρ_p of K_p by L_p be given. By (a) we may assume that almost all ρ_p are the inclusion $K_p \to L_p$, let Σ be the set of the remaining primes. For $p \in \Sigma$ we use again Folgerung 4.4 of [19] to extend ρ_p to an automorphism $\widetilde{\rho_p}$ of V_p. By Satz 21.5 of [19] there is a lattice L' on V with $L'_p = \widetilde{\rho_p}^{-1}(L_p)$ for the $p \in \Sigma$, $L'_p = L_p$ for the primes not in Σ. The mapping constructed above then maps the genus of $i_{L'}$ to the family $(\overline{\rho_p})_p$, and we see that the mapping is surjective, which proves (c).

Assertion (d) is an obvious consequence of (c). □

Corollary 2. *Let $S \in \mathrm{Mat}_n(\mathbb{Z})$ be a nonsingular symmetric matrix, $T \in \mathrm{Mat}_m(\mathbb{Z})$ symmetric.*

(a) *The number of genera of primitive representations of T by a matrix S' in the genus of S is equal to the product over all primes of the numbers of $\mathbb{Z}_p$-classes of primitive representations of T by S.*

(b) *The following two statements are equivalent.*

  (i) *The sum over all integral equivalence classes of S' in the genus of S, of the numbers of classes of primitive representations of T by S', equals the product over all primes of the numbers of $\mathbb{Z}_p$-classes of primitive representations of T by S.*

(ii) *Each genus of primitive representations of T by a matrix S' in the genus of S contains only one class of representations.*

Proof. Part (a) is the translation into matrix terminology of part (d) of the theorem, and (b) is an obvious consequence of (a). □

References

[1] B. Berggren, *Pytagoreiska trianglar*, Tidskr. Elem. Mat. Fys. Kem. **17** (1934), 129–139.

[2] M. Borovoi, *On representations of integers by indefinite ternary quadratic forms*, J. Number Theory **90** (2001), 281–293.

[3] M. Borovoi and Z. Rudnick, *Hardy–Littlewood varieties and semisimple groups*, Invent. Math. **119** (1995), 37–66.

[4] K. Conrad, *Pythagorean descent*, `https://kconrad.math.uconn.edu/blurbs/linmultialg/descentPythag.pdf`.

[5] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, F. Vieweg und sohn, Braunschweig, 1879.

[6] W. Duke, J. Friedlander and H. Iwaniec, *Bounds for automorphic L-functions*, Invent. Math. **112** (1993), 1–8.

[7] W. Duke, Z. Rudnick and P. Sarnak, *Density of integer points on affine homogeneous varieties*, Duke Math. J. **71** (1993), 143–179.

[8] A. Eskin, Z. Rudnick and P. Sarnak, *A proof of Siegel's weight formula*, Internat. Math. Res. Notices **1991** (1991), 65–69.

[9] J. Franke, Y. I. Manin and Y. Tschinkel, *Rational points of bounded height on Fano varieties*. Invent. Math. **95** (1989), 421–435.

[10] R. Fricke and F. Klein, *Vorlesungen über die Theorie der Automorphen Funktionen. Vols. 1, 2*, Teubner, Stuttgart, 1897.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer, New York, 1986.

[12] D. R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149–206.

[13] C. Hooley, *Some recent advances in analytical number theory*, in *Proceedings of the International Congress of Mathematicians, Vol. 1, (Warsaw, 1983)*, PWN—Polish Scientific Publishers, Warsaw, 1984, pp. 85{97.

[14] G. Humbert, *Sur les formes quadratiques ternaires indefinies*, C. R. Acad. Sci. Paris **167** (1918), 181–186.

[15] H. Iwaniec, *Spectral Methods of Automorphic Forms*, American Mathematical Society, Providence, RI; Revista Matemática Iberoamericana, Madrid, 2002.

[16] M. Kneser, *Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen*, Arch. Math. (Basel) **7** (1956), 323–332.

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

[18] M. Kneser, *Representations of integral quadratic forms*, in *Quadratic and Hermitian Forms (Hamilton, Ont., 1983)*, American Mathematical Society, Providence, RI, 1984, pp. 159–172;

[19] M. Kneser, *Quadratische Formen*, Springer, Berlin, 2002.

[20] A.-M. Legendre, *Reserches d'Analyse Indetérminée*, Mem. Math. Phys. Ac. Sci. Paris (1785), 465–559.

[21] W. Magnus, *Noneuclidean Tesselations and Their Groups*, Academic Press, New York–London, 1974.

[22] A. Meyer, *Über die Klassenanzahl derjenigen ternären quadratischen Formen, durch welche die Null rational darstellbar ist*, J. Reine Angew. Math. **98** (1885), 177–230.

[23] E. Peyre, *Hauteurs et mesures de Tamagawa sur les variétés de Fano*, Duke Math. J. **79** (1995), 101–218.

[24] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen*. Ann. of Math. (2) **36** (1935), 527–606.

[25] C. L. Siegel, *Über die analytische Theorie der quadratischen Formen. II*, Ann. of Math. (2) **37** (1936), 230–263.

[26] C. L. Siegel, *On the Theory of Indefinite Quadratic Forms*. Ann. of Math. (2) **45**, (1944), 577–622.

[27] E. Sofos, *Uniformly counting rational points on conics*, Acta Arith. **166** (2014), 1–14.

[28] A. Weil, *Number Theory*, Birkhäuser, Boston, MA, 1984.

William Duke
MATHEMATICS DEPARTMENT
UNIVERSITY OF CALIFORNIA AT LOS ANGELES
BOX 951555
LOS ANGELES, CA 90095-1555
email: wdduke@ucla.edu

Rainer Schulze-Pillot
UNIVERSITÄT DES SAARLANDES
POSTFACH 151150
66041 SAARBRÜCKEN, GERMANY
email: schulzep@math.uni-sb.de

(Received December 11, 2022 and in revised form May 1, 2023)