On representations of integers by indefinite ternary quadratic forms

Mikhail Borovoi

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, 69978 Tel Aviv, Israel
E-mail: borovoi@math.tau.ac.il

Let f be an indefinite ternary integral quadratic form and let q be a nonzero integer such that $-q\det(f)$ is not a square. Let $N(T, f, q)$ denote the number of integral solutions of the equation $f(x) = q$ where x lies in the ball of radius T centered at the origin. We are interested in the asymptotic behavior of $N(T, f, q)$ as $T \to \infty$. We deduce from the results of our joint paper with Z. Rudnick that $N(T, f, q) \sim cE_{HL}(T, f, q)$ as $T \to \infty$, where $E_{HL}(T, f, q)$ is the Hardy-Littlewood expectation (the product of local densities) and $0 \leq c \leq 2$. We give examples of f and q such that c takes the values 0, 1, 2.

Key Words: Ternary quadratic forms

0. INTRODUCTION

Let f be a nondegenerate indefinite integral-matrix quadratic form of n variables:

$$f(x_1, \dots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j, \quad a_{ij} \in \mathbf{Z}, \quad a_{ij} = a_{ji}\,.$$

Let $q \in \mathbf{Z}$, $q \neq 0$. Let $W = \mathbf{Q}^n$. Consider the affine quadric X in W defined by the equation

$$f(x_1, \dots, x_n) = q\,.$$

We wish to count the representations of q by the quadratic form f, that is the integer points of X.

Partially supported by the Hermann Minkowski Center for Geometry

Since f is indefinite, the set $X(\mathbf{Z})$ can be infinite. We fix a Euclidean norm $|\cdot|$ on $\mathbf{R}^n$. Consider the counting function

$$N(T,X)=\#\{x\in X(\mathbf{Z}) : |x|\leq T\}$$

where $T\in\mathbf{R},\ T>0$. We are interested in the asymptotic behavior of $N(T,X)$ as $T\to\infty$.

When $n\geq 4$, the counting function $N(T,X)$ can be approximated by the product of local densities. For a prime p set

$$\mu_p(X)=\lim_{k\to\infty}\frac{\#X(\mathbf{Z}/p^k\mathbf{Z})}{(p^k)^{n-1}}\ .$$

For almost all p it suffices to take $k=1$:

$$\mu_p(X)=\frac{\#X(\mathbf{F}_p)}{p^{n-1}}\ .$$

Set $\mathfrak{S}(X)=\prod_p\mu_p(X)$; this product converges absolutely (for $n\geq 4$); it is called the singular series. Set

$$\mu_\infty(T,X)=\lim_{\varepsilon\to 0}\frac{\mathrm{Vol}\{x\in\mathbf{R}^n : |x|\leq T,\ |f(x)-q|<\varepsilon/2\}}{\varepsilon}\ ;$$

it is called the singular integral. For $n\geq 4$ the following asymptotic formula holds:

$$N(T,X)\sim\mathfrak{S}(X)\mu_\infty(T,X)\ \text{as}\ T\to\infty.$$

This follows from results of [2], 6.4 (which are based on analytical results of [6], [7], [8]). For certain non-Euclidean norms the similar result was earlier proved by the Hardy-Littlewood circle method, cf. [5] in the case $n\geq 5$ and [9] in the more difficult case $n=4$.

We are interested here in the case $n=3$, a ternary quadratic form. This case is beyond the range of the Hardy-Littlewood circle method. Set $D=\det(a_{ij})$. We assume that $-qD$ is not a square. Then the product $\mathfrak{S}(X)=\prod\mu_p(X)$ conditionally converges (see Sect. 1 below), but in general $N(T,X)$ is not asymptotically $\mathfrak{S}(X)\mu_\infty(T,X)$. From results of [2] it follows that

$$N(T,X)\sim c_X\mathfrak{S}(X)\mu_\infty(T,X)\ \text{as}\ T\to\infty$$

with $0\leq c_X\leq 2$, see details in Subsection 1.5 below. We wish to know what values can c_X take.

A case when $c_X=0$ was already known to Siegel, see also [2], 6.4.1. Consider the quadratic form

$$f_1(x_1,x_2,x_3)=-9x_1^2+2x_1x_2+7x_2^2+2x_3^2\ ,$$

and take $q = 1$. Let X be defined by $f_1(x) = q$. Then f_1 does not represent 1 over $\mathbf{Z}$, so $N(T, X) = 0$ for all T. On the other hand, f_1 represents 1 over $\mathbf{R}$ and over $\mathbf{Z}_p$ for all p, and $\mathfrak{S}(X)\mu_\infty(T, X) \to \infty$ as $T \to \infty$. Thus $c_X = 0$ (see details in Sect. 2).

We show that c_X can take the value 2. Recall that two integral quadratic forms f, f' are in the same genus, if they are equivalent over $\mathbf{R}$ and over $\mathbf{Z}_p$ for every prime p, cf. e.g. [3].

Theorem 0.1. *Let f be an indefinite integral-matrix ternary quadratic form, $q \in \mathbf{Z}$, $q \neq 0$, and let X be the affine quadric defined by the equation $f(x) = q$. Assume that f represents q over $\mathbf{Z}$ and that there exists a quadratic form f' in the genus of f, such that f' does not represent q over $\mathbf{Z}$. Then $c_X = 2$:*

$$N(T, X) \sim 2\mathfrak{S}(X)\mu_\infty(T, X) \text{ as } T \to \infty.$$

Theorem 0.1 will be proved in Sect. 3.

Example 0.1.1. Let $f_2(x_1, x_2, x_3) = -x_1^2 + 64x_2^2 + 2x_3^2$, $q = 1$. Then f_2 represents 1 ($f_2(1, 0, 1) = 1$) and the quadratic form f_1 considered above is in the genus of f_2 (cf. [4], 15.6). The form f_1 does not represent 1. Take $|x| = (x_1^2 + 64x_2^2 + 2x_3^2)^{1/2}$. By Theorem 0.1 $c_X = 2$ for the variety $X : f_2(x) = 1$. Analytic and numeric calculations give $2\mathfrak{S}(X)\mu_\infty(T, X) \sim 0.794T$. On the other hand, numeric calculations give for $T = 10,000$ the value $N(T, X)/T = 0.8024$.

We also show that c_X can take the value 1.

Theorem 0.2. *Let f be an indefinite integral-matrix ternary quadratic form, $q \in \mathbf{Z}$, $q \neq 0$, and let X be the affine quadric defined by the equation $f(x) = q$. Assume that $X(\mathbf{R})$ is two-sheeted (has two connected components). Then $c_X = 1$:*

$$N(T, X) \sim \mathfrak{S}(X)\mu_\infty(T, X) \text{ as } T \to \infty.$$

Theorem 0.2 will be proved in Sect. 4.

Example 0.2.1. Let f_2 and $|x|$ be as in Example 0.1.1, $q = -1$, $X : f_2(x) = q$. Then $X(\mathbf{R})$ has two connected components, and by Theorem 0.2 $c_X = 1$. Analytic and numeric calculations give $\mathfrak{S}(X)\mu_\infty(T, X) \sim 0.7065T$. On the other hand, numeric calculations give for $T = 10,000$ the value $N(T, X)/T = 0.7048$.

Question 0.3. Can c_X take values other than 0, 1, 2?

The plan of the paper is the following. In Section 1 we describe results of [2] in the case of 2-dimensional affine quadrics. In Section 2 we treat in detail the example of $c_X = 0$. In Section 3 we prove Theorem 0.1. In Section 4 we prove Theorem 0.2.

1. RESULTS OF [2] IN THE CASE OF TERNARY QUADRATIC FORMS

Let f be an indefinite ternary integral-matrix quadratic form

$$f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij} x_i x_j, \quad a_{ij} \in \mathbf{Z}, \quad a_{ij} = a_{ji}\,.$$

Let $q \in \mathbf{Z}$, $q \neq 0$. Let $D = \det(a_{ij})$. We assume that $-qD$ is not a square.

Let $W = \mathbf{Q}^3$ and let X denote the affine variety in W defined by the equation $f(x) = q$, where $x = (x_1, x_2, x_3)$. We assume that X has a $\mathbf{Q}$-point x^0. Set $G = \mathrm{Spin}(W, f)$, the spinor group of f. Then G acts on W on the left, and X is an orbit (a homogeneous space) of G.

1.1. Rational points in adelic orbits

Let $\mathbf{A}$ denote the adèle ring of $\mathbf{Q}$. The group $G(\mathbf{A})$ acts on $X(\mathbf{A})$; let $\mathcal{O}_{\mathbf{A}}$ be an orbit. We would like to know whether $\mathcal{O}_{\mathbf{A}}$ has a $\mathbf{Q}$-rational point.

Let W' denote the orthogonal complement of x^0 in W, and let f' denote the restriction of f to W'. Let H be the stabilizer of x^0 in G, then $H = \mathrm{Spin}(W', f')$. Since $\dim W' = 2$, the group H is a one-dimensional torus.

We have $\det f' = D/q$, so up to multiplication by a square $\det f' = qD$. It follows that up to multiplication by a scalar, f' is equivalent to the quadratic form $u^2 + qDv^2$. Set $K = \mathbf{Q}(\sqrt{-qD})$, then K is a quadratic extension of $\mathbf{Q}$, because $-qD$ is not a square. The torus H is anisotropic over $\mathbf{Q}$ (because $-qD$ is not a square), and H splits over K. Let $\mathbf{X}_*(H_K)$ denote the cocharacter group of H_K, $\mathbf{X}_*(H_K) = \mathrm{Hom}(\mathbb{G}_{m,K}, H_K)$; then $\mathbf{X}_*(H_K) \simeq \mathbf{Z}$. The non-neutral element of $\mathrm{Gal}(K/\mathbf{Q})$ acts on $\mathbf{X}_*(H_K)$ by multiplication by -1.

Let $\mathcal{O}_{\mathbf{A}}$ be an orbit of $G(\mathbf{A})$ in $X(\mathbf{A})$, $\mathcal{O}_{\mathbf{A}} = \prod \mathcal{O}_v$ where $\mathcal{O}_v$ is an orbit of $G(\mathbf{Q}_v)$ in $X(\mathbf{Q}_v)$, v runs over the places of $\mathbf{Q}$, and $\mathbf{Q}_v$ denotes the completion of $\mathbf{Q}$ at v. We define local invariants $\nu_v(\mathcal{O}_v) = \pm 1$. If $\mathcal{O}_v = G(\mathbf{Q}_v) \cdot x^0$, then we set $\nu_v(\mathcal{O}_v) = +1$, if not, we set $\nu_v(\mathcal{O}_v) = -1$. Then $\nu_v(\mathcal{O}_v) = +1$ for almost all v. We define $\nu(\mathcal{O}_{\mathbf{A}}) = \prod \nu_v(\mathcal{O}_v)$ where $\mathcal{O}_{\mathbf{A}} = \prod \mathcal{O}_v$. Note that the local invariants $\nu_v(\mathcal{O}_v)$ depend on the choice of the rational point $x^0 \in X(\mathbf{Q})$; one can prove, however, that their product $\nu(\mathcal{O}_{\mathbf{A}})$ does not depend on x^0.

Let $x \in X(\mathbf{A})$. We set $\nu(x) = \nu(G(\mathbf{A}) \cdot x)$. Then $\nu(x)$ takes values ± 1; it is a locally constant function on $X(\mathbf{A})$, because the orbits of $G(\mathbf{A})$ are open in $X(\mathbf{A})$.

For $x \in X(\mathbf{A})$ define $\delta(x) = \nu(x) + 1$. In other words, if $\nu(x) = -1$ then $\delta(x) = 0$, and if $\nu(x) = +1$ then $\delta(x) = 2$. Then δ is a locally constant function on $X(\mathbf{A})$.

THEOREM 1.1. *An orbit $\mathcal{O}_{\mathbf{A}}$ of $G(\mathbf{A})$ in $X(\mathbf{A})$ has a $\mathbf{Q}$-rational point if and only if $\nu(\mathcal{O}_{\mathbf{A}}) = +1$.*

Below we will deduce Theorem 1.1 from [2], Thm. 3.6.

1.2. Proof of Theorem 1.1

For a torus T over a field k of characteristic 0 we define a finite abelian group $C(T)$ as follows:

$$C(T) = (\mathbf{X}_*(T_{\bar{k}})_{\mathrm{Gal}(\bar{k}/k)})_{\mathrm{tors}}$$

where $\bar{k}$ is a fixed algebraic closure of k, $\mathbf{X}_*(T_{\bar{k}})_{\mathrm{Gal}(\bar{k}/k)}$ denotes the group of coinvariants, and $(\cdot)_{\mathrm{tors}}$ denotes the torsion subgroup. If k is a number field and k_v is the completion of k at a place v, then we define $C_v(T) = C(T_{k_v})$. There is a canonical map $i_v \colon C_v(T) \to C(T)$ induced by an inclusion $\mathrm{Gal}(\bar{k}_v/k_v) \to \mathrm{Gal}(\bar{k}/k)$. These definitions were given for connected reductive groups (not only for tori) by Kottwitz [10], see also [2], 3.4. Kottwitz writes $A(T)$ instead of $C(T)$.

We compute $C(H)$ for our one-dimensional torus H over $\mathbf{Q}$. Clearly

$$C(H) = (\mathbf{X}_*(H_K)_{\mathrm{Gal}(K/\mathbf{Q})})_{\mathrm{tors}} = \mathbf{Z}/2\mathbf{Z}\ .$$

We have $C_v(H) = 1$ if $K \otimes \mathbf{Q}_v$ splits, and $C_v(H) \simeq \mathbf{Z}/2\mathbf{Z}$ if $K \otimes \mathbf{Q}_v$ is a field. The map i_v is injective for any v.

We now define the local invariants $\kappa_v(\mathcal{O}_v)$ as in [2], where $\mathcal{O}_v$ is an orbit of $G(\mathbf{Q}_v)$ in $X(\mathbf{Q}_v)$. The set of orbits of $G(\mathbf{Q}_v)$ in $X(\mathbf{Q}_v)$ is in canonical bijection with $\ker[H^1(\mathbf{Q}_v, H) \to H^1(\mathbf{Q}_v, G)]$, cf. [13], I-5.4, Cor. 1 of Prop. 36. Hence $\mathcal{O}_v$ defines a cohomology class $\xi_v \in H^1(\mathbf{Q}_v, H)$. The local Tate–Nakayama duality for tori defines a canonical homomorphism $\beta_v \colon H^1(\mathbf{Q}_v, H) \to C_v(H)$, see Kottwitz [10], Thm. 1.2. (Kottwitz defines the map β_v in a more general setting, when H is any connected reductive group over a number field.) The homomorphism β_v is an isomorphism for any v. We set $\kappa_v(\mathcal{O}_v) = \beta_v(\xi_v)$. Note that if $\mathcal{O}_v = G(\mathbf{Q}_v) \cdot x^0$, then $\xi_v = 0$ and $\kappa_v(\mathcal{O}_v) = 0$; if $\mathcal{O}_v \neq G(\mathbf{Q}_v) \cdot x^0$, then $\xi_v \neq 0$ and $\kappa_v(\mathcal{O}_v) = 1$.

We define the Kottwitz invariant $\kappa(\mathcal{O}_{\mathbf{A}})$ of an orbit $\mathcal{O}_{\mathbf{A}} = \prod \mathcal{O}_v$ of $G(\mathbf{A})$ in $X(\mathbf{A})$ by $\kappa(\mathcal{O}_{\mathbf{A}}) = \sum_v i_v(\kappa_v(\mathcal{O}_v))$. We identify $C(H)$ with $\mathbf{Z}/2\mathbf{Z}$, and $C_v(H)$ with a subgroup of $\mathbf{Z}/2\mathbf{Z}$. With this identifications $\kappa(\mathcal{O}_{\mathbf{A}}) = \sum \kappa_v(\mathcal{O}_v)$.

We prefer the multiplicative rather than additive notation. Instead of $\mathbf{Z}/2\mathbf{Z}$ we consider the group $\{+1, -1\}$, and set

$$\nu_v(\mathcal{O}_v) = (-1)^{\kappa_v(\mathcal{O}_v)},\ \nu(\mathcal{O}_{\mathbf{A}}) = (-1)^{\kappa(\mathcal{O}_{\mathbf{A}})}.$$

Here $\nu_v(\mathcal{O}_v)$ and $\nu(\mathcal{O}_{\mathbf{A}})$ take the values ± 1. We have $\nu(\mathcal{O}_{\mathbf{A}}) = \prod \nu_v(\mathcal{O}_v)$. Since $\kappa_v(\mathcal{O}_v) = 0$ if and only if $\mathcal{O}_v = G(\mathbf{Q}_v) \cdot x^0$, we see that $\nu_v(\mathcal{O}_v) = +1$ if and only if $\mathcal{O}_v = G(\mathbf{Q}_v) \cdot x^0$. Hence our $\nu_v(\mathcal{O}_v)$ and $\nu(\mathcal{O}_{\mathbf{A}})$ coincide with $\nu_v(\mathcal{O}_v)$ and $\nu(\mathcal{O}_{\mathbf{A}})$, resp., introduced in Subsection 1.1.

By Thm. 3.6 of [2] an adelic orbit $\mathcal{O}_{\mathbf{A}}$ contains $\mathbf{Q}$-rational points if and only if $\kappa(\mathcal{O}_{\mathbf{A}}) = 0$. With our multiplicative notation $\kappa(\mathcal{O}_{\mathbf{A}}) = 0$ if and only if $\nu(\mathcal{O}_{\mathbf{A}}) = +1$. Thus $\mathcal{O}_{\mathbf{A}}$ contains $\mathbf{Q}$-points if and only if $\nu(\mathcal{O}_{\mathbf{A}}) = +1$. We have deduced Thm. 1.1 from [2], Thm. 3.6. ▮

1.3. Tamagawa measure

We define a gauge form on X, i.e. a regular differential form $\omega \in \Lambda^2(X)$ without zeroes. Recall that X is defined by the equation $f(x) = q$. Choose a differential form μ of degree 2 on W such that $\mu \wedge df = dx_1 \wedge dx_2 \wedge dx_3$, where x_1, x_2, x_3 are the coordinates in $W = \mathbf{Q}^3$. Let $\omega = \mu|_X$, the restriction of μ to X. Then ω is a gauge form on X, cf. [2], 1.3, and it does not depend on the choice of μ. The gauge form ω is G-invariant, because there exists a G-invariant gauge form on X, cf. [2], 1.4, and a gauge form on X is unique up to a scalar multiple, cf. [2], Cor. 1.5.4.

For any place v of $\mathbf{Q}$ one associates with ω a local measure m_v on $X(\mathbf{Q}_v)$, cf. [14], 2.2. We show how to define a Tamagawa measure on $X(\mathbf{A})$, following [2], 1.6.2.

We have by [2], 1.8.1, $\mu_p(X) = m_p(X(\mathbf{Z}_p))$, where $\mu_p(X)$ is defined in the Introduction. By [14], Thm. 2.2.5, for almost all p we have $m_p(X(\mathbf{Z}_p)) = \#X(\mathbf{F}_p)$.

We compute $\#X(\mathbf{F}_p)$. The group $\mathrm{SO}(f)(\mathbf{F}_p)$ acts on $X(\mathbf{F}_p)$ with stabilizer $\mathrm{SO}(f')(\mathbf{F}_p)$, where $\mathrm{SO}(f')(\mathbf{F}_p)$ is defined for almost all p. This action is transitive by Witt's theorem. Thus we obtain that $\#X(\mathbf{F}_p) = \#\mathrm{SO}(f)(\mathbf{F}_p)/\#\mathrm{SO}(f')(\mathbf{F}_p)$. By [1], III-6,

$$\#\mathrm{SO}(f)(\mathbf{F}_p) = p(p^2-1), \quad \#\mathrm{SO}(f')(\mathbf{F}_p) = p - \chi(p),$$

where $\chi(p) = -1$ if f' mod p does not represent 0, and $\chi(p) = +1$ if f' mod p represents 0. We have $\chi(p) = \left(\frac{-qD}{p}\right)$. We obtain for $p \nmid qD$

$$\#X(\mathbf{F}_p) = \frac{p(p^2-1)}{p-\chi(p)}, \quad \mu_p(X) = \frac{\#X(\mathbf{F}_p)}{p^2} = \frac{1-1/p^2}{1-\chi(p)/p} \ .$$

For $p|qD$ set $\chi(p) = 0$. We define

$$L_p(s,\chi) = (1-\chi(p)p^{-s})^{-1}, \quad L(s,\chi) = \prod_p L_p(s,\chi)$$

where s is a complex variable. We set

$$\lambda_p = L_p(1,\chi)^{-1} = 1 - \frac{\chi(p)}{p}, \quad r = L(1,\chi)^{-1}.$$

Then the product $\prod_p(\lambda_p^{-1}\mu_p)$ converges absolutely, hence the family (λ_p) is a family of convergence factors in the sense of [14], 2.3. We define, as in [2], 1.6.2, the measures

$$m_f = r^{-1}\prod_p(\lambda_p^{-1}m_p), \quad m = m_\infty m_f \ ,$$

then m_f is a measure on $X(\mathbf{A}_f)$ (where $\mathbf{A}_f$ is the ring of finite adèles) and m is a measure on $X(\mathbf{A})$. We call m the Tamagawa measure on $X(\mathbf{A})$.

1.4. Counting integer points

For $T > 0$ set $X(\mathbf{R})^T = \{x \in X(\mathbf{R}) : |x| \le T\}$.

Theorem 1.2.

$$N(T,X) \sim \int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x)dm.$$

In other words,

$$N(T,X) \sim 2m(\{x \in X(\mathbf{R})^T \times X(\hat{\mathbf{Z}}) : \nu(x) = +1\}). \quad (1)$$

Theorem 1.2 follows from [2], Thm. 5.3 (cf. [2], 6.4 and [2], Def. 2.3). For comparison note that

$$m(X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})) = m_\infty(X(\mathbf{R})^T)m_f(X(\hat{\mathbf{Z}})) = \mu_\infty(T,X)\mathfrak{S}(X), \quad (2)$$

cf. [2], 1.8.

The following lemma will be used in the proof of Theorem 0.1.

LEMMA 1.3. *Assume that there exists $y \in X(\mathbf{R} \times \hat{\mathbf{Z}})$ such that $\nu(y) = +1$. Then the set $X(\mathbf{Z})$ is infinite.*

Proof. Since ν is a locally constant function on $X(\mathbf{A})$, there exists a nonempty open subset $\mathcal{U}_f \in X(\hat{\mathbf{Z}})$ and an orbit $\mathcal{U}_\infty$ of $G(\mathbf{R})$ in $X(\mathbf{R})$ such that $\nu(x) = +1$ for all $x \in \mathcal{U}_\infty \times \mathcal{U}_f$. Set $\mathcal{U}_\infty^T = \{x \in \mathcal{U}_\infty : |x| \leq T\}$, then $m_\infty(\mathcal{U}_\infty^T) \to \infty$ as $T \to \infty$. We have

$$\int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x) dm \geq \int_{\mathcal{U}_\infty^T \times \mathcal{U}_f} \delta(x) dm = 2m_\infty(\mathcal{U}_\infty^T) m_f(\mathcal{U}_f) \; .$$

Since $2m_\infty(\mathcal{U}_\infty^T) m_f(\mathcal{U}_f) \to \infty$ as $T \to \infty$, we see that

$$\int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x) dm \to \infty \text{ as } T \to \infty,$$

and by Theorem 1.2 $N(T, X) \to \infty$. Hence $X(\mathbf{Z})$ is infinite. ∎

1.5. The constant c_X

Here we prove the following result:

PROPOSITION 1.4.

$$N(T, X) \sim c_X \mathfrak{S}(X) \mu_\infty(T, X) \; \textit{as} \; T \to \infty$$

with some constant c_X, $0 \leq c_X \leq 2$.

Proof. If $X(\mathbf{R})$ has two connected components, then by Theorem 0.2 (which we will prove in Sect. 4 below), $N(T, X) \sim \mathfrak{S}(X) \mu_\infty(T, X)$, so the proposition holds with $c_X = 1$.

If $X(\mathbf{R})$ has one connected component, then $X(\mathbf{R})$ consists of one $G(\mathbf{R})$-orbit and $\nu_\infty(X(\mathbf{R})) = +1$. For an orbit $\mathcal{O}_f = \prod \mathcal{O}_p$ of $G(\mathbf{A}_f)$ in $X(\mathbf{A}_f)$ we set $\nu_f(\mathcal{O}_f) = \prod_p \nu_p(\mathcal{O}_p)$. We regard ν_f as a locally constant function on $X(\mathbf{A}_f)$ taking the values ± 1. Define $X(\hat{\mathbf{Z}})_+ = \{x_f \in X(\hat{\mathbf{Z}}) : \nu_f(x_f) = +1\}$. We have

$$\int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x) dm = 2m_\infty(X(\mathbf{R})^T) m_f(X(\hat{\mathbf{Z}})_+).$$

Set $c_X = 2m_f(X(\hat{\mathbf{Z}})_+)/m_f(X(\hat{\mathbf{Z}}))$, then $0 \leq c_X \leq 2$ and

$$\int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x) dm = c_X m_\infty(X(\mathbf{R})^T) m_f(X(\hat{\mathbf{Z}})) = c_X \mu_\infty(T, X) \mathfrak{S}(X).$$

Using Theorem 1.2, we see that

$$N(T,X) \sim c_X \mu_\infty(T,X)\mathfrak{S}(X) \text{ as } T \to \infty.$$

$\blacksquare$

2. AN EXAMPLE OF $c_X = 0$

Let

$$f_1(x_1,x_2,x_3) = -9x_1^2 + 2x_1x_2 + 7x_2^2 + 2x_3^2,\ q = 1.$$

This example was mentioned in [2], 6.4.1. Here we provide a detailed exposition.

Consider the variety X defined by the equation $f_1(x) = q$. We have $f_1(-\frac{1}{2}, \frac{1}{2}, 1) = 1$. It follows that f_1 represents 1 over $\mathbf{R}$ and over $\mathbf{Z}_p$ for $p > 2$.

We have $f_1(4,1,1) = -127 \equiv 1 \pmod{2^7}$. We prove that f_1 represents 1 over $\mathbf{Z}_2$. Define a polynomial of one variable $F(Y) = f_1(4,1,Y) - 1$, $F \in \mathbf{Z}_2[Y]$. Then $F(1) = -2^7$, $|F(1)|_2 = 2^{-7}$, $F'(Y) = 4Y$, $|F'(1)^2|_2 = 2^{-4}$, $|F(1)|_2 < |F'(1)^2|_2$. By Hensel's lemma (cf. [11], II-§2, Prop. 2) F has a root in $\mathbf{Z}_2$. Thus f_1 represents 1 over $\mathbf{Z}_2$.

Now we prove that f_1 does not represent 1 over $\mathbf{Z}$. I know the following elementary proof from D. Zagier.

We prove the assertion by contradiction. Assume on the contrary that

$$-9x_1^2 + 2x_1x_2 + 7x_2^2 + 2x_3^2 = 1 \text{ for some } x_1, x_2, x_3 \in \mathbf{Z}.$$

We may write this equation as follows:

$$2x_3^2 - 1 = (x_1 - x_2)^2 + 8(x_1 - x_2)(x_1 + x_2).$$

The left hand side is odd, hence $x_1 - x_2$ is odd and therefore $x_1 + x_2$ is odd. We have $(x_1 - x_2)^2 \equiv 1 \pmod 8$. Hence the right hand side is congruent to $1 \pmod 8$. We see that x_3 is odd, hence $2x_3^2 - 1 \equiv 1 \pmod{16}$. But

$$8(x_1 - x_2)(x_1 + x_2) \equiv 8 \pmod{16}.$$

It follows that

$$\begin{aligned} (x_1 - x_2)^2 &\equiv 9 \pmod{16} \\ x_1 - x_2 &\equiv \pm 3 \pmod 8. \end{aligned}$$

Therefore $x_1 - x_2$ must have a prime factor $p \equiv \pm 3 \pmod 8$. Hence $2x_3^2 - 1$ has a prime factor $p \equiv \pm 3 \pmod 8$. On the other hand, if

$p|(2x_3^2-1)$, then

$$2x_3^2 \equiv 1 \pmod p$$

and 2 is a square modulo p, $\left(\dfrac{2}{p}\right) = 1$. By the quadratic reciprocity law $p \equiv \pm 1 \pmod 8$. Contradiction. We have proved that f_1 does not represent 1 over $\mathbf{Z}$, hence $N(T,X)=0$ for all T.

On the other hand,

$$\mathfrak{S}(X)\mu_\infty(T,X) = m_f(X(\hat{\mathbf{Z}}))m_\infty(X(\mathbf{R})^T).$$

Since $X(\hat{\mathbf{Z}})$ is a nonempty open subset in $X(\mathbf{A}_f)$, $m_f(X(\hat{\mathbf{Z}}))>0$. Now $m_\infty(X(\mathbf{R})^T)\to\infty$ as $T\to\infty$. Hence $\mathfrak{S}(X)\mu_\infty(T,X)\to\infty$ as $T\to\infty$, and thus $c_X=0$.

3. PROOF OF THEOREM 0.1

Lemma 3.1. *Let k be a field of characteristic different from 2, and let V be a finite-dimensional vector space over k. Let f be a non-degenerate quadratic form on V. Let $u\in \mathrm{GL}(V)(k)$, $f'=u^*f$. Then the map $y\mapsto uy\colon V\to V$ takes the orbits of $\mathrm{Spin}(f)(k)$ in V to the orbits of $\mathrm{Spin}(f')(k)$.*

Proof. Let $x\in V$, $f(x)\neq 0$. The reflection (symmetry) $r_x=r_{f,x}\colon V\to V$ is defined by

$$r_x(y) = y - \frac{2B(x,y)}{f(x)}x, \quad y\in V,$$

where B is the symmetric bilinear form on V associated with f. Every $s\in \mathrm{SO}(f)(k)$ can be written as

$$s = r_{x_1}\cdots r_{x_l} \tag{3}$$

cf. [12], Thm. 43:3. The spinor norm $\theta(s)$ of s is defined by

$$\theta(s) = f(x_1)\cdots f(x_l) \pmod{k^{*2}} \ \in k^*/k^{*2}$$

and it does not depend on the choice of the representation given by (3), cf. [12], §55. Let $\Theta(f)$ denote the image of $\mathrm{Spin}(f)(k)$ in $\mathrm{SO}(f)(k)$. Then $s\in\mathrm{SO}(f)(k)$ is contained in $\Theta(f)$ if and only if $\theta(s)=1$, cf. [13], III-3.2 or [3], Ch. 10, Thm. 3.3.

Now let u, f' be as above. Then $r_{f',ux}=ur_{f,x}u^{-1}$, $f'(ux)=f(x)$, and so $\theta_{f'}(usu^{-1})=\theta_f(s)$. We conclude that $u\Theta(f)u^{-1}=\Theta(f')$ and that the map $y\mapsto uy$ takes the orbits of $\Theta(f)$ in V to the orbits of $\Theta(f')$. ∎

Let f, f' be integral-matrix quadratic forms on $\mathbf{Z}^n$ and assume that f' is in the genus of f. Then there exists $u \in \mathrm{GL}_n(\mathbf{R} \times \hat{\mathbf{Z}})$ such that $f'(x) = f(u^{-1}x)$ for $x \in \mathbf{A}^n$. Let $q \in \mathbf{Z}$, $q \neq 0$. Let X denote the affine quadric $f(x) = q$, and X' denote the quadric $f'(x) = q$.

Lemma 3.2. *The map $x \mapsto ux\colon \mathbf{A}^n \to \mathbf{A}^n$ takes $X(\mathbf{R} \times \hat{\mathbf{Z}})$ to $X'(\mathbf{R} \times \hat{\mathbf{Z}})$ and takes orbits of $\mathrm{Spin}(f)(\mathbf{A})$ in $X(\mathbf{A})$ to orbits of $\mathrm{Spin}(f')(\mathbf{A})$ in $X'(\mathbf{A})$.*

Proof. Let A denote the matrix of f, and A' denote the matrix of f'. We have

$$(u^{-1})^t A u^{-1} = A', \qquad A = u^t A' u \,.$$

The variety X is defined by the equation $x^t A x = q$, and X' is defined by $x^t A' x = q$. One can easily check that the map $x \mapsto ux$ takes $X(\mathbf{R} \times \hat{\mathbf{Z}})$ to $X'(\mathbf{R} \times \hat{\mathbf{Z}})$ and $X(\mathbf{A})$ to $X'(\mathbf{A})$.

In order to prove that the map $x \mapsto ux\colon X(\mathbf{A}) \to X'(\mathbf{A})$ takes the orbits of $\mathrm{Spin}(f)(\mathbf{A})$ to the orbits of $\mathrm{Spin}(f')(\mathbf{A})$, it suffices to prove that the map $x \mapsto u_v x\colon X(\mathbf{Q}_v) \to X'(\mathbf{Q}_v)$ takes the orbits of $\mathrm{Spin}(f)(\mathbf{Q}_v)$ to the orbits of $\mathrm{Spin}(f')(\mathbf{Q}_v)$ for every v, where u_v is the v-component of u. This last assertion follows from Lemma 3.1. ▮

Proposition 3.3. *Let f' and q be as in Theorem 0.1, in particular f' represents q over $\mathbf{Z}_v$ for any v (we set $\mathbf{Z}_\infty = \mathbf{R}$), but not over $\mathbf{Z}$. Let X' be the quadric defined by $f'(x) = q$. Then $X'(\mathbf{R} \times \hat{\mathbf{Z}})$ is contained in one orbit of $\mathrm{Spin}(f')(\mathbf{A})$.*

Proof. Set $G' = \mathrm{Spin}(f')$. We prove that $X'(\mathbf{Z}_v)$ is contained in one orbit of $G'(\mathbf{Q}_v)$ for every v by contradiction. Assume on the contrary that for some v the set $X'(\mathbf{Z}_v)$ has nontrivial intersection with two orbits of $G'(\mathbf{Q}_v)$. Then ν_v takes both values $+1$ and -1 on $X'(\mathbf{Z}_v)$. It follows that ν takes both values $+1$ and -1 on $X'(\mathbf{R} \times \hat{\mathbf{Z}})$. Hence by Lemma 1.3 X' has infinitely many $\mathbf{Z}$-points. This contradicts to the assumption that f' does not represent q over $\mathbf{Z}$. ▮

Proof of Theorem 0.1. Let $u \in \mathrm{GL}_3(\mathbf{R} \times \hat{\mathbf{Z}})$ be such that $f'(x) = f(u^{-1}x)$. Let X, X' be as above, in particular X' has no $\mathbf{Z}$-points. By Prop. 3.3 $X'(\mathbf{R} \times \hat{\mathbf{Z}})$ is contained in one orbit of $\mathrm{Spin}(f')(\mathbf{A})$. It follows from Lemma 3.2 that $X(\mathbf{R} \times \hat{\mathbf{Z}})$ is contained in one orbit of $\mathrm{Spin}(f)(\mathbf{A})$. Since f represents q over $\mathbf{Z}$, this orbit has $\mathbf{Q}$-rational points, and ν equals $+1$ on $X(\mathbf{R} \times \hat{\mathbf{Z}})$. Thus δ equals 2 on $X(\mathbf{R} \times \hat{\mathbf{Z}})$, and by Formulas (1) and (2) of Subsection 1.4 $N(T, X) \sim 2\mathfrak{S}(X)\mu_\infty(T, X)$. ▮

4. PROOF OF THEOREM 0.2

We prove Theorem 0.2. We define an involution τ_∞ of $X(\mathbf{R})$ by $\tau_\infty(x) = -x$, $x \in X(\mathbf{R}) \subset \mathbf{R}^3$. Since $f(x) = f(-x)$, τ_∞ is well defined, i.e takes $X(\mathbf{R})$ to itself. Since $|-x| = |x|$, τ_∞ takes $X(\mathbf{R})^T$ to itself. We define an involution τ of $X(\mathbf{A})$ by defining τ as τ_∞ on $X(\mathbf{R})$ and as 1 on $X(\mathbf{Q}_p)$ for all prime p. Then τ respects the Tamagawa measure m on $X(\mathbf{A})$.

By assumption $X(\mathbf{R})$ has two connected components. These are the two orbits of $\mathrm{Spin}(f)(\mathbf{R})$. The involution τ_∞ of $X(\mathbf{R})$ interchanges these two orbits. Thus we have

$$\nu_\infty(\tau_\infty(x_\infty)) = -\nu_\infty(x_\infty) \text{ for all } x_\infty \in X(\mathbf{R}) \tag{4}$$

$$\nu(\tau(x)) = -\nu(x) \text{ for all } x \in X(\mathbf{A}) \tag{5}$$

Let $X(\mathbf{R})_1$ and $X(\mathbf{R})_2$ be the two connected components of $X(\mathbf{R})$. Set

$$X(\mathbf{R})_1^T = X(\mathbf{R})_1 \cap X(\mathbf{R})^T, \quad X(\mathbf{R})_2^T = X(\mathbf{R})_2 \cap X(\mathbf{R})^T$$

Then τ interchanges $X(\mathbf{R})_1^T \times X(\hat{\mathbf{Z}})$ and $X(\mathbf{R})_2^T \times X(\hat{\mathbf{Z}})$. From Formula (5) in this section we have

$$\int_{X(\mathbf{R})_1^T \times X(\hat{\mathbf{Z}})} \nu(x) dm = -\int_{X(\mathbf{R})_2^T \times X(\hat{\mathbf{Z}})} \nu(x) dm,$$

hence

$$\int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \nu(x) dm = 0.$$

Since $\delta(x) = \nu(x) + 1$, we obtain

$$\int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x) dm = \int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} dm = m(X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})),$$

and $m(X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})) = \mathfrak{S}(X)\mu_\infty(T,X)$. By Theorem 1.2

$$N(T,X) \sim \int_{X(\mathbf{R})^T \times X(\hat{\mathbf{Z}})} \delta(x) dm.$$

Thus $N(T,X) \sim \mathfrak{S}(X)\mu_\infty(T,X)$ as $T \to \infty$, i.e. $c_X = 1$. ∎

ACKNOWLEDGMENT

This paper was partly written when the author was visiting Sonderforschungsbereich 343 "Diskrete Strukturen in der Mathematik" at Bielefeld University, and I am grateful to SFB 343 for hospitality and support. I thank Rainer Schulze-Pillot and John S. Hsia for useful e-mail correspondence. I am grateful to Zeév Rudnick for useful discussions and help in analytic calculations.

REFERENCES

1. E. Artin, Geometric Algebra, Interscience Publishers, New York, 1957.
2. M. Borovoi and Z. Rudnick, Hardy-Littlewood varieties and semisimple groups, *Invent. Math.* **111** (1995), 37–66.
3. J. W. S. Cassels, Rational Quadratic Forms, Academic Press, London, 1978.
4. J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups, 2nd edition, Springer-Verlag, New York, 1993.
5. H. Davenport, Analytic Methods for Diophantine Equations and Diophantine Inequalities, Ann Arbor Publishers, Ann Arbor, Mich., 1962.
6. W. Duke, Z. Rudnick and P. Sarnak, Density of integer points on affine homogeneous varieties, *Duke Math. J.* **71** (1993), 143–179.
7. A. Eskin and C. McMullen, Mixing, counting, and equidistribution in Lie groups, *Duke Math. J.* **71** (1993), 181–209.
8. A. Eskin, S. Mozes and N. Shah, Unipotent flows and counting lattice points on homogeneous spaces, *Ann. of Math.* (2) **143** (1996), 253–299.
9. T. Estermann, A new application of the Hardy-Littlewood-Kloosterman method, *Proc. London Math. Soc.* **12** (1962), 425–444.
10. R. E. Kottwitz, Stable trace formula: elliptic singular terms, *Math. Ann.* **275** (1986), 365–399.
11. S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.
12. O. T. O'Meara, Introduction to Quadratic Forms, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.
13. J.-P. Serre, Cohomologie galoisienne, 5th edition, Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin-Heidelberg-New York, 1994.
14. A. Weil, Adeles and Algebraic Groups, Birkhäuser, Boston, 1982