ON REPRESENTATIONS OF INTEGERS BY INDEFINITE TERNARY QUADRATIC FORMS

Mikhail Borovoi

Abstract. 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 values 0, 1, 2.

0. Introduction

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

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

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

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

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

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

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

where $T \in \mathbb{R}$, $T > 0$. 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

$$\mu_p(X) = \lim_{k \to \infty} \frac{\#X(\mathbb{Z}/p^k\mathbb{Z})}{(p^k)^{n-1}}.$$
For almost all \( p \) it suffices to take \( k = 1 \):

\[
\mu_p = \frac{\#X(F_p)}{p^{n-1}}.
\]

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

\[
\mu_\infty(T, X) = \lim_{\varepsilon \to 0} \frac{\text{Vol}\{x \in \mathbb{R}^n : |x| \leq T, |f(x) - q| < \varepsilon/2, \}}{\varepsilon},
\]

it is called the singular integral.

**Theorem.** For \( n \geq 4 \)

\[
N(T, X) \sim \mathcal{S}(X)\mu_\infty(T, X) \text{ as } T \to \infty.
\]

This theorem follows from results of [BR], 6.4 (based on analytical results of [DRS], [EM], [EMS]). For certain non-Euclidean norms it was earlier proved by the Hardy-Littlewood circle method, cf. [Da], [Est].

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 \( \mathcal{S}(X) = \prod \mu_p(X) \) conditionally converges (see Sect. 1 below), but in general \( N(T, X) \) is not asymptotically \( \mathcal{S}(X)\mu_\infty(T, X) \). From results of [BR] it follows that

\[
N(T, X) \sim c_X \mathcal{S}(X)\mu_\infty(T, X) \text{ as } T \to \infty
\]

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

A case when \( c_X = 0 \) was already known to Siegel, see also [BR], 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 \( \mathbb{Z} \), so \( N(T, X) = 0 \) for all \( T \). On the other hand, \( f_1 \) represents 1 over \( \mathbb{R} \) and over \( \mathbb{Z}_p \) for all \( p \), and \( \mathcal{S}(X)\mu_\infty(T, X) \to \infty \) as \( T \to \infty \). Thus \( c_X = 0 \) (see details in Sect. 2).

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

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

\[
N(T, X) \sim 2\mathcal{S}(X)\mu_\infty(T, X) \text{ as } T \to \infty.
\]

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. [CS], 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 \( 2 \mathcal{G}(X)\mu_\infty(T, X) \sim 0.794T \). On the other hand, numeric calculations give \( N(T, X)/T = 0.8024 \).

We also show that \( c_X \) can take the value 1.

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

\[
N(T, X) \sim \mathcal{G}(X)\mu_\infty(T, X) \text{ as } T \to \infty.
\]

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 \( X(\mathbb{R}) \) has two connected components, and by Theorem 0.2 \( c_X = 1 \). Analytic and numeric calculations give \( \mathcal{G}(X)\mu_\infty(T, X) \sim 0.7065T \). On the other hand, numeric calculations give \( N(T, X)/T = 0.7048 \).

**Question 0.3.** Can \( c_X \) take values other than 0, 1, 2?

**Remark 0.4.** It seems that Theorems 0.1 and 0.2 also can be proved using a result of Kneser ([Kn], Satz 2) together with Siegel’s weight formula [Si] and the results of [DRS], [EM], [EMS].

The plan of the paper is the following. In Section 1 we expose results of [BR] 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.

**Acknowledgements.** 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 Zéev Rudnick for useful discussions and help in analytic calculations.

1. Results of [BR] in the case of ternary quadratic forms

1.0. Let \( f \) be an indefinite ternary integral-matrix quadratic form

\[
f(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \quad a_{ij} \in \mathbb{Z}, \quad a_{ij} = a_{ji}.
\]

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

Let \( W = \mathbb{Q}^3 \) 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 \( \mathbb{Q} \)-point \( x^0 \). Set \( G = \text{Spin}(W, f) \), 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 $A$ denote the adèle ring of $Q$. The group $G(A)$ acts on $X(A)$; let $O_A$ be an orbit. We are interested whether $O_A$ has a $Q$-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 $H = \text{Spin}(W', f')$. 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 $K = Q(\sqrt{-qD})$, then $K$ is a quadratic extension of $Q$, because $-qD$ is not a square. The torus $H$ is anisotropic over $Q$ (because $-qD$ is not a square), and $H$ splits over $K$. Let $X_*(H_K)$ denote the cocharacter group of $H_K$, $X_*(H_K) = \text{Hom}(\mathbb{G}_{m,K}, H_K)$; then $X_*(H_K) \simeq \mathbb{Z}$. The non-neutral element of $\text{Gal}(K/Q)$ acts on $X_*(H_K)$ by multiplication by $-1$.

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

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

For $x \in X(A)$ 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 $\delta$ is a locally constant function on $X(A)$.

**Theorem 1.1.1.** An orbit $O_A$ of $G(A)$ in $X(A)$ has a $Q$-rational point if and only if $\nu(O_A) = +1$.

Below we will deduce Theorem 1.1.1 from [BR], Thm. 3.6.

1.2. Proof of Theorem 1.1.1. For a torus $T$ over a field $k$ of characteristic 0 we define a finite abelian group $C(T)$ as follows:

$$C(T) = (X_*(T_k)_{\text{Gal}(\bar{k}/k)})_{\text{tors}}$$

where $\bar{k}$ is a fixed algebraic closure of $k$, $X_*(T_k)_{\text{Gal}(\bar{k}/k)}$ denotes the group of coinvariants, and $(\cdot)_{\text{tors}}$ 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 $i_v : C_v(T) \to C(T)$ induced by an inclusion $\text{Gal}(\bar{k}_v/k_v) \to \text{Gal}(\bar{k}/k)$. These definitions were given for connected reductive groups (not only for tori) by Kottwitz [Ko], see also [BR], 3.4. Kottwitz writes $A(T)$ instead of $C(T)$.

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

$$C(H) = (X_*(H_{\bar{k}})_{\text{Gal}(\bar{k}/Q)})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}.$$ 

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

We now define the local invariants $\kappa_v(O_v)$ as in [BR], where $O_v$ is an orbit of $G(Q_v)$ in $X(Q_v)$. The set of orbits of $G(Q_v)$ in $X(Q_v)$ is in canonical bijection with $\text{ker}[H_1(O_v, H) \to H^1(Q_v, G)]$, cf. [Se], I.5.4, Cor. 1 of Prop. 36. Hence $O_v$ defines
a cohomology class $\xi_v \in H^1(Q_v, H)$. The local Tate–Nakayama duality for tori defines a canonical homomorphism $\beta_v: H^1(Q_v, H) \to C_v(H)$, see [Ko], Thm. 1.2. (Kottwitz defines the map $\beta_v$ in a more general setting, when $H$ is any connected reductive group over a number field.) The homomorphism $\beta_v$ is an isomorphism for any $v$. We set $\kappa_v(O_v) = \beta_v(\xi_v)$. Note that if $O_v = G(Q_v) \cdot x^0$, then $\xi_v = 0$ and $\kappa_v(O_v) = 0$; if $O_v \neq G(Q_v) \cdot x^0$, then $\xi_v \neq 0$ and $\kappa_v(O_v) = 1$.

We define the Kottwitz invariant $\kappa(O_A)$ of an orbit $O_A = \prod O_v$ of $G(A)$ in $X(A)$ by $\kappa(O_A) = \prod_v \kappa_v(O_v)$. We identify $C(H)$ with $\mathbb{Z}/2\mathbb{Z}$, and $C_v(H)$ with a subgroup of $\mathbb{Z}/2\mathbb{Z}$. With this identifications $\kappa(O_A) = \sum \kappa_v(O_v)$.

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

$$\nu_v(O_v) = (-1)^{\kappa_v(O_v)}, \quad \nu(O_A) = (-1)^{\kappa(O_A)}.$$ 

Here $\nu_v(O_v)$ and $\nu(O_A)$ take values $\pm 1$. We have $\nu(O_A) = \prod \nu_v(O_v)$. Since $\kappa_v(O_v) = 0$ if and only if $O_v = G(Q_v) \cdot x^0$, and $\nu_v(O_v) = +1$ if and only if $O_v = G(Q_v) \cdot x^0$. Hence our $\nu_v(O_v)$ and $\nu(O_A)$ coincide with $\nu_v(O_v)$ and $\nu(O_A)$ introduced in 1.1.

By Thm. 3.6 of [BR] an adelic orbit $O_A$ contains $\mathbb{Q}$-rational points if and only if $\kappa(O_A) = 0$. With our multiplicative notation $\kappa(O_A) = 0$ if and only if $\nu(O_A) = +1$. Thus $O_A$ contains $\mathbb{Q}$-points if and only if $\nu(O_A) = +1$. We have deduced Thm. 1.1.1 from [BR], 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 $\mu \in \Lambda^2(W)$ such that $\mu \wedge df = dx_1 \wedge dx_2 \wedge dx_3$, where $x_1, x_2, x_3$ are the coordinates in $W = Q^3$. Let $\omega = \mu|_X$, the restriction of $\mu$ to $X$. Then $\omega$ is a gauge form on $X$, cf. [BR], 1.3, and it does not depend on the choice of $\mu$. The gauge form $\omega$ is $G$-invariant, because there exists a $G$-invariant gauge form on $X$, cf. [BR], 1.4, and a gauge form on $X$ is unique up to a scalar multiple, cf. [BR], Cor. 1.5.4.

For any place $v$ of $Q$ one associates with $\omega$ a local measure $m_v$ on $X(Q_v)$, cf. [We], 2.2. We show how to define a Tamagawa measure on $X(A)$, following [BR], 1.6.2.

We have by [BR], 1.8.1, $\mu_p(X) = m_p(X(Z_p))$, where $\mu_p(X)$ is defined in the Introduction. By [We], Thm. 2.2.5, for almost all $p$ we have $m_p(X(Z_p)) = \#X(F_p)$.

We compute $\#X(F_p)$. The group $SO(f)(F_p)$ acts on $X(F_p)$ with stabilizer $SO(f')(F_p)$, where $SO(f')(F_p)$ is defined for almost all $p$. This action is transitive by Witt’s theorem. Thus $\#X(F_p) = \#SO(f)(F_p)/\#SO(f')(F_p)$. By [A], III-6,

$$\#SO(f)(F_p) = p(p^2 - 1), \quad \#SO(f')(F_p) = p - \chi(p),$$

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 $p \nmid qD$

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

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

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

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 $(\lambda_p)$ is a family of convergence factors in the sense of [We], 2.3. We define, as in [BR], 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 $X(\mathbb{A}_f)$ (where $\mathbb{A}_f$ is the ring of finite adèles) and $m$ is a measure on $X(\mathbb{A})$. We call $m$ the Tamagawa measure on $X(\mathbb{A})$.

1.4. Counting integer points. For $T > 0$ set $X(\mathbb{R})^T = \{ x \in X(\mathbb{R}) : |x| \leq T \}$.

Theorem 1.4.1.

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

In other words,

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

Theorem 1.4.1 follows from [BR], Thm. 5.3 (cf. [BR], 6.4 and [BR], Def. 2.3).

For comparison note that

$$
m(X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})) = m_{\infty}(X(\mathbb{R})^T)m_f(X(\hat{\mathbb{Z}})) = \mu_{\infty}(T, X) \mathcal{S}(X),
$$

cf. [BR], 1.8.

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

Lemma 1.4.2. Assume that there exists $y \in X(\mathbb{R} \times \hat{\mathbb{Z}})$ such that $\nu(y) = +1$. Then the set $X(\mathbb{Z})$ is infinite.

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

$$
\int_{X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})} \delta(x) dm \geq \int_{U_{\infty}^T \times U_f} \delta(x) dm = 2m_{\infty}(U_{\infty}^T)m_f(U_f).
$$

Since $2m_{\infty}(U_{\infty}^T)m_f(U_f) \rightarrow \infty$ as $T \rightarrow \infty$, we see that

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

and by Theorem 1.4.1 $N(T, X) \rightarrow \infty$. Hence $X(\mathbb{Z})$ is infinite. \square

1.5. The constant $c$. Here we prove the following result:
Proposition 1.5.1.

\[ N(T, X) \sim c_X \mathcal{G}(X) \mu_\infty(T, X) \text{ as } T \to \infty \]

with some constant \( c_X \), \( 0 \leq c_X \leq 2 \).

Proof. If \( X(\mathbb{R}) \) has two connected components, then by Theorem 0.2 (which we will prove in Sect. 3 below), \( N(T, X) \sim \mathcal{G}(X) \mu_\infty(T, X) \), so the proposition holds with \( c_X = 1 \).

If \( X(\mathbb{R}) \) has one connected component, then \( X(\mathbb{R}) \) consists of one \( G(\mathbb{R}) \)-orbit and \( \nu_\infty(X(\mathbb{R})) = +1 \). For an orbit \( O_f = \prod \mathcal{O}_p \) of \( G(\mathbb{A}_f) \) in \( X(\mathbb{A}_f) \) we set \( \nu_f(O_f) = \prod_p \nu_p(O_p) \). We regard \( \nu_f \) as a locally constant function on \( X(\mathbb{A}_f) \) taking values \pm 1. We have

\[
\int_{X(\mathbb{R})^r \times X(\mathbb{Z})} \delta(x) dm = 2m_\infty(X(\mathbb{R})^T) m_f(X(\hat{Z})_+) \]

where \( X(\hat{Z})_+ = \{ x_f \in X(\hat{Z}) : \nu_f(x_f) = +1 \} \). Set \( c_X = 2m_f(X(\hat{Z})_+)/m_f(X(\hat{Z})) \), then \( 0 \leq c_X \leq 2 \) and

\[
\int_{X(\mathbb{R})^r \times X(\mathbb{Z})} \delta(x) dm = c_X m_\infty(X(\mathbb{R})^T) m_f(X(\hat{Z})) = c_X \mu_\infty(T, X) \mathcal{G}(X). \]

Using Theorem 1.4.1, we see that

\[ N(T, X) \sim c_X \mu_\infty(T, X) \mathcal{G}(X) \text{ as } T \to \infty. \]

\[ \square \]

2. An example of \( c_X = 0 \)

Let

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

This example was mentioned by Siegel and later mentioned in [BR], 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 \( \mathbb{R} \) and over \( \mathbb{Z}_p \) for \( p > 2 \).

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

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

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

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

We may write this equation as follows:

\[ 2x_1^2 - 1 = (x_1 - x_2)(x_1 + x_2) + 8(x_1 - x_2)(x_1 + x_2). \]
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
\[
(x_1 - x_2)^2 \equiv 9 \pmod{16}
\]
\[
x_1 - x_2 \equiv \pm 3 \pmod{8}.
\]
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 \( p \). By the quadratic reciprocity law \( p \equiv \pm 1 \pmod{8} \). Contradiction. We have proved that \( f_1 \) does not represent 1 over \( \mathbb{Z} \), hence \( N(T, X) = 0 \) for all \( T \).

On the other hand,
\[
\mathcal{G}(X)\mu_\infty(T, X) = m_f(X(\mathbb{Z}))m_\infty(X(\mathbb{R})^T).
\]
Since \( X(\mathbb{Z}) \) is a non-empty open subset in \( X(\mathbb{A}_f) \), \( m_f(X(\mathbb{Z})) > 0 \). Now the measure \( m_\infty(X(\mathbb{R})^T) \to \infty \) as \( T \to \infty \). Hence \( \mathcal{G}(X)\mu_\infty(T, X) \to \infty \) as \( T \to \infty \), and thus \( c_X = 0 \).

3. Proof of Theorem 0.1

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

**Proof.** Let \( x \in V \), \( f(x) \neq 0 \). The reflection (symmetry) \( r_x = r_{f,x} : V \to V \) 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 \( s \in \text{SO}(f)(k) \) can be written as
\[
s = r_{x_1} \cdots r_{x_l}
\]
cf. [OM], Thm. 43.3. The spinor norm \( \theta(s) \) of \( s \) is defined by
\[
\theta(s) = f(x_1) \cdots f(x_l) \pmod{k^*/k^2}
\]
and it does not depend on the choice of the representation (3.1), cf. [OM], §55. Let \( \Theta(f) \) denote the image of \( \text{Spin}(f)(k) \) in \( \text{SO}(f)(k) \). Then \( s \in \text{SO}(f)(k) \) is contained in \( \Theta(f) \) if and only if \( \theta(s) = 1 \), cf. [Se], III-3.2 or [Ca], 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 \( \Theta(f') \). \( \square \)

Let \( f, f' \) be integral-matrix quadratic forms on \( \mathbb{Z}^n \) and assume that \( f' \) is in the genus of \( f \). Then there exists \( u \in \text{GL}_n(\mathbb{R} \times \mathbb{Z}) \) such that \( f'(x) = f(u^{-1}x) \) for \( x \in \mathbb{A}^n \). Let \( q \in \mathbb{Z}, q \neq 0 \). Let \( X \) denote the affine quadric \( f(x) = q \), and \( X' \) denote the quadric \( f'(x) = q \).
Lemma 3.2. The map $x \mapsto ux: \mathbb{A}^n \to \mathbb{A}^n$ takes $X(\mathbb{R} \times \hat{\mathbb{Z}})$ to $X'(\mathbb{R} \times \hat{\mathbb{Z}})$ and takes orbits of $\text{Spin}(f)(\mathbb{A})$ in $X(\mathbb{A})$ to orbits of $\text{Spin}(f')(\mathbb{A})$ in $X'(\mathbb{A})$.

Proof. Let $A$ denote the matrix of $f$, and $A'$ denote the matrix of $f'$. We have
\[
(u^{-1})^tAu^{-1} = A'.
\]
The variety $X$ is defined by the equation $x^tAx = q$, and $X'$ is defined by $x'^tA'x = q$. One can easily check that the map $x \mapsto ux$ takes $X(\mathbb{R} \times \hat{\mathbb{Z}})$ to $X'(\mathbb{R} \times \hat{\mathbb{Z}})$ and $X(\mathbb{A})$ to $X'(\mathbb{A})$.

In order to prove that the map $x \mapsto ux: X(\mathbb{A}) \to X'(\mathbb{A})$ takes the orbits of $\text{Spin}(f)(\mathbb{A})$ to the orbits of $\text{Spin}(f')(\mathbb{A})$, it suffices to prove that the map $x \mapsto u_vx: X(\mathbb{Q}_v) \to X'(\mathbb{Q}_v)$ takes the orbits of $\text{Spin}(f)(\mathbb{Q}_v)$ to the orbits of $\text{Spin}(f')(\mathbb{Q}_v)$ 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 $\mathbb{Z}_v$ for any $v$ (we set $\mathbb{Z}_\infty = \mathbb{R}$), but not over $\mathbb{Z}$. Let $X'$ be the quadric defined by $f'(x) = q$. Then $X'(\mathbb{R} \times \hat{\mathbb{Z}})$ is contained in one orbit of $\text{Spin}(f')(\mathbb{A})$.

Proof. Set $G' = \text{Spin}(f')$. We prove that $X'(\mathbb{Z}_v)$ is contained in one orbit of $G'(\mathbb{Q}_v)$ for every $v$ by contradiction. Assume on the contrary that for some $v$ $X'(\mathbb{Z}_v)$ has nontrivial intersection with two orbits of $G'(\mathbb{Q}_v)$. Then $u_v$ takes both values $+1$ and $-1$ on $X'(\mathbb{Z}_v)$. It follows that $v$ takes both values $+1$ and $-1$ on $X'(\mathbb{R} \times \hat{\mathbb{Z}})$. Hence by Lemma 1.4.2 $X'$ has infinitely many $\mathbb{Z}$-points. This contradicts to the assumption that $f'$ does not represent $q$ over $\mathbb{Z}$. □

Proof of Theorem 0.1. Let $u \in \text{GL}_2(\mathbb{R} \times \hat{\mathbb{Z}})$ be such that $f'(x) = f(u^{-1}x)$. Let $X, X'$ be as in the beginning of this section, in particular $X'$ has no $\mathbb{Z}$-points. By Prop. 3.3 $X'(\mathbb{R} \times \hat{\mathbb{Z}})$ is contained in one orbit of $\text{Spin}(f')(\mathbb{A})$. It follows from Lemma 3.2 that $X(\mathbb{R} \times \hat{\mathbb{Z}})$ is contained in one orbit of $\text{Spin}(f)(\mathbb{A})$. Since $f$ represents $q$ over $\mathbb{Z}$, this orbit has $\mathbb{Q}$-rational points, and $v$ equals $+1$ on $X(\mathbb{R} \times \hat{\mathbb{Z}})$. Thus $\delta$ equals 2 on $X(\mathbb{R} \times \hat{\mathbb{Z}})$, and by Formulas (1.4.1) and (1.4.2) $N(T, X) \sim 2\tilde{\mathcal{S}}(X)\mu_{\infty}(T, X)$. □

4. Proof of Theorem 0.2

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

By assumption $X(\mathbb{R})$ has two connected components. These are two orbits of $\text{Spin}(f)(\mathbb{R})$. The involution $\tau_\infty$ of $X(\mathbb{R})$ interchanges these two orbits. Thus we have
\[
\nu_\infty(\tau_\infty(x_\infty)) = -\nu_\infty(x_\infty) \text{ for all } x_\infty \in X(\mathbb{R})
\]
(4.1)
\[
\nu(\tau(x)) = -\nu(x) \text{ for all } x \in X(\mathbb{A})
\]

Let $X(\mathbb{R})_1$ and $X(\mathbb{R})_2$ be the two connected components of $X(\mathbb{R})$. Set
\[
X(\mathbb{R})^T = X(\mathbb{R})_1 \lor X(\mathbb{R})_2 \lor X(\mathbb{R})^T = X(\mathbb{R})_1 \lor X(\mathbb{R})_2 \lor X(\mathbb{R})^T.
\]
Then $\tau$ interchanges $X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})$ and $X(\mathbb{R})^T_2 \times X(\hat{\mathbb{Z}})$. From Formula (4.1) we have
\[
\int_{X(\mathbb{R})^T_1 \times X(\hat{\mathbb{Z}})} \nu(x) dm = -\int_{X(\mathbb{R})^T_2 \times X(\hat{\mathbb{Z}})} \nu(x) dm,
\]
hence
\[
\int_{X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})} \nu(x) dm = 0.
\]
Since $\delta(x) = \nu(x) + 1$, we obtain
\[
\int_{X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})} \delta(x) dm = \int_{X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})} dm = m(X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})) = \mathfrak{G}(X)\mu_{\infty}(T, X).
\]
By Theorem 1.4.1
\[
N(T, X) \sim \int_{X(\mathbb{R})^T \times X(\hat{\mathbb{Z}})} \delta(x) dm.
\]
Thus $N(T, X) \sim \mathfrak{G}(X)\mu_{\infty}(T, X)$ as $T \to \infty$, i.e. $c_X = 1$. □

References

[A] E. Artin, Geometric Algebra, Interscience Publishers, New York, 1957.
[BR] M. Borovoi, Z. Rudnick, Hardy-Littlewood varieties and semisimple groups, Invent. Math. 111 (1995), 37–66.
[Ca] J. W. S. Cassels, Rational Quadratic Forms, Academic Press, London, 1978.
[CS] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups, 2nd edition, Springer-Verlag, New York, 1993.
[Da] H. Davenport, Analytic Methods for Diophantine Equations and Diophantine Inequalities, Ann Arbor Publishers, Ann Arbor, Michigan, 1962.
[DRS] W. Duke, Z. Rudnick and P. Sarnak, Density of integer points on affine homogeneous varieties, Duke Math. Jour. 71 (1993), 143–179.
[EM] A. Eskin and C. McMullen, Mixing, counting, and equidistribution in Lie groups, Duke Math. J. 71 (1993), 181–209.
[EMS] A. Eskin, S. Mozes and N. Shah, Unipotent flows and counting lattice points on homogeneous spaces, Ann. of Math. (2) 143 (1996), 253–299.
[Est] T. Estermann, A new application of the Hardy-Littlewood-Kloosterman method, Proc. London Math. Soc. 12 (1962), 425–444.
[Kn] M. Kneser, Darstellungsmaße indefiniter quadratischer Formen, Math. Z. 77 (1961), 188–194.
[Ko] R. E. Kottwitz, Stable trace formula: elliptic singular terms, Math. Ann. 275 (1986), 365–399.
[La] S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.
[OM] O. T. O’Meara, Introduction to Quadratic Forms, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.
[Se] J.-P. Serre, Cohomologie galoisienne, Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin-Heidelberg-New York, 1965.
[Si] C. L. Siegel, Über die analytische Theorie der quadratischen Formen II, Ann. of Math. 37 (1936), 230–263.
[We] A. Weil, Adeles and Algebraic Groups, Birkhäuser, Boston, 1982.

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