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
Communicated by J. S. Hsia
Received March 28, 2000; published online July 23, 2001

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 $0 \leq c \leq \frac{1}{2}$. 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:

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

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 $X$.

1 Partially supported by the Hermann Minkowski Center for Geometry.
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 \( k = 1 \):

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

Set \( \Xi(X) = \prod_p \mu_p(X) \); this product converges absolutely (for \( n \geq 4 \)) and is called the singular series. Set

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

which is called the singular integral. For \( n \geq 4 \) the following asymptotic formula holds:

\[
N(T, X) \sim \Xi(X) \rho(T, X) \quad \text{as} \quad T \to \infty.
\]

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 \( \Xi(X) = \prod \mu_p(X) \) conditionally converges (see Sect. 1 below), but in general \( N(T, X) \) is not asymptotically \( \Xi(X) \rho(T, X) \). From results of [2] it follows that

\[
N(T, X) \sim c_X \Xi(X) \rho(T, X) \quad \text{as} \quad T \to \infty
\]

with \( 0 \leq c_X \leq 2 \), see details in Section 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 $\mathbb{Z}$, 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 $\mathcal{E}(X) \mu_w(T, X) \to \infty$ 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 $\mathbb{R}$ and over $\mathbb{Z}_p$ for every prime $p$, cf. e.g. [3].

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

$$N(T, X) \sim 2\mathcal{E}(X) \mu_w(T, X) \quad \text{as } T \to \infty.$$ 

Theorem 0.1 will be proved in Section 3.

**Example 0.1.** 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 $2\mathcal{E}(X) \mu_w(T, X) \sim 0.794 T$. 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, $q \in \mathbb{Z}$, $q \neq 0$, 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 $c_X = 1$:

$$N(T, X) \sim \mathcal{E}(X) \mu_w(T, X) \quad \text{as } T \to \infty.$$ 

Theorem 0.2 will be proved in Section 4.
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 $\mathcal{Z}(X)(\mu, T, X) \sim 0.7065T$. On the other hand, numeric calculations give for $T = 10,000$ the value $N(T, X) = 0.7048$.

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

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

Let $q \in \mathbb{Z}$, $q \neq 0$. Let $D = \text{det}(a_{ij})$. 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 adele ring of $\mathbb{Q}$. The group $G(A)$ acts on $X(A)$; let $\mathfrak{o}_A$ be an orbit. We would like to know whether $\mathfrak{o}_A$ has a $\mathbb{Q}$-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 $K = \mathbb{Q}(\sqrt{-qD})$, then $K$ is a quadratic extension of $\mathbb{Q}$, because $-qD$ is not a square. The torus $H$ is anisotropic over $\mathbb{Q}$ (because $-qD$ is not a square), and $H$ splits over $K$. Let $X_a(H_K)$ denote the cocharacter group of $H_K$. $X_a(H_K) = \text{Hom}(\mathbb{G}_m, H_K)$; then $X_a(H_K) \cong \mathbb{Z}$. The non-neutral element of $\text{Gal}(K/\mathbb{Q})$ acts on $X_a(H_K)$ by multiplication by $-1$. 

MIKHAIL BOROVOI

Let \( \mathcal{O}_A \) be an orbit of \( G(A) \) in \( X(A) \), \( \mathcal{O}_A = \prod \mathcal{O}_v \), where \( \mathcal{O}_v \) 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 \( v_\lambda(\mathcal{O}_v) = \pm 1 \). If \( \mathcal{O}_v = G(Q_v) \cdot x^0 \), then we set \( v_\lambda(\mathcal{O}_v) = +1 \), if not, we set \( v_\lambda(\mathcal{O}_v) = -1 \). Then \( v_\lambda(\mathcal{O}_v) = +1 \) for almost all \( v \). We define \( v(\mathcal{O}_A) = \prod v_\lambda(\mathcal{O}_v) \) where \( \mathcal{O}_v = \prod \mathcal{O}_v \). Note that the local invariants \( v_\lambda(\mathcal{O}_v) \) depend on the choice of the rational point \( x^0 \in X(Q) \); one can prove, however, that their product \( v(\mathcal{O}_A) \) does not depend on \( x^0 \).

Let \( x \in X(A) \). We set \( v(x) = v(G(A) \cdot x) \). Then \( v(x) \) 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 \( \delta(x) = v(x) + 1 \). In other words, if \( v(x) = -1 \) then \( \delta(x) = 0 \), and if \( v(x) = +1 \) then \( \delta(x) = 2 \). Then \( \delta \) is a locally constant function on \( X(A) \).

**Theorem 1.1.** An orbit \( \mathcal{O}_A \) of \( G(A) \) in \( X(A) \) has a \( Q \)-rational point if and only if \( v(\mathcal{O}_A) = +1 \).

Below we will deduce Theorem 1.1 from [2, Theorem 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

\[
C(T) = (X_T(T_k)_{\text{Gal}(\overline{k}/k)})_{\text{tor}}
\]

where \( k \) is a fixed algebraic closure of \( k \), \( X_T(T_k)_{\text{Gal}(\overline{k}/k)} \) denotes the group of coinvariants, and \( (\cdot)_{\text{tor}} \) 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 \( C_v(T) = C(T_v) \). There is a canonical map \( i_v : C_v(T) \to C(T) \) induced by an inclusion \( \text{Gal}(\overline{k}_v/k_v) \to \text{Gal}(\overline{k}/k) \). 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 \( Q \). Clearly

\[
C(H) = (X_H(T_\overline{Q})_{\text{Gal}(\overline{Q}/Q)})_{\text{tor}} = \mathbb{Z}/2\mathbb{Z}.
\]

We have \( C_v(H) = 1 \) if \( K \otimes \mathbb{Q}_v \) splits, and \( C_v(H) \simeq \mathbb{Z}/2\mathbb{Z} \) if \( K \otimes \mathbb{Q}_v \) 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 \( G(Q_v) \) in \( X(Q_v) \). The set of orbits of \( G(Q_v) \) in \( X(Q_v) \) is in canonical bijection with \( \ker \left[H^1(Q_v, H) \to H^1(Q_v, G)\right] \), cf. [13, 1-5.4, Corollary 1 of Proposition 36]. Hence \( \kappa_v \) defines a cohomology class \( \xi_v \in H^1(Q_v, G) \). The local Tate–Nakayama duality for tori defines a canonical homomorphism \( \beta_\xi : H^1(Q_v, H) \to C_v(H) \), see Kottwitz [10, Theorem 1.2]. (Kottwitz defines...
the map $\beta_\ast$ in a more general setting, when $H$ is any connected reductive group over a number field.) The homomorphism $\beta_\ast$ is an isomorphism for any $v$. We set $\kappa_\ast(\xi_0) = \beta_\ast(\xi_0)$. Note that if $\xi_0 = G(\mathbb{Q}_p) \cdot \mathbf{x}_0^\circ$, then $\xi_0 = 0$ and $\kappa_\ast(\xi_0) = 0$; if $\xi_0 \neq G(\mathbb{Q}_p) \cdot \mathbf{x}_0^\circ$, then $\xi_0 \neq 0$ and $\kappa_\ast(\xi_0) = 1$.

We define the Kottwitz invariant $\kappa(\ell_\Lambda)$ of an orbit $\ell_\Lambda = \prod \ell_\sigma$ of $G(\mathbb{A})$ in $X(\Lambda)$ by $\kappa(\ell_\Lambda) = \sum_\sigma i_\sigma(\kappa_\ast(\xi_0))$. We identify $C(H)$ with $\mathbb{Z}/2\mathbb{Z}$, and $C_\ast(H)$ with a subgroup of $\mathbb{Z}/2\mathbb{Z}$. With this identifications $\kappa(\ell_\Lambda) = \sum \kappa_\ast(\xi_0)$.

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

$$v_\ell(\xi_0) = (-1)^{\kappa(\ell_\Lambda)}, \quad v(\ell_\Lambda) = (-1)^{\kappa(\ell_\Lambda)}.$$  

Here $v_\ell(\xi_0)$ and $v(\ell_\Lambda)$ take the values $\pm 1$. We have $v(\ell_\Lambda) = \prod v(\xi_0)$. Since $\kappa_\ast(\xi_0) = 0$ if and only if $\xi_0 = G(\mathbb{Q}_p) \cdot \mathbf{x}_0^\circ$, we see that $v(\xi_0) = +1$ if and only if $\xi_0 = G(\mathbb{Q}_p) \cdot \mathbf{x}_0^\circ$. Hence our $v_\ell(\xi_0)$ and $v(\ell_\Lambda)$ coincide with $v_\ell(\xi_0)$ and $v(\ell_\Lambda)$, resp., introduced in Section 1.1.

By Theorem 3.6 of [2] an adelic orbit $\ell_\Lambda$ contains $\mathbb{Q}$-rational points if and only if $\kappa(\ell_\Lambda) = 0$. With our multiplicative notation $\kappa(\ell_\Lambda) = 0$ if and only if $v_\ell(\xi_0) = +1$. Thus $\ell_\Lambda$ contains $\mathbb{Q}$-points if and only if $v(\ell_\Lambda) = +1$.

We have deduced Theorem 1.1 from [2, Theorem 3.6].

1.3. Tamagawa Measure

We define a gauge form on $X$, i.e. a regular differential form $\omega \in A^2(X)$ without zeroes. Recall that $X$ is defined by the equation $f(x) = q$. Choose a differential form $\mu$ 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 $W = \mathbb{Q}^3$. Let $\omega = \mu|_X$, the restriction of $\mu$ to $X$. Then $\omega$ is a gauge form on $X$, cf. [2, 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. [2, 1.4], and a gauge form on $X$ is unique up to a scalar multiple, cf. [2, Corollary 1.5.4].

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

We have by [2, 1.8.1], $\mu_\omega(X) = m_\mu(X(\mathbb{Z}_p))$, where $\mu_\mu(X)$ is defined in the Introduction. By [14, Theorem 2.2.5], for almost all $p$ we have $m_\mu(X(\mathbb{Z}_p)) = \#X(\mathbb{F}_p)$.

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

$$\#\text{SO}(f)(\mathbb{F}_p) = p(p^2 - 1), \quad \#\text{SO}(f')(\mathbb{F}_p) = p - \varphi(p),$$
where \( \chi(p) = -1 \) if \( f^* \mod p \) does not represent 0, and \( \chi(p) = +1 \) if \( f^* \mod p \) represents 0. We have \( \chi(p) = \left( \frac{-D}{p} \right) \). We obtain for \( p \mid qD \)

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

For \( p \mid qD \) 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 \( (\lambda_p) \)

is a family of convergence factors in the sense of [14, 2.3]. We define, as

in [2, 1.6.2], the measures

\[
m_f = m \lambda_p^{-1} m_p, \quad m = m_{\infty} m_f,
\]

then \( m_f \) is a measure on \( X(A_f) \) (where \( A_f \) is the ring of finite adeles) and

\( m \) is a measure on \( X(A) \). We call \( m \) the Tamagawa measure on \( X(A) \).

### 1.4. Counting Integer Points

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

**Theorem 1.2.**

\[
N(T, X) \sim \int_{X(R)^T \times X(Z)} \delta(x) \ dm.
\]

In other words,

\[
N(T, X) \sim 2m( \{ x \in X(R)^T \times X(\hat{Z}) : v(x) = +1 \} ). \tag{1}
\]

Theorem 1.2 follows from [2, Theorem 5.3] (cf. [2, 6.4] and [2, Definition 2.3]).

For comparison note that

\[
m(X(R)^T \times X(\hat{Z})) = m_{\infty}(X(R)^T) m_f(X(\hat{Z})) = \mu_{\infty}(T, X) \mathcal{E}(X), \tag{2}
\]

cf. [2, 1.8].

The following lemma will be used in the proof of Theorem 0.1.
Lemma 1.3. Assume that there exists \( y \in X(\mathbb{R} \times \hat{Z}) \) such that \( \nu(y) = +1 \). Then the set \( X(\mathbb{Z}) \) is infinite.

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

\[
\int_{X(\mathbb{R} \times \hat{Z})} \delta(x) \, dm \geq \int_{\mathcal{U}_f^T \times \mathcal{U}_f} \delta(x) \, dm = 2m_u(\mathcal{U}_f^T) \mu_f(\mathcal{U}_f).
\]

Since \( 2m_u(\mathcal{U}_f^T) \mu_f(\mathcal{U}_f) \to \infty \) as \( T \to \infty \), we see that

\[
\int_{X(\mathbb{R} \times \hat{Z})} \delta(x) \, dm \to \infty \quad \text{as} \quad T \to \infty,
\]

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

1.5. The Constant \( c_X \)

Here we prove the following result:

Proposition 1.4.

\[
N(T, X) \sim c_X \Xi(X) \mu_u(T, X) \quad \text{as} \quad T \to \infty
\]

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

Proof. If \( X(R) \) has two connected components, then by Theorem 0.2 (which we will prove in Section 4 below), \( N(T, X) \sim \Xi(X) \mu_u(T, X) \), so the proposition holds with \( c_X = 1 \).

If \( X(R) \) has one connected component, then \( X(R) \) consists of one \( G(R) \)-orbit and \( \nu_v(\pi_1(R)) = +1 \). For an orbit \( \psi_f = \prod \psi_{f_j} \) of \( G(A_f) \) in \( X(A_f) \) we set \( \nu_f(\psi_f) = \prod \nu_{f_j}(\psi_{f_j}) \). We regard \( \nu_f \) as a locally constant function on \( X(A_f) \) taking the values \( \pm 1 \). Define \( \hat{X}(\hat{Z}) = \{ x_f \in X(\hat{Z}) : \nu_f(x_f) = +1 \} \).

We have

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

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

\[
\int_{X(\mathbb{R} \times \hat{Z})} \delta(x) \, dm = c_X m_u(X(R)^T) m_f(X(\hat{Z})) = c_X \mu_u(T, X) \Xi(X).
\]
Using Theorem 1.2, we see that
\[ N(T, X) \sim c_x \mu_{\omega}(T, X) \Xi(X) \quad \text{as} \quad T \to \infty. \]

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 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 \( \mathbb{R} \) and over \( \mathbb{Z}_p \) for \( p > 2 \).

We have \( f_1(4, 1, 1) = -127 \equiv 1 \mod 2^7 \). We prove that \( f_1 \) represents 1 over \( \mathbb{Z}_2 \). Define a polynomial of one variable \( F(Y) = f_1(4, 1, Y) - 1 \), \( F \in \mathbb{Z}_2[Y] \). 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. [11, II-§2, Proposition 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
\[ -9x_1^2 + 2x_1x_2 + 7x_2^2 + 2x_3^2 = 1 \quad \text{for some} \quad x_1, x_2, x_3 \in \mathbb{Z}. \]

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 \((x_1 - x_2)^2 \equiv 1 \mod 8\). Hence the right hand side is congruent to 1 \mod 8. We see that \( x_3 \) is odd, hence \( 2x_3^2 - 1 \equiv 1 \mod 16 \). But
\[ 8(x_1 - x_2)(x_1 + x_2) \equiv 8 \mod 16. \]

It follows that
\[ (x_1 - x_2)^2 \equiv 9 \mod 16 \]
\[ x_1 - x_2 \equiv \pm 3 \mod 8. \]
Therefore $x_1 - x_2$ must have a prime factor $p \equiv \pm 3 \pmod{8}$. Hence $2x_1^2 - 1$ has a prime factor $p \equiv \pm 3 \pmod{8}$. On the other hand, if $p \mid (2x_1^2 - 1)$, then

$$2x_1^2 \equiv 1 \pmod{p}$$

and 2 is a square modulo $p$, $(\frac{2}{p}) = 1$. 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,

$$\Xi(X) \mu_{\omega}(T, X) = m_f(X(\mathbb{Z})) m_{\omega}(X(\mathbb{R})).$$

Since $X(\mathbb{Z})$ is a nonempty open subset in $X(\mathbb{A})$, $m_f(X(\mathbb{Z})) > 0$. Now $m_{\omega}(X(\mathbb{R})) \to \infty$ as $T \to \infty$. Hence $\Xi(X) \mu_{\omega}(T, X) \to \infty$ 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 $u \in \text{GL}(V(k))$, $f' = uf$. 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

$$s = r_{g_1} \cdots r_{g_i}$$

(3)

cf. [12, Theorem 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 $\text{Spin}(f)(k)$ 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. [13, III-3.2] or [3, Chap. 10, Theorem 3.3].
Now let \( u, f' \) be as above. Then \( r_{f', u} = u r_{f, u} u^{-1}, f'(ux) = f(x), \) and so \( \theta_{f'}(ux) = \theta_{f}(x) \). We conclude that \( u \theta(f) u^{-1} = \theta(f') \) \( x \) 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 \( \mathbb{Z}^n \) 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 \( f'(x) = f(ux) \) 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 \( X(\mathbb{R} \times \mathbb{Z}) \) to \( X'(\mathbb{R} \times \mathbb{Z}) \) 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

\[
(u^{-1})' A u^{-1} = A', \quad A = u'A'u.
\]

The variety \( X \) is defined by the equation \( x'Ax = q \), and \( X' \) is defined by \( x'A'x = q \). One easily checks that the map \( x \mapsto ux \) takes \( X(\mathbb{R} \times \mathbb{Z}) \) to \( X'(\mathbb{R} \times \mathbb{Z}) \) 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 \( x \mapsto u_x x : X(\mathbb{Q}_r) \to X'(\mathbb{Q}_r) \) takes the orbits of \( \text{Spin}(f)(\mathbb{Q}_r) \) to the orbits of \( \text{Spin}(f')(\mathbb{Q}_r) \) for every \( r \), where \( u_x \) is the \( r \)-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 \( X'(\mathbb{R} \times \mathbb{Z}) \) 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 \( v \) the set \( X'(\mathbb{Z}_v) \) has nontrivial intersection with two orbits of \( G'(\mathbb{Q}_v) \). Then \( v \) takes both values \( +1 \) and \( -1 \) on \( X'(\mathbb{Z}_v) \). It follows that \( v \) takes both values \( +1 \) and \( -1 \) on \( X'(\mathbb{R} \times \mathbb{Z}) \). Hence by Lemma 1.3 \( X' \) 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 \( u \in \text{GL}_n(\mathbb{R} \times \mathbb{Z}) \) be such that \( f'(x) = f(ux^{-1}) \). Let \( X, X' \) be as above, in particular \( X' \) has no \( \mathbb{Z} \)-points. By Proposition 3.3 \( X'(\mathbb{R} \times \mathbb{Z}) \) is contained in one orbit of \( \text{Spin}(f')(\mathbb{A}) \). It follows from Lemma 3.2 that \( X(\mathbb{R} \times \mathbb{Z}) \) 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
\(X/R\times\mathbb{Z}\). Thus \(\delta\) equals 2 on \(X/R\times\mathbb{Z}\), and by Formulas (1) and (2) of Section 1.4 \(N(T, X) \sim 2\Xi(X) \mu_{x_0}(T, X)\).

4. PROOF OF THEOREM 0.2

We prove Theorem 0.2. We define an involution \(\tau_{x_0}\) of \(X(R)\) by \(\tau_{x_0}(x) = -x, \ x \in X(R) \in \mathbb{R}^3\). Since \(f(x) = f(-x)\), \(\tau_{x_0}\) is well defined, i.e. takes \(X(R)\) to itself. Since \(\|x\| = |x|\), \(\tau_{x_0}\) takes \(X(R)^T\) to itself. We define an involution \(\tau_{x_0}\) of \(X(A)\) by defining \(\tau_{x_0}\) on \(X(R)\) and as 1 on \(X(Q_p)\) for all prime \(p\). Then \(\tau\) respects the Tamagawa measure \(m\) on \(X(A)\).

By assumption \(X(R)\) has two connected components. These are the two orbits of \(\text{Spin}(f)(R)\). The involution \(\tau_{x_0}\) of \(X(R)\) interchanges these two orbits. Thus we have

\[v_{x_0}(\tau_{x_0}(x_{x_0})) = -v_{x_0}(x_{x_0}) \quad \text{for all} \quad x_{x_0} \in X(R) \quad (4)\]

\[v(\tau(x)) = -v(x) \quad \text{for all} \quad x \in X(A). \quad (5)\]

Let \(X(R)_1\) and \(X(R)_2\) be the two connected components of \(X(R)\). Set \(X(R)_1^T = X(R)_1 \cap X(R)^T, \quad X(R)_2^T = X(R)_2 \cap X(R)^T\)

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

\[\int_{X(R)_1^T} v(x) \, dm = -\int_{X(R)_2^T} v(x) \, dm,\]

hence

\[\int_{X(R)^T \times X(\hat{Z})} v(x) \, dm = 0.\]

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

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

and \(m(X(R)^T \times X(\hat{Z})) = \Xi(X) \mu_{x_0}(T, X)\). By Theorem 1.2

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

Thus \(N(T, X) \sim \Xi(X) \mu_{x_0}(T, X)\) as \(T \to \infty\), i.e. \(\epsilon_x = 1\).
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 Zeev Rudnick for useful discussions and help in analytic calculations.

REFERENCES