ACTA ARITHMETICA
166.1 (2014)

Uniformly counting rational points on conics

by

Efthymios Sofos (Bristol)

1. Introduction. Let $Q(\mathbf{x}) \in \mathbb{Z}[x_1, x_2, x_3]$ be a non-singular quadratic form. We denote by $\mathbb{Z}^3_{\text{prim}}$ the integer vectors $\mathbf{x}$ that are primitive, i.e. $\gcd(\mathbf{x}) = 1$. Our main concern in this paper is the number of primitive integer zeros of Q contained in an expanding region of $\mathbb{R}^3$. It is therefore only the case that Q is isotropic that we are interested in, and we will proceed under this assumption for the rest of the paper.

For an arbitrary norm $\|\cdot\| : \mathbb{R}^3 \to \mathbb{R}_{\geq 0}$ define the counting function

$$N(Q, B) := \#\{\mathbf{x} \in \mathbb{Z}^3_{\text{prim}} : Q(\mathbf{x}) = 0, \|\mathbf{x}\| \leq B\}.$$

A very special case of [7] establishes the asymptotic formula

$$N(Q, B) \sim c_Q B$$

as $B \to \infty$. This confirms the Manin conjecture; furthermore $c_Q = c_Q(\|\cdot\|)$ is a positive constant which was later interpreted by Peyre [10].

Let $\langle Q \rangle$ denote the maximum modulus of the coefficients of Q. As pointed out in [2], one expects the existence of absolute constants $\beta, \gamma > 0$ such that

$$N(Q, B) = c_Q B + O(B^{1-\gamma} \langle Q \rangle^{\beta}).$$

Our aim is to establish such an estimate and furthermore to state explicitly admissible values for β and γ.

We begin by recalling some related results. Let $w : \mathbb{R}^3 \to \mathbb{R}_{\geq 0}$ be a smooth weight function of compact support and let

$$N_w(Q, B) := \sum_{\substack{\mathbf{x} \in \mathbb{Z}^3_{\text{prim}} \\ Q(\mathbf{x}) = 0}} w(B^{-1}\mathbf{x}).$$

It is proved in [8, Cor. 2] that there exists a positive constant c_1 such that

$$N_w(Q, B) = c_{Q,w} B + O_{Q,w}(B \exp\{-c_1 \sqrt{\log B}\})$$

as $B \to \infty$. The proof is carried out via a modification of the circle method.

2010 *Mathematics Subject Classification*: Primary 11D45; Secondary 14G05.
Key words and phrases: rational points, quadratic forms.

DOI: 10.4064/aa166-1-1

Let Δ_Q and δ_Q be respectively the discriminant and the greatest common divisor of the 2×2 minors of the matrix of the form Q. In [1, Cor. 2], it is proved that

$$N(Q,B) \ll \tau(|\Delta_Q|)\bigg(1+\frac{B\delta_Q^{1/2}}{|\Delta_Q|^{1/3}}\bigg),$$

where τ denotes the divisor function. It should be stressed that the implied constant is absolute.

We provide the definition of the leading constant c_Q before stating our main result. We define the Hardy–Littlewood local densities following [8]. Let

$$\sigma_\infty := \sigma_\infty(Q,\|\cdot\|) = \lim_{\epsilon\to 0}\frac{1}{2\epsilon}\int\limits_{\substack{|Q(\mathbf{x})|\le\epsilon\\ \|\mathbf{x}\|\le 1}} 1\,d\mathbf{x}, \tag{1.1}$$

and similarly for any prime p, let

$$\sigma_p := \sigma_p(Q) = \lim_{n\to\infty}\frac{1}{p^{2n}}N_Q^*(p^n), \tag{1.2}$$

where for any positive integer n,

$$N_Q^*(p^n) := \#\{\mathbf{x} \pmod{p^n} : p\nmid \mathbf{x},\, Q(\mathbf{x})\equiv 0 \pmod{p^n}\}.$$

The Peyre constant is then defined as

$$c_Q = \frac{1}{2}\sigma_\infty\prod_p \sigma_p$$

where the product is taken over the set of primes and is convergent. Let $C\subseteq\mathbb{P}^2$ be the smooth projective curve defined by Q. The factor $\alpha(C)=\frac{1}{2}$ is due to the fact that the anticanonical line bundle is twice the generator of the Picard group $\mathrm{Pic}(C)\cong\mathbb{Z}$, where $\alpha(C)$ is the volume of a certain polytope contained in the cone of effective divisors.

As usual, we denote by $\|\cdot\|$ and $\|\cdot\|_2$ the maximum and the Euclidean norm on $\mathbb{R}^3$ respectively. Next, for any norm $\|\cdot\|:\mathbb{R}^3\to\mathbb{R}_{\ge 0}$, let

$$K_{\|\cdot\|} := 1+\sup_{\mathbf{x}\neq\mathbf{0}}\frac{\|\mathbf{x}\|_\infty}{\|\mathbf{x}\|}, \tag{1.3}$$

and notice that $K_{\|\cdot\|}$ is a constant depending only on the choice of $\|\cdot\|$.

Finally, let us recall that two norms $\|\cdot\|,\|\cdot\|':\mathbb{R}^3\to\mathbb{R}_{\ge 0}$ are called *isometric* when there exists a matrix $\mathfrak{g}\in\mathrm{GL}_3(\mathbb{R})$ such that $\|\mathfrak{g}\mathbf{x}\|=\|\mathbf{x}\|'$ for all $\mathbf{x}\in\mathbb{R}^3$.

We have the following result.

Main Theorem 1.1. *Let Q be a ternary non-singular integer quadratic form with a rational zero and $\|\cdot\|$ be any norm isometric to the maximum or the Euclidean norm. Then*

$$N(Q,B) = c_Q B + O\big((BK_{\|\cdot\|})^{1/2}\log(BK_{\|\cdot\|})\langle Q\rangle^5\big)$$

for $B \geq 2$. The implied constant is absolute.

The proof of Theorem 1.1 reveals that for any $\epsilon > 0$, at the expense of an implied constant that depends on ϵ, one can replace $\langle Q\rangle^5$ in the error term by $\langle Q\rangle^{19/20+\epsilon}$ as well as by $\langle Q\rangle^{4+\epsilon}\delta_Q^{1/2}$ (see (6.2)). Further improvements may follow using [9, Theorem 1]. We hope it will be apparent to the reader that the main value of Theorem 1.1 lies in its generality rather than the exponent of $\langle Q\rangle$ obtained.

The proof is conducted in two stages. Firstly, in §2–§5, we prove Theorem 1.1 for conics of a special shape, using the fact that since $C(\mathbb{Q}) \neq \emptyset$, there is a morphism $\mathbb{P}^1 \to C$. The conditions involving the resulting parametrising functions lead to a lattice counting problem. We stress that the choice of the parametrising functions is not unique, and choosing them appropriately plays a significant rôle. Some related work has been done in [4] and [11]. The second stage is performed in §6. Here we apply a unimodular transformation to a conic of general shape to transform the problem into the one we have already treated.

Notation. The implied constants in the $O(\cdot)$ notation will be absolute throughout this paper, except where specifically indicated by a subscript. The norm notation $\|\cdot\|$ will be reserved for norms of elements of $\mathbb{R}^3$ while $\|\cdot\|_\infty$ will be used for the matrix supremum norm in $\mathbb{R}^{3\times 3}$, defined by $\|(a_{i,j})_{1\leq i,j\leq 3}\|_\infty := \max_{1\leq i,j\leq 3}|a_{i,j}|$, as well as the supremum norm in $\mathbb{R}^3$. We denote the generalised divisor function by $\tau_k(n)$, which is defined to be the number of representations of n as the product of k natural numbers. The well-known bound $\tau_k(n) \ll_{k,\epsilon} n^\epsilon$, valid for each $\epsilon > 0$, will be used. By $\sum^*_{(s,t)\,(\mathrm{mod}\,n)}$, we shall denote summation over $s,t \in [1,n]$ subject to the condition $\gcd(s,t,n) = 1$.

2. Preliminary estimates. Throughout §2–§5, we denote by Q quadratic forms of which $(0,1,0)$ is a zero, i.e.

$$Q(\mathbf{x}) = ax^2 + bxy + dxz + eyz + fz^2,$$

where $a,\dots,f \in \mathbb{Z}$. We will denote by Δ_Q its discriminant,

$$\Delta_Q = ae^2 - deb + fb^2.$$

It is our intention in the aforementioned sections to prove the following special version of Theorem 1.1. Its proof hinges upon the classical parametrisation of a conic by the lines going through a given point.

Proposition 2.1. *Let Q be a non-singular integer ternary quadratic form as above. Then for any norm isometric to the maximum or the Euclidean norm and for any $\epsilon > 0$,*

$$N(Q,B) = c_Q B + O_\epsilon\big((BK_{\|\cdot\|})^{1/2}\log(BK_{\|\cdot\|})\min\{|\Delta_Q|^{1/4}, \delta_Q^{1/2}\}(|\Delta_Q|+\langle Q\rangle)\langle Q\rangle^\epsilon\big)$$

for $B \geq 2$.

Let

$$\Pi := \begin{pmatrix} b & e & 0 \\ -a & -d & -f \\ 0 & b & e \end{pmatrix}$$

and define the three binary quadratic forms q_1, q_2, q_3 via

$$\mathbf{q}(s,t) = \Pi \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix} \tag{2.1}$$

where $\mathbf{q} = (q_1, q_2, q_3)^T$. One can verify that $\det(\Pi) = \Delta_Q$, in particular the matrix Π is invertible. Hence

$$\mathrm{adj}(\Pi)\mathbf{q}(s,t) = \Delta_Q \begin{pmatrix} s^2 \\ st \\ t^2 \end{pmatrix}. \tag{2.2}$$

Notice that for

$$\begin{aligned} g(s,t) &:= as^2 + dst + ft^2, \\ L(s,t) &:= bs + et, \end{aligned} \tag{2.3}$$

one has

$$\begin{aligned} q_1(s,t) &= sL(s,t), \\ q_2(s,t) &= -g(s,t), \\ q_3(s,t) &= tL(s,t). \end{aligned} \tag{2.4}$$

For each integer n, let

$$\rho^*(n) := \#\{(s,t) \in [0,n)^2 : n \,|\, \mathbf{q}(s,t),\ \gcd(s,t,n) = 1\}, \tag{2.5}$$

and note that ρ^* is a multiplicative function. Equations (2.4) imply that

$$\rho^*(n) = \#\{(s,t) \in [0,n)^2 : n \,|\, (L(s,t), g(s,t)),\ \gcd(s,t,n) = 1\}.$$

Lemma 2.2.

(i) *The function ρ^* is supported on the divisors of $\Delta_Q/\gcd(b,e)$.*

(ii) *For all integers n we have*

$$\rho^*(n) \leq n\gcd(b,e).$$

Proof. (i) It suffices to show that for each prime p and integer $\nu \geq 1$ with $\rho^*(p^\nu) \neq 0$ we have

$$\nu + \min\{v_p(b), v_p(e)\} \leq v_p(\Delta_Q).$$

Let (s,t) be counted by $\rho^*(p^\nu)$. We may assume without loss of generality that $v_p(b) \leq v_p(e)$. Since $\gcd(b,e)^2 \mid \Delta_Q$, in the case $\nu \leq v_p(b)$ our claim is trivial. If $\nu > v_p(b)$ then we may write $b = p^{v_p(b)}b'$, $e = p^{v_p(e)}e'$ with $p \nmid b'e'$. Plugging these values into the congruence $L(s,t) \equiv 0 \pmod{p^\nu}$ yields

$$b's \equiv -p^{v_p(e)-v_p(b)}e't \pmod{p^{\nu-v_p(b)}} \tag{2.6}$$

and hence $p \nmid t$, since otherwise we would have $p \mid (s,t)$, which would contradict the definition of $\rho^*(p^n)$. We deduce that

$$t^2(ae^2p^{-2v_p(b)} - deb'p^{-v_p(b)} + fb'^2) \equiv b'^2 g(s,t) \equiv 0 \pmod{p^{\nu-v_p(b)}}$$

and therefore $p^{\nu+v_p(b)} \mid ae^2 - deb + fb^2 = \Delta_Q$, which concludes the proof of the first part.

(ii) It suffices to prove that for all primes p and integers $\nu \geq 1$ we have

$$\rho^*(p^\nu)/p^\nu \leq p^{\min\{v_p(b),v_p(e)\}}. \tag{2.7}$$

Let (s,t) be counted by $\rho^*(p^\nu)$. As previously, we may assume $v_p(b) \leq v_p(e)$. If $\nu \leq v_p(b)$, then (2.7) is a consequence of the trivial bound $\rho^*(p^\nu) \leq p^{2\nu}$. In the opposite case we proceed as in the proof of (i). Then (2.6) shows that $s/t \pmod{p^{\nu-v_p(b)}}$ is uniquely determined and can be lifted to at most $p^{v_p(b)}$ values modulo p^ν, which proves (2.7) in all cases. ∎

We record a generalisation of Möbius inversion that will be used later.

LEMMA 2.3. *Let $\mathcal{A}$ be a finite subset of $\mathbb{Z}^2$ and n a fixed integer. Then*

$$\#\{(s,t) \in \mathcal{A} : \gcd(s,t) = 1\} = \sum_{\substack{m=1 \\ \gcd(m,n)=1}}^{\infty} \mu(m) \#\left\{(s,t) \in \mathcal{A} : \begin{array}{l} \gcd(s,t,n) = 1, \\ m \mid s,\ m \mid t \end{array}\right\}.$$

Proof. Define $\mathbb{1}_{\mathcal{A}} : \mathbb{Z}^2 \to \{0,1\}$ to be the indicator function of $\mathcal{A}$. Möbius inversion gives

$$\sum_{\substack{\gcd(s,t,n)=1 \\ \gcd(s,t)=1}} \mathbb{1}_{\mathcal{A}}(s,t) = \sum_{m=1}^{\infty} \mu(m) \sum_{\substack{\gcd(s,t,n)=1 \\ m \mid s,\, m \mid t}} \mathbb{1}_{\mathcal{A}}(s,t).$$

Our assertion is proved upon noticing that only m coprime to n are taken into account in the summation. ∎

3. Parametrisation of the conic. In this section, we begin by showing how the problem of counting points on conics can be rephrased using the parametrisation functions $\mathbf{q}(s,t)$. This will lead us to count primitive integer points in regions of $\mathbb{R}^2$.

Let

$$\mathcal{N}(Q,B) := \#\{(s,t) \in \mathbb{Z}^2_{\text{prim}} : t > 0,\ \|\mathbf{q}(s,t)\| \le \lambda B\}, \tag{3.1}$$

where $\lambda = \gcd(\mathbf{q}(s,t)) \in \mathbb{Z}$.

LEMMA 3.1. *$N(Q,B) = \mathcal{N}(Q,B) + O(1)$, where the implied constant is absolute.*

Proof. Let $C \subset \mathbb{P}^2$ be the curve given by $Q = 0$ and denote the point $(0,1,0)$ of C by ξ. The tangent line to C through ξ is given by

$$L_\xi := \{ez = bx\}.$$

Let $\mathcal{L}$ be the set of projective lines in $\mathbb{P}^2$ that pass through ξ, and $\mathcal{L}(\mathbb{Q})$ be the corresponding subset of lines that are defined over $\mathbb{Q}$. Define $U \subset C$ as the open subset formed by deleting ξ from C. Letting $\mathcal{U} := \mathcal{L} \setminus \{L_\xi\}$, we note that the sets $U(\mathbb{Q})$ and $\mathcal{U}(\mathbb{Q})$ are in bijection.

The general element of $\mathcal{L}(\mathbb{Q})$ is given by

$$L_{s,t} := \{sz = tx\}$$

for integer pairs (s,t) such that $\gcd(s,t) = 1$. The condition $(s,t) \neq \frac{(b,e)}{\gcd(b,e)}$ ensures that we have a point in $\mathcal{U}(\mathbb{Q})$. One can ignore this, since the contribution of such s,t is $O(1)$. The bijection between lines with $t > 0$ and $t < 0$ allows us to consider the contribution coming from the former. The contribution of pairs (s,t) with $t = 0$ is $O(1)$ due to the condition $\gcd(s,t) = 1$.

The bijection between $U(\mathbb{Q})$ and $\mathcal{U}(\mathbb{Q})$ can be made explicit as follows. Recall the definition of L, g in (2.3). A computation reveals that the line $L_{s,t}$ intersects C in the point (x,y,z) if and only if either $zg(s,t) + ytL(s,t) = 0$ or $z = 0$. In the latter case, one gets the point ξ, which is to be ignored. In the former case, we have

$$-g(s,t)xt = -g(s,t)sz = syL(s,t)t,$$

by the equation for $L_{s,t}$. The primitive integer vectors (x,y,z) represent a point in $C(\mathbb{Q})$ if and only if

$$(x,y,z) = \pm\big(sL(s,t)/\lambda, -g(s,t)/\lambda, tL(s,t)/\lambda\big),$$

where $\lambda = \gcd(sL(s,t), -g(s,t), tL(s,t))$. Making use of (2.4) concludes the proof of the lemma. ∎

For any $T \in \mathbb{R}_{\geq 1}$ and $n, \sigma, \tau \in \mathbb{N}$, define

$$M^*_{\sigma,\tau}(T,n) := \#\left\{(s,t) \in \mathbb{Z}^2_{\text{prim}} : \begin{array}{l} (s,t) \equiv (\sigma,\tau) \pmod{n}, \\ t > 0,\ \|\mathbf{q}(s,t)\| \leq T \end{array}\right\}. \tag{3.2}$$

Lemma 3.2.

$$\mathcal{N}(Q,B) = \sum_{k\lambda \mid \Delta_Q/\gcd(b,e)} \mu(k) \sideset{}{^*}\sum_{\substack{(\sigma,\tau) \pmod{k\lambda} \\ k\lambda \mid (L(\sigma,\tau), g(\sigma,\tau))}} M^*_{\sigma,\tau}(B\lambda, k\lambda).$$

Proof. Any integer λ that appears in (3.1) satisfies $\lambda \,|\, \mathbf{q}(s,t)$ for some coprime integers s,t, so Lemma 2.2(i) implies that $\lambda \,|\, \frac{\Delta_Q}{\gcd(b,e)}$. Therefore

$$\mathcal{N}(Q,B) = \sum_{\lambda \mid \Delta_Q/\gcd(b,e)} \#\left\{(s,t) \in \mathbb{Z}^2_{\text{prim}} : \begin{array}{l} \lambda \,|\, \mathbf{q}(s,t),\ \gcd(\mathbf{q}(s,t)/\lambda) = 1, \\ t > 0,\ \|\mathbf{q}(s,t)\| \leq B\lambda \end{array}\right\}.$$

Using Lemma 2.3 with $n = 1$ gives

$$\mathcal{N}(Q,B) = \sum_{k\lambda \mid \Delta_Q/\gcd(b,e)} \mu(k) M^*(B\lambda, k\lambda), \tag{3.3}$$

where for any $T \geq 1$ and $n \in \mathbb{N}$,

$$M^*(T,n) := \#\left\{(s,t) \in \mathbb{Z}^2_{\text{prim}} : \begin{array}{l} n \,|\, \mathbf{q}(s,t),\ t > 0, \\ \|\mathbf{q}(s,t)\| \leq T \end{array}\right\}.$$

Partitioning into congruence classes modulo n yields

$$M^*(T,n) = \sideset{}{^*}\sum_{\substack{(\sigma,\tau) \pmod{n} \\ n \mid (L(\sigma,\tau), g(\sigma,\tau))}} M^*_{\sigma,\tau}(T,n),$$

which, when used along with (3.3), yields the proof of the lemma. ∎

4. Counting lattice points. The quantity appearing in (3.2) involves integer points (s,t) which are primitive. We will use Möbius inversion to deal with this condition. This will lead us to count integer points in a dilated region. In order to do so, one needs certain information regarding this region, which is the purpose of the next lemma.

Recall the definition (2.1). Define

$$V := \{(s,t) \in \mathbb{R}^2 : t > 0,\ \|\mathbf{q}(s,t)\| \leq 1\}. \tag{4.1}$$

Lemma 4.1. *The region V is bounded, and in particular contained in the rectangle given by*

$$|s|, |t| \ll \langle Q \rangle (K_{\|\cdot\|}/|\Delta_Q|)^{1/2}.$$

The length of the boundary of V, denoted by $|\partial V|$, satisfies

$$|\partial V| \ll \langle Q \rangle (K_{\|\cdot\|}/|\Delta_Q|)^{1/2},$$

where the implied constant is absolute. Furthermore, any line parallel to one of the two coordinate axes intersects V in a set of points which, if not empty, consists of at most $O(1)$ intervals, where the implied constant is absolute.

Proof. For each $(s,t) \in V$, from (2.2) one gets

$$|s|^2, |t|^2 \ll K_{\|\cdot\|} \|\mathrm{adj}(\Pi)\|_\infty |\Delta_Q|^{-1}.$$

Using the estimates $\|\mathrm{adj}(\Pi)\|_\infty \ll \|\Pi\|^2 \ll \langle Q \rangle^2$ concludes the proof of the first assertion. The assumption that the norm $\|\cdot\|$ is isometric to the maximum or the Euclidean norm implies that V is a finite union of at most $O(1)$ convex sets. Therefore $|\partial V|$ is bounded by an absolute constant multiplied by the length of the box that contains V. Our last assertion is a consequence of [6] as the set V is semi-algebraic, owing to the fact that $\|\cdot\|$ is isometric to the supremum or the Euclidean norm. ∎

For any $T \in \mathbb{R}_{\geq 1}$ and $n, \sigma, \tau \in \mathbb{N}$ such that $\gcd(\sigma, \tau, n) = 1$, define

$$M_{\sigma,\tau}(T,n) := \#\left\{ (s,t) \in \mathbb{Z}^2 : \begin{array}{l} (s,t) \equiv (\sigma,\tau) \pmod n, \\ t > 0,\ \|\mathbf{q}(s,t)\| \leq T \end{array} \right\}. \tag{4.2}$$

Lemma 4.2. *For any T, n, σ, τ as above with $\gcd(\sigma, \tau, n) = 1$ and $n \,|\, \mathbf{q}(\sigma, \tau)$, one has*

$$M^*_{\sigma,\tau}(T,n) = \sum_{\substack{1 \leq m \leq (2TK_{\|\cdot\|}/n)^{1/2} \\ \gcd(m,n)=1}} \mu(m) M_{\bar{m}\sigma,\bar{m}\tau}(T/m^2, n),$$

where $\bar{m}$ denotes the inverse of m modulo n.

Proof. The condition $\|\mathbf{q}(s,t)\| \leq T$ implies, by Lemma 4.1, that the number of (s,t) counted by $M^*_{\sigma,\tau}(T,n)$ is finite. Therefore Lemma 2.3 may be applied to yield

$$M^*_{\sigma,\tau}(T,n) = \sum_{\substack{m=1 \\ \gcd(m,n)=1}}^{\infty} \mu(m) M_{\bar{m}\sigma,\bar{m}\tau}\left(\frac{T}{m^2}, n\right). \tag{4.3}$$

If we have $m > (2K_{\|\cdot\|}T/n)^{1/2}$, then each (s,t) taken into account by $M_{\bar{m}\sigma,\bar{m}\tau}(T/m^2, n)$, satisfies $\|\mathbf{q}(s,t)\|_\infty < n/2$, due to (1.3). The assumptions on σ, τ, n imply that $n \,|\, \mathbf{q}(s,t)$, which is only possible if $\mathbf{q}(s,t) = \mathbf{0}$. Due to (2.2), one has $t = 0$, which contradicts the definition of (4.2). This shows that only integers $m \leq (2K_{\|\cdot\|}T/n)^{1/2}$ make a non-zero contribution to (4.3), which concludes the proof. ∎

Recall the definitions (4.1) and (4.2).

LEMMA 4.3. *For any T, n, σ, τ as above, we have*

$$M_{\sigma,\tau}(T,n) = \mathrm{vol}(V)\frac{T}{n^2} + O\bigg(1 + \frac{(K_{\|\cdot\|}T)^{1/2}}{n}\,\frac{\langle Q\rangle}{|\Delta_Q|^{1/2}}\bigg).$$

Proof. The quantity $M_{\sigma,\tau}(T,n)$ equals the number of integer points in the region

$$\frac{T^{1/2}}{n}V - \bigg(\frac{\sigma}{n},\frac{\tau}{n}\bigg),$$

where V is defined in (4.1). We thus deduce that

$$M_{\sigma,\tau}(T,n) = \sharp\bigg\{\mathbb{Z}^2 \cap V\frac{T^{1/2}}{n}\bigg\} + O\bigg(1 + |\partial V|\frac{T^{1/2}}{n}\bigg),$$

where $|\partial V|$ denotes the length of the boundary of V. The assumptions of the theorem in [5, p. 180] are fulfilled due to Lemma 4.1, thus yielding

$$\sharp\bigg\{\mathbb{Z}^2 \cap V\frac{T^{1/2}}{n}\bigg\} = \mathrm{vol}(V)\frac{T}{n^2} + O\bigg(1 + \frac{(K_{\|\cdot\|}T)^{1/2}}{n}\,\frac{\langle Q\rangle}{|\Delta_Q|^{1/2}}\bigg).$$

This estimate, when combined with the second assertion of Lemma 4.1, finishes the proof. ∎

5. The asymptotic formula. We are now in possession of the required lemmata to show the validity of Proposition 2.1. Before proceeding to the proof we should remark that we shall show the asymptotic formula of Proposition 2.1 with a different constant in place of c_Q, and at the end of this section we will explain why the two constants coincide.

Let us now define the new constant, which we denote by c'_Q. Recall the definitions (2.5) and (4.1). Let

$$\sigma'_\infty := \mathrm{vol}(V)$$

and for any prime p, let

$$\sigma'_p := \bigg(1 - \frac{1}{p^2}\bigg)\bigg(1 + \frac{1}{1+1/p}\sum_{d\geq 1}\frac{\rho^*(p^d)}{p^d}\bigg).$$

Lemma 2.2 shows that the product $\prod_p \sigma'_p$ taken over all primes p converges and we may thus define

$$c'_Q := \sigma'_\infty \prod_p \sigma'_p.$$

Notice that Lemma 4.3 implies that

$$\sigma'_\infty \ll \langle Q\rangle^2 \frac{K_{\|\cdot\|}}{|\Delta_Q|}. \tag{5.1}$$

In light of Lemma 3.1, it suffices to prove Proposition 2.1 for $\mathcal{N}(Q,B)$ in place of $N(Q,B)$. Combining Lemmata 3.2 and 4.2 gives

$$\begin{aligned}(5.2)\quad &\mathcal{N}(Q,B)\\ &= \sum_{k\lambda\mid \Delta_Q/\gcd(b,e)} \mu(k) \sideset{}{^*}\sum_{\substack{(\sigma,\tau) \pmod{k\lambda}\\ k\lambda\mid \mathbf{q}(\sigma,\tau)}} \sum_{\substack{m\le (2BK_{\|\cdot\|}/k)^{1/2}\\ \gcd(m,k\lambda)=1}} \mu(m) M_{\bar{m}\sigma,\bar{m}\tau}(B\lambda/m^2, k\lambda).\end{aligned}$$

Now notice that for

$$\mathcal{L} := \frac{(K_{\|\cdot\|}B)^{1/2}}{k\lambda^{1/2}} \frac{\langle Q\rangle}{|\Delta_Q|^{1/2}},$$

the bound (5.1) and Lemma 4.3 imply that

$$M_{\bar{m}\sigma,\bar{m}\tau}\left(\frac{B\lambda}{m^2}, k\lambda\right) = \begin{cases} \sigma'_\infty \dfrac{B}{m^2k^2\lambda} + O\left(\dfrac{\mathcal{L}}{m}\right) & \text{if } m\le \mathcal{L},\\ O(1) & \text{otherwise.}\end{cases}$$

The contribution to (5.2) coming from those m with $m > \mathcal{L}$ is therefore $\ll_\epsilon (BK_{\|\cdot\|})^{1/2}|\Delta_Q|\langle Q\rangle^\epsilon$. We have used the bound $\tau_k(n) \ll_{k,\epsilon} n^\epsilon$ as well as the second part of Lemma 2.2. The contribution of the remaining m is

$$\begin{aligned}\sigma'_\infty B \sum_{k\lambda\mid\Delta_Q} \frac{\mu(k)\rho^*(k\lambda)}{k^2\lambda} \sum_{\substack{m\le\mathcal{L}\\ \gcd(m,k\lambda)=1}} \frac{\mu(m)}{m^2}\\ + O_\epsilon\big((BK_{\|\cdot\|})^{1/2}\log(BK_{\|\cdot\|})\langle Q\rangle^{1+\epsilon}\gcd(b,e)^{1/2}\big).\end{aligned}$$

If we extend the summation over m to infinity, the error introduced in the main term is $\ll_\epsilon (BK_{\|\cdot\|})^{1/2}\langle Q\rangle^{1+\epsilon}\gcd(b,e)^{1/2}$, where we have made use of (5.1). The fact that $\gcd(b,e)^2 \mid \Delta_Q$ and $\gcd(b,e)\mid \delta_Q$ provides the error term in Proposition 2.1. Using the fact that ρ^* is multiplicative and supported on the divisors of Δ_Q we deduce that

$$\sum_{k,\lambda\in\mathbb{N}} \frac{\mu(k)\rho^*(k\lambda)}{k^2\lambda} \sum_{\substack{m\in\mathbb{N}\\ \gcd(m,k\lambda)=1}} \frac{\mu(m)}{m^2} = \prod_p \left(1-\frac{1}{p^2}+\left(1-\frac{1}{p}\right)\sum_{d\in\mathbb{N}}\frac{\rho^*(p^d)}{p^d}\right),$$

which shows that the leading constant is equal to c'_Q, as desired.

We proceed to explain why the leading constants c_Q and c'_Q are equal. One can indeed produce an elementary, yet lengthy, argument of this assertion, performing a parametrisation argument over $\mathbb{Z}/p^n\mathbb{Z}$ for appropriately chosen primes p and positive integers n, instead of over $\mathbb{Q}$. However, as the referee kindly pointed out, it is shown in [10, Sections 3 and 6.2] that the equality $c_Q = c'_Q$ follows from [7]. More precisely, the fact that points are equidistributed on the projective line implies that the leading constants

agree for any height, including the one coming from the embedding of the projective line as a conic. This concludes the proof of Proposition 2.1.

6. The proof of Theorem 1.1. In this section we complete the proof of Theorem 1.1 by transforming the general form Q into one to which Proposition 2.1 applies. The next lemma shows that one can find a suitable transformation with the lowest possible height.

LEMMA 6.1. *Let* $\mathbf{a} \in \mathbb{Z}^3_{\text{prim}}$. *Then there exists* $M \in \mathrm{SL}_3(\mathbb{Z})$ *whose second column is* $\mathbf{a}$ *and whose entries have maximum modulus* $O(\|\mathbf{a}\|_\infty)$.

Proof. By renaming indices if needed, we may assume that

$$0 < |a_1| \leq |a_2| \leq |a_3|.$$

Let us notice that an integer solution to the equation $\mathbf{a}^t\mathbf{y} = 1$ exists, owing to the coprimality of $\mathbf{a}$. The previous inequality implies that we can pick $s, t \in \mathbb{Z}$ such that $\max\{|y_3 - a_1 t|, |y_2 - a_1 s|\} \leq |a_1|/2$. Then the integer vector

$$\mathbf{x} := \mathbf{y} + s(a_2, -a_1, 0) + t(a_3, 0, -a_1)$$

satisfies $\mathbf{a}^t\mathbf{x} = 1$ and $\|\mathbf{x}\|_\infty \ll \|\mathbf{a}\|_\infty$.

We now let $x_i' := x_i/\gcd(x_1, x_2), i = 1, 2$, so that $\gcd(x_1', x_2') = 1$. We know therefore that an integer solution (x, y) of $x_1'x + x_2'y = x_3$ can be found. Considering $y - tx_1'$ in place of y if needed, we can prove as before that we can find (x, y) that satisfy the previous equation in addition to $\max\{|x|, |y|\} \ll \|\mathbf{x}\|_\infty$. A direct calculation then reveals that the matrix

$$M := \begin{pmatrix} x_2' & a_1 & -x \\ -x_1' & a_2 & -y \\ 0 & a_3 & \gcd(x_1, x_2) \end{pmatrix}$$

has the required properties. ∎

Proof of Theorem 1.1. Since the quadratic form Q has a rational zero, one can find, using Cassels [3], a non-trivial integer zero $\boldsymbol{\xi} := (x_0, y_0, z_0) \in \mathbb{Z}^3_{\text{prim}}$ of Q such that $\|\boldsymbol{\xi}\|_\infty \ll \langle Q \rangle$. We now transform the form Q using $\mathbf{a} = \boldsymbol{\xi}$ in the previous lemma. This provides an integer matrix M of determinant 1 and of size

$$\|M\|_\infty \ll \langle Q \rangle \tag{6.1}$$

such that the quadratic form Q' defined by

$$Q'(\mathbf{x}) := Q(M\mathbf{x})$$

is zero at $(0, 1, 0)$. We define a norm by

$$\|\mathbf{x}\|' := \|M\mathbf{x}\|$$

and notice that

$$\langle Q' \rangle \ll \langle Q \rangle^3.$$

The fact that M is unimodular implies that the integer vector $\mathbf{x}$ is primitive if and only if $M\mathbf{x}$ is. It therefore follows that

$$N(Q, B) = N'(Q', B),$$

where the notation N' indicates the use of the norm $\|\cdot\|'$. Recall the definition (1.3) of $K_{\|\cdot\|}$. Using the inequality $\|M^{-1}\|_\infty \leq 2\|M\|_\infty^2$ and writing $\mathbf{x} = M^{-1}(M\mathbf{x})$ for all $\mathbf{x} \neq \mathbf{0}$ implies that

$$\|\mathbf{x}\|_\infty \leq 2\|M\|_\infty^2 K_{\|\cdot\|}\|\mathbf{x}\|'.$$

Therefore (6.1) shows that for $K_{\|\cdot\|'} := 1 + \sup_{\mathbf{x}\neq 0} \|\mathbf{x}\|_\infty / \|\mathbf{x}\|'$, we have

$$K_{\|\cdot\|'} \ll K_{\|\cdot\|} \langle Q \rangle^2.$$

Finally, notice that the discriminants Δ_Q and $\Delta_{Q'}$ as well as the greatest common divisors δ_Q and $\delta_{Q'}$ of the 2×2 minors of the matrices of the quadratic forms Q and Q' remain invariant under the unimodular transformation M.

We are now in a position to apply Proposition 2.1 to the form Q' with all the quantities involved modified as indicated. We get an error term

$$\ll_\epsilon (BK_{\|\cdot\|})^{1/2} \log(BK_{\|\cdot\|}) \min\{|\Delta_Q|^{1/4}, \delta_Q^{1/2}\} \langle Q \rangle^{4+\epsilon}. \tag{6.2}$$

The bound $|\Delta_Q| \ll \langle Q \rangle^3$ implies that this is

$$\ll_\epsilon (BK_{\|\cdot\|})^{1/2} \log(BK_{\|\cdot\|}) \langle Q \rangle^{19/4+\epsilon},$$

so that using the value $\epsilon = 1/4$ we obtain the error term appearing in Theorem 1.1. Recall the definitions (1.1) and (1.2) of the local densities. It remains to show that they satisfy

$$\sigma_\infty(Q', \|\cdot\|') = \sigma_\infty(Q, \|\cdot\|) \quad \text{and} \quad \sigma_p(Q') = \sigma_p(Q)$$

for any prime p. The fact that the matrix M is invertible modulo p^n shows that $N_Q^*(p^n) = N_{Q'}^*(p^n)$, which when used in (1.2) proves the latter equality. The former is proved by performing the unimodular linear change of variables $\mathbf{x} = M\mathbf{X}$ in (1.1). Hence

$$\int\limits_{\substack{|Q(\mathbf{x})|\leq\epsilon \\ \|\mathbf{x}\|\leq 1}} 1 \, d\mathbf{x} = \int\limits_{\substack{|Q'(\mathbf{X})|\leq\epsilon \\ \|\mathbf{X}\|'\leq 1}} 1 \, d\,\mathbf{X},$$

which finishes the proof of Theorem 1.1.

Acknowledgments. The author would like to express his gratitude to T. Browning for suggesting the problem and for his valuable assistance during the course of this project. He is furthermore indebted to Dr. Christopher Frei for useful comments regarding an earlier version of this paper.

References

[1] T. D. Browning and D. R. Heath-Brown, *Counting rational points on hypersurfaces*, J. Reine Angew. Math. 584 (2005), 83–115.

[2] T. D. Browning and K. Van Valckenborgh, *Sums of three squareful numbers*, Experiment. Math. 21 (2012), 204–211.

[3] J. W. S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations*, Proc. Cambridge Philos. Soc. 51 (1955), 262–264.

[4] J. E. Cremona and D. Rusin, *Efficient solution of rational conics*, Math. Comp. 72 (2003), 1417–1441.

[5] H. Davenport, *On a principle of Lipschitz*, J. London Math. Soc. 26 (1951), 179–183.

[6] H. Davenport, *Corrigendum: "On a principle of Lipschitz"*, J. London Math. Soc. 39 (1964), 580.

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

[8] 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.

[9] C. Hooley, *On the Diophantine equation* $ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy = 0$, Arch. Math. (Basel) 19 (1968), 472–478.

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

[11] D. Simon, *Sur la paramétrisation des solutions des équations quadratiques*, J. Théorie Nombres Bordeaux 18 (2006), 265–283.

Efthymios Sofos
School of Mathematics
University of Bristol
Bristol, BS8 1TW, United Kingdom
E-mail: efthymios.sofos@bristol.ac.uk

Received on 2.5.2013
and in revised form on 1.9.2014 (7426)