Annals of Mathematics **175** (2012), 297–343
http://dx.doi.org/10.4007/annals.2012.175.1.8

On Manin's conjecture for a family of Châtelet surfaces

By Régis de la Bretèche, Tim Browning, and Emmanuel Peyre

Abstract

The Manin conjecture is established for Châtelet surfaces over $\mathbf{Q}$ arising as minimal proper smooth models of the surface $Y^2 + Z^2 = f(X)$ in $\mathbf{A}^3_{\mathbf{Q}}$, where $f \in \mathbf{Z}[X]$ is a totally reducible polynomial of degree 3 without repeated roots. These surfaces do not satisfy weak approximation.

Contents

1. Introduction

The purpose of this paper is to prove Manin's conjecture about points of bounded height for a family of Châtelet surfaces over $\mathbf{Q}$. These surfaces have been considered by F. Châtelet in [Châ59] and [Châ66], by V. A. Iskovskikh [Isk71], by D. Coray and M. A. Tsfasman [CT88], and by J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer in [CTSSD87a] and [CTSSD87b], among others.

The surfaces considered here are smooth proper models of the affine surfaces given in $\mathbf{A}^3_{\mathbf{Q}}$ by an equation of the form

$$Y^2 + Z^2 = X(a_3X + b_3)(a_4X + b_4)$$

for suitable a_3, b_3, a_4, $b_4 \in \mathbf{Z}$.

It is important to note that the surfaces we consider do not satisfy weak approximation, the lack of which is explained by the Brauer-Manin obstruction, as described in [CTSSD87a] and [CTSSD87b]. Up to now, the only cases for which Manin's principle was proven despite weak approximation not holding were obtained using harmonic analysis and required the action of an algebraic group on the variety with an open orbit. The method used in this paper is completely different. Following ideas of P. Salberger [Sal98], we use versal torsors introduced by Colliot-Thélène and Sansuc in [CTS77], [CTS80], and [CTS87] to estimate the number of rational points of bounded height on the surface. Such a combination of descent methods with analytic number theory was used in [HBS02] to prove that the Brauer-Manin obstruction to weak approximation is the only one for hypersurfaces related to norm forms. Therefore we can reasonably hope that further developments of these techniques may be successful in proving the refined conjectures of Manin for other such varieties.

This paper is organised as follows. In Section 2, we recall some facts about the geometry of the surfaces. In Section 3, we define the height and state our main result. Section 4 contains the description of the versal torsors we use. In Section 5, we describe the lifting of rational points to the versal torsors. This lifting reduces the initial problem to the estimation of some arithmetic sums denoted by $\mathscr{U}(T)$. The following sections contain the key analytical tools used in the proof. In Section 7 we give a uniform upper bound for $\mathscr{U}(T)$ and in Section 8 an asymptotic formula for it. The last section is devoted to an interpretation of the leading constant.

Let us fix some notation for the remainder of this text.

Notation and conventions. If k is a field, we denote by $\overline{k}$ an algebraic closure of k. For any variety X over k and any k-algebra A, we denote by X_A the product $X \times_{\mathrm{Spec}(k)} \mathrm{Spec}(A)$ and by $X(A)$ the set $\mathrm{Hom}_{\mathrm{Spec}(k)}(\mathrm{Spec}(A), X)$. We also put $\overline{X} = X_{\overline{k}}$. The cohomological Brauer group of X is defined as $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbf{G}_m)$, where $\mathbf{G}_m$ denotes the multiplicative group. The projective space of dimension n over A is denoted by $\mathbf{P}^n_A$ and the affine space by $\mathbf{A}^n_A$. For any $(x_0, \ldots, x_n) \in k^{n+1} - \{0\}$, we denote by $(x_0 : \cdots : x_n)$ its image in $\mathbf{P}^n(k)$.

Acknowledgements. While working on this paper the second author was supported by EPSRC grant number EP/E053262/1. Parts of the work were supported by the ANR project *Points entiers et points rationnels.*

2. A family of Châtelet surfaces

Let us fix a_1, a_2, a_3, a_4, b_1, b_2, $b_3, b_4 \in \mathbf{Z}$ such that

$$\Delta_{i,j} = \begin{vmatrix} a_i & a_j \\ b_i & b_j \end{vmatrix} \neq 0$$

for any $i, j \in \{1, 2, 3, 4\}$ with $i \neq j$. We then consider the linear forms L_i defined by $L_i(U, V) = a_i U + b_i V$ for $i \in \{1, 2, 3, 4\}$ and define the hypersurface S_1 of $\mathbf{P}^2_{\mathbf{Q}} \times \mathbf{A}^1_{\mathbf{Q}}$ given by the equation

$$X^2 + Y^2 = T^2 \prod_{i=1}^{4} L_i(U, 1)$$

and the hypersurface S_2 given by the equation

$$X'^2 + Y'^2 = T'^2 \prod_{i=1}^{4} L_i(1, V).$$

Let U_1 be the open subset of S_1 defined by $U \neq 0$ and U_2 be the open subset of S_2 defined by $V \neq 0$. The map $\Phi : U_1 \to U_2$ which maps $((X : Y : T), U)$ onto $((X : Y : U^2T), 1/U)$ is an isomorphism and we define S as the surface obtained by glueing S_1 to S_2 using the isomorphism Φ. The surface S is a smooth projective surface and is a particular case of a Châtelet surface. The geometry of such surfaces has been described by J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer in [CTSSD87b, §7]. For the sake of completeness, let us recall part of this description which will be useful for the description of versal torsors.

The map $S_1 \to \mathbf{P}^1_{\mathbf{Q}}$ (resp. $S_2 \to \mathbf{P}^1_{\mathbf{Q}}$) which maps $((X : Y : T), U)$ onto $(U : 1)$ (resp. $((X' : Y' : T'), V)$ onto $(1 : V)$) glue together to give a conic fibration $\pi : S \to \mathbf{P}^1_{\mathbf{Q}}$ with four degenerate fibres over the points given by $P_i = (-b_i : a_i) \in \mathbf{P}^1(\mathbf{Q})$ for $i \in \{1, 2, 3, 4\}$. In fact, the glueing of $\mathbf{P}^2_{\mathbf{Q}} \times \mathbf{A}^1_{\mathbf{Q}}$ to $\mathbf{P}^2_{\mathbf{Q}} \times \mathbf{A}^1_{\mathbf{Q}}$ through the map

$$((X : Y : T), U) \mapsto ((X : Y : U^2T), 1/U) \tag{2.1}$$

gives the projective bundle[1] $\mathcal{P} = \mathbf{P}(\mathscr{O}^2 \oplus \mathscr{O}(-2))$ over $\mathbf{P}^1_{\mathbf{Q}}$ and S may be seen as a hypersurface in that bundle.

Over $\mathbf{Q}(i)$, if $\xi \in \{-i, i\}$, then the map $\mathbf{A}_{\mathbf{Q}(i)} \to S_{1\mathbf{Q}(i)}$ which is given by $u \mapsto ((\xi : 1 : 0), U)$ extends to a section σ_ξ of π. The surface $S_{\mathbf{Q}(i)}$ contains 10 exceptional curves, that is irreducible curves with negative self-intersection.

[1]We define here $\mathbf{P}(\mathscr{O}^2 \oplus \mathscr{O}(-2))$ as the projective bundle associated to the sheave of graded commutative algebras $\underline{\mathrm{Sym}}(\mathscr{O}^2 \oplus \mathscr{O}(2))$. In other words the fibre over a point is given by the lines in the fibre of the vector bundle and not by the hyperplanes.

Eight of them are given in $S_{\mathbf{Q}(i)}$ by the following equations:

$$D_j^\xi: \qquad L_j(\pi(P)) = 0 \quad \text{and} \quad X - \xi Y = 0$$

for $\xi \in \{-i, i\}$ and $j \in \{1, 2, 3, 4\}$; the last ones correspond to the section σ_ξ and are given by the equations

$$E^\xi: \qquad T = 0 \quad \text{and} \quad X - \xi Y = 0.$$

Here X, Y, and T are seen as sections of $\mathscr{O}_{\mathcal{P}}(1)$. Let us denote by $\mathscr{G}$ the Galois group of $\mathbf{Q}(i)$ over $\mathbf{Q}$ and by $z \mapsto \overline{z}$ the nontrivial element in $\mathscr{G}$. Then we have

$$\overline{E^\xi} = E^{\overline{\xi}} \quad \text{and} \quad \overline{D_j^\xi} = D_j^{\overline{\xi}}$$

for $\xi \in \{-i, i\}$ and $j \in \{1, 2, 3, 4\}$. We shall also write D_j^+ (resp. D_j^-, E^+, E^-) for D_j^i (resp. D_j^{-i}, E^i, E^{-i}). The intersection multiplicities of these divisors are given by

$$(E^\xi, E^\xi) = -2, \quad (D_j^\xi, D_j^\xi) = -1, \quad (D_j^\xi, D_j^{-\xi}) = 1, \quad (E^\xi, D_j^\xi) = 1,$$

where $\xi \in \{-i, i\}$ and $j \in \{1, 2, 3, 4\}$, all other intersection multiplicities being equal to 0 (see [CTSSD87b, p. 73]). The geometric Picard group of S, that is $\mathrm{Pic}(\overline{S})$, is isomorphic to $\mathrm{Pic}(S_{\mathbf{Q}(i)})$ and is generated by these exceptional divisors with the relations

$$[D_j^+] + [D_j^-] = [D_k^+] + [D_k^-] \tag{2.2}$$

for $j, k \in \{1, 2, 3, 4\}$ and

$$[E^+] + [D_j^+] + [D_k^+] = [E^-] + [D_l^-] + [D_m^-] \tag{2.3}$$

whenever $\{j, k, l, m\} = \{1, 2, 3, 4\}$. Using the fact that $\mathrm{Pic}(S) = (\mathrm{Pic}(S_{\mathbf{Q}(i)}))^{\mathscr{G}}$ it is easy to deduce that $\mathrm{Pic}(S)$ has rank 2.

It follows from the adjunction formula that the class of the anticanonical line bundle is given by

$$\omega_S^{-1} = 2E^+ + \sum_{j=1}^4 D_j^+ = 2E^- + \sum_{j=1}^4 D_j^-.$$

LEMMA 2.1. *Using the trivialisation described by* (2.1), *the* 5-*tuple of functions*

$$(T, UT, U^2T, X, Y)$$

gives a basis of $\Gamma(S, \omega_S^{-1})$.

Proof. Let C be a generic divisor in $|\omega_S^{-1}|$. Then C is a smooth irreducible curve; let g_C be its genus. According to the adjunction formula, we have that $2g_C - 2 = \omega_S.(\omega_S - \omega_S) = 0$. Thus $g_C = 1$. The exact sequence of sheaves

$$0 \longrightarrow \mathscr{O}_S \longrightarrow \omega_S^{-1} \longrightarrow \omega_S^{-1} \otimes \mathscr{O}_C \longrightarrow 0$$

gives an exact sequence

$$0 \longrightarrow H^0(S,\mathscr{O}_S) \longrightarrow H^0(S,\omega_S^{-1}) \longrightarrow H^0(C,\omega_S^{-1}{}_{|C}) \longrightarrow H^1(S,\mathscr{O}_S).$$

But S is geometrically rational and $H^1(S,\mathscr{O}_S)=\{0\}$. We get that

$$h^0(S,\omega_S^{-1}) = 1 + h^0(C,\omega_S^{-1}{}_{|C}).$$

Let $D=\omega_S^{-1}{}_{|C}$. We have that $\deg(D)=4$ and $\deg(\omega_C - D) = -4$ since $\omega_C = 0$. Applying the Riemann-Roch theorem to C, we get that

$$h^0(D) = \deg(D) + 2g_C - 2 = 4$$

and $h^0(S,\omega_S^{-1}) = 5$. Since the sections T, UT, U^2T, X, and Y are linearly independent, and extend to a section of $\mathscr{O}_{\mathcal{P}}(1)$, we get a basis of $\Gamma(S,\omega_S^{-1})$. $\square$

Lemma 2.2. *The linear system $|\omega_S^{-1}|$ has no base point and the basis given in Lemma* 2.1 *gives a morphism from S to $\mathbf{P}^4_{\mathbf{Q}}$, the image of which is the surface S' given by the system of equations*

$$\begin{cases} X_0X_2 - X_1^2 = 0, \\ X_3^2 + X_4^2 = (aX_0 + bX_1 + cX_2)(a'X_0 + b'X_1 + c'X_2), \end{cases}$$

where

$$a = a_1a_2, \qquad b = a_1b_2 + a_2b_1, \qquad c = b_1b_2,$$
$$a' = a_3a_4, \qquad b' = a_3b_4 + a_4b_3, \qquad c' = b_3b_4.$$

The induced map $\psi : S \to S'$ is the blowing up of the conjugate singular points of S' given by $P^\xi = (0:0:0:1:-\xi)$ with $\xi^2 = -1$ and $\psi^{-1}(P^\xi) = E^\xi$.

Proof. This follows from the fact that the map from S to $\mathbf{P}^4_{\mathbf{Q}}$ induces the maps

$$((x:y:t),u) \longmapsto (t : ut : u^2t : x : y)$$

from S_1 to $\mathbf{P}^4_{\mathbf{Q}}$ and

$$((x':y':t'),v) \longmapsto (v^2t' : vt' : t' : x' : y')$$

from S_2 to $\mathbf{P}^4_{\mathbf{Q}}$. $\square$

Remark 2.3. The surface S' is an Iskovskikh surface [CT88]; it is a singular Del Pezzo surface of degree 4 with a singularity of type $2A_1$, and $\psi : S \to S'$ is a minimal resolution of singularities for S'.

3. Points of bounded height

Over $\overline{\mathbf{Q}}$ or even $\mathbf{Q}(i)$, the only geometrical invariant of S is the cross-ratio

$$\alpha = \frac{\begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix} \Big/ \begin{vmatrix} a_3 & a_2 \\ b_3 & b_2 \end{vmatrix}}{\begin{vmatrix} a_4 & a_1 \\ b_4 & b_1 \end{vmatrix} \Big/ \begin{vmatrix} a_4 & a_2 \\ b_4 & b_2 \end{vmatrix}} \quad \in \mathbf{Q}.$$

Indeed the automorphisms of $\mathbf{P}^1_{\mathbf{Q}}$ sending the points P_1, P_2, P_3 onto the points $\infty = (0:1)$, $0 = (1:0)$, and $1 = (1:1)$ lifts to an isomorphism from S to the Châtelet surface with an equation of the form

$$X^2 + Y^2 = \beta U(U-1)(U-\alpha)T^2,$$

where $\beta \in \mathbf{Q}$. Over $\mathbf{Q}(i)$ we may further reduce to the case where $\beta = 1$. In particular, without any loss of generality, we may assume that

$$a_1 = b_2 = 1 \qquad \text{and} \qquad a_2 = b_1 = 0. \tag{3.1}$$

Hypothesis 3.1. From now on we assume relations (3.1), that we have $\gcd(a_3, b_3) = \gcd(a_4, b_4) = 1$, and that $a_3 b_3 a_4 b_4 (a_3 b_4 - a_4 b_3) \neq 0$.

Notation 3.2. Let $C = \sqrt{\prod_{j=1}^4 (|a_j| + |b_j|)}$. We equip the projective space $\mathbf{P}^4_{\mathbf{Q}}$ with the exponential height $H_4 : \mathbf{P}^4(\mathbf{Q}) \to \mathbf{R}$ defined by

$$H_4(x_0 : x_1 : x_2 : x_3 : x_4) = \max\left(|x_0|, |x_1|, |x_2|, \frac{|x_3|}{C}, \frac{|x_4|}{C}\right)$$

if $x_0, \ldots, x_4$ are coprime integers. Using the morphism $\psi : S \to S'$, we get a height $H = H_4 \circ \psi$ which is associated to the anticanonical line bundle ω_S^{-1}.

We denote by $\mathrm{Val}(\mathbf{Q})$ the set of places of $\mathbf{Q}$. For any $v \in \mathrm{Val}(\mathbf{Q})$, $\mathbf{Q}_v$ is the corresponding completion of $\mathbf{Q}$. As explained in [Pey95, §2], such a height enables us to define a Tamagawa measure $\boldsymbol{\omega}_H$ on the adelic space $S(\boldsymbol{A}_{\mathbf{Q}}) = \prod_{v \in \mathrm{Val}(\mathbf{Q})} S(\mathbf{Q}_v)$. We also consider the constant $\alpha(S)$ defined in [Pey95, Def. 2.4] which is equal to $\frac{1}{2}$ in our particular case and, following Batyrev and Tschinkel [BT95], we also put $\beta(S) = \sharp\big(\mathrm{coker}(\mathrm{Br}(\mathbf{Q}) \to \mathrm{Br}(S))\big) = 4$ (see [Sko01, Prop. 7.1.2]). We then set

$$C_H(S) = \alpha(S)\beta(S)\boldsymbol{\omega}_H(S(\boldsymbol{A}_{\mathbf{Q}})^{\mathrm{Br}}),$$

where $S(\boldsymbol{A}_{\mathbf{Q}})^{\mathrm{Br}}$ is the set of points in the adelic space for which the Brauer-Manin obstruction to weak approximation is trivial.

We are interested in the asymptotic behaviour of the number of points of bounded height in $S(\mathbf{Q})$, that is by the number

$$N_{S,H}(B) = \sharp\{P \in S(\mathbf{Q}),\ H(P) \leqslant B\}$$

for $B \in \mathbf{R}$ with $B > 1$.

We can now state the main result of this paper.

THEOREM 3.3. *For any Châtelet surface as above*, *we have the asymptotic formula*

$$N_{S,H}(B) = C_H(S)B\log(B) + O\Big(B\log(B)^{0.972}\Big). \tag{F}$$

Remarks 3.4. (i) One may note that, as $S(\mathbf{Q})$ is dense in $S(\boldsymbol{A}_{\mathbf{Q}})^{\mathrm{Br}}$ by [CTSSD87a, Th. B], this formula is compatible with the empirical formula (F) described in [Pey03, formule empirique 5.1] which is a refinement of a conjecture of Batyrev and Manin [BM90].

(ii) Over $\mathbf{R}$, the image of $S(\mathbf{R})$ on $\mathbf{P}^1(\mathbf{R})$ is the union of two intervals defined by the conditions $\prod_{j=1}^4 L_j(U,V) > 0$. Therefore we may choose indices $j,k\in\{1,2,3,4\}$ such that $j\neq k$ and the sign of $L_j(U,V)L_k(U,V)$ is not constant on $S(\mathbf{R})$. The evaluation of the element $(-1, L_j(U,V)/L_k(U,V)) \in \mathrm{Br}(S)$ (see [Sko01, Prop. 7.1.2]) is not constant on $S(\mathbf{R})$. Therefore in all the cases we consider, $S(\boldsymbol{A}_{\mathbf{Q}})^{\mathrm{Br}} \neq S(\boldsymbol{A}_{\mathbf{Q}})$.

4. Description of versal torsors

Versal torsors were first introduced by J.-L. Colliot-Thélène and J.-J. Sansuc in [CTS77], [CTS80], and [CTS87] as a tool to prove that the Brauer–Manin obstruction to the Hasse principle and weak approximation is the only one. In [CTS87, §2.6], these authors give a description of the versal torsors for Châtelet surfaces up to birational equivalence. To be able to parametrise the points of $S(\mathbf{Q})$ we in fact need to construct the versal torsors themselves. Our construction is akin to the one used by Colliot-Thélène and Sansuc but also to the constructions based upon Cox rings.

We shall first introduce an intermediate versal torsor which corresponds to the Picard group of S over $\mathbf{Q}$, that is to the maximal split quotient of T_{NS}.

Definition 4.1. Let $\mathscr{T}_{\mathrm{spl}}$ be the subscheme of $\mathbf{A}^5_{\mathbf{Z}} = \mathrm{Spec}(\mathbf{Z}[X,Y,T,U,V])$ defined by the equation

$$X^2+Y^2 = T^2\prod_{j=1}^4 L_j(U,V) \tag{4.1}$$

and the conditions

$$(X,Y,T)\neq 0 \quad\text{and}\quad (U,V)\neq 0.$$

The split algebraic torus $T_{\mathrm{spl}} = \mathbf{G}^2_{m,\mathbf{Z}}$ acts on $\mathscr{T}_{\mathrm{spl}}$ via the morphism of tori

$$(\lambda,\mu)\mapsto(\lambda,\lambda,\mu^{-2}\lambda,\mu,\mu)$$

from $\mathbf{G}^2_{m,\mathbf{Z}}$ to $\mathbf{G}^5_{m,\mathbf{Z}}$ and the natural action of $\mathbf{G}^5_{m,\mathbf{Z}}$ on $\mathbf{A}^5_{\mathbf{Z}}$. Let $\mathcal{T}_{\mathrm{spl}}$ be the variety $\mathscr{T}_{\mathrm{spl},\mathbf{Q}}$. We have an obvious morphism π_{spl} from $\mathcal{T}_{\mathrm{spl}}$ to S which may be described as follows: for any extension $\mathbf{K}$ of $\mathbf{Q}$ and any point (x, y, t, u, v) of $\mathcal{T}_{\mathrm{spl}}(\mathbf{K})$, if $v \neq 0$, then the point $((x : y : tv^2), u/v)$ belongs to $S_1(\mathbf{K}) \subset S(\mathbf{K})$. If $u \neq 0$, then the point $((x : y : tu^2), v/u)$ belongs to $S_2(\mathbf{K}) \subset S(\mathbf{K})$ and the points obtained in $S(\mathbf{K})$ coincide if $uv \neq 0$. The morphism π_{spl} makes of $\mathcal{T}_{\mathrm{spl}}$ a $\mathbf{G}_m^2$-torsor over S.

We now turn to the construction of the versal torsors.

Notation 4.2. We denote by $\boldsymbol{\Delta}$ the set of exceptional divisors in $S_{\mathbf{Q}(i)}$ and consider it as a $\mathscr{G}$-set. Let $\boldsymbol{\Delta}_{\mathbf{Q}}$ be the set of $\mathscr{G}$-orbits in $\boldsymbol{\Delta}$. We put $E = \{E^+, E^-\}$ and $D_j = \{D_j^+, D_j^-\}$ for $j \in \{1, 2, 3, 4\}$. Then

$$\boldsymbol{\Delta}_{\mathbf{Q}} = \{E, D_1, D_2, D_3, D_4\}.$$

For $\delta \in \boldsymbol{\Delta}_{\mathbf{Q}}$, we may also write $\delta = \{\delta^+, \delta^-\}$. We consider the affine space $\mathbf{A}_{\boldsymbol{\Delta},\mathbf{Z}}$ of dimension 10 over $\mathbf{Z}$

$$\mathbf{A}_{\boldsymbol{\Delta},\mathbf{Z}} = \mathrm{Spec}(\mathbf{Z}[X_\delta, Y_\delta, \delta \in \boldsymbol{\Delta}_{\mathbf{Q}}])$$

and define $\mathbf{A}_{\boldsymbol{\Delta}} = (\mathbf{A}_{\boldsymbol{\Delta},\mathbf{Z}})_{\mathbf{Q}}$. For any $\delta \in \boldsymbol{\Delta}_{\mathbf{Q}}$, we put $Z_{\delta^+} = X_\delta + iY_\delta$ and $Z_{\delta^-} = X_\delta - iY_\delta$. We may then consider the algebraic torus

$$T_{\boldsymbol{\Delta}} = \mathrm{Spec}\left((\mathbf{Q}(i)[Z_\delta, Z_\delta^{-1}, \delta \in \boldsymbol{\Delta}])^{\mathscr{G}}\right)$$

as an open subvariety of $\mathbf{A}_{\boldsymbol{\Delta}}$. We shall also write Z_k^ε (resp. Z_0^ε) for $Z_{D_k^\varepsilon}$ (resp. Z_{E^ε}) and use similar conventions for the variables X_δ and Y_δ.

We now wish to construct for each isomorphism class of versal torsors over S with a rational point a representative of this class in $\mathbf{A}_{\boldsymbol{\Delta}}$.

Notation 4.3. Let $\boldsymbol{n} = (n_1, n_2, n_3, n_4)$ belong to $(\mathbf{Z} - \{0\})^4$. We define $\mathscr{Y}_{\boldsymbol{n}}$ as the subscheme of $\mathbf{A}_{\boldsymbol{\Delta},\mathbf{Z}}$ given by the equations

$$\Delta_{j,k} n_l (X_l^2 + Y_l^2) + \Delta_{k,l} n_j (X_j^2 + Y_j^2) + \Delta_{l,j} n_k (X_k^2 + Y_k^2) = 0 \tag{4.2}$$

if $1 \leqslant j < k < l \leqslant 4$. The scheme $\mathscr{T}_{\boldsymbol{n}}$ is the open subset of $\mathscr{Y}_{\boldsymbol{n}}$ given by the conditions

$$(Z_{\delta_1}, Z_{\delta_2}) \neq (0, 0), \tag{4.3}$$

whenever $\delta_1 \cap \delta_2 = \emptyset$. We denote by $\mathcal{T}_{\boldsymbol{n}}$ the variety $(\mathscr{T}_{\boldsymbol{n}})_{\mathbf{Q}}$.

Remark 4.4. Equations (4.2) define an intersection of two quadrics in $\mathbf{A}_{\mathbf{Q}}^8$, upon which we will ultimately need to count integral points of bounded height. As shown by Cook in [Coo71], the Hardy-Littlewood circle method can be adapted to handle intersections of diagonal quadrics in at least nine variables. Here we will need to deal with an intersection of diagonal quadrics in only eight variables. For this we will call upon the alternative approach based on the geometry of numbers in [dlBB08].

It follows from [CTS80, Prop. 2] that the set of isomorphism classes of versal torsors over S with a rational point is finite. We introduce a finite set which parametrises this set.

Notation 4.5. Let $\mathcal{S}$ be the set of primes p such that[2] $p \mid \prod_{1\leqslant j<k\leqslant 4} \Delta_{j,k}$. For any j in $\{1,2,3,4\}$, we put

$$\mathcal{S}_j = \left\{p \in \mathcal{S},\ p \equiv 3 \bmod 4 \quad \text{and} \quad p \mid \prod_{k\neq j} \Delta_{j,k}\right\}$$

and

$$\Sigma_j = \left\{(-1)^{\varepsilon_{-1}} \prod_{p\in\mathcal{S}_j} p^{\varepsilon_p}, (\varepsilon_{-1}, (\varepsilon_p)_{p\in\mathcal{S}_j}) \in \{0,1\} \times \{0,1\}^{\mathcal{S}_j}\right\}.$$

Finally, we define Σ to be the set of $\boldsymbol{m} = (m_j)_{1\leqslant j\leqslant 4} \in \prod_{j=1}^4 \Sigma_j$ such that the four integers are relatively prime, m_1 is positive and $\prod_{j=1}^4 m_j$ is a square. For any $\boldsymbol{m} \in \Sigma$, we denote by $\alpha_{\boldsymbol{m}}$ the positive square root of $\prod_{j=1}^4 m_j$.

Let $\boldsymbol{m}$ belong to Σ. We define a morphism $\pi_{\boldsymbol{m}} : \mathcal{T}_{\boldsymbol{m}} \to S$. In order to do this, it is enough to define a morphism $\widehat{\pi}_{\boldsymbol{m}} : \mathcal{T}_{\boldsymbol{m}} \to \mathcal{T}_{\mathrm{spl}}$ which is done as follows. For any extension $\mathbf{K}$ of $\mathbf{Q}$ and any $\boldsymbol{z} = (z_\delta)_{\delta\in\Delta}$ in $\mathcal{T}_{\boldsymbol{m}}(\mathbf{K})$, conditions (4.2) and (4.3) ensure that there exists a pair $(u,v) \in \mathbf{K}^2 - \{0\}$ such that

$$L_j(u,v) = m_j z_j^+ z_j^- \tag{4.4}$$

for $j \in \{1,2,3,4\}$. Let $(x,y,t) \in \mathbf{K}^3 - \{0\}$ be given by the conditions

$$\begin{cases} x + iy = \alpha_{\boldsymbol{m}} (z_0^+)^2 \prod_{j=1}^4 z_j^+, \\ x - iy = \alpha_{\boldsymbol{m}} (z_0^-)^2 \prod_{j=1}^4 z_j^-, \\ t = z_0^+ z_0^-. \end{cases} \tag{4.5}$$

Then we have the relation

$$x^2 + y^2 = t^2 \prod_{j=1}^4 L_j(u,v)$$

and (x,y,t,u,v) belongs to $\mathcal{T}_{\mathrm{spl}}(\mathbf{K})$.

It remains to describe the action of the torus T_{NS} associated to the $\mathscr{G}$-lattice $\mathrm{Pic}(\overline{S})$ on $\mathcal{T}_{\boldsymbol{m}}$. The algebraic torus $T_{\boldsymbol{\Delta}}$ corresponds to the $\mathscr{G}$-lattice $\mathbf{Z}^{\boldsymbol{\Delta}}$ and $T_{\boldsymbol{\Delta}}$ acts by multiplication of the coordinates on $\mathbf{A}_{\boldsymbol{\Delta}}$. The natural surjective morphism of $\mathscr{G}$-lattices

$$-\mathrm{pr} : \mathbf{Z}^{\boldsymbol{\Delta}} \longrightarrow \mathrm{Pic}(\overline{S})$$

induces an embedding of the algebraic torus T_{NS} on $T_{\boldsymbol{\Delta}}$.[3]

[2] Over $\mathbf{Z}/2\mathbf{Z}$, one of the $\Delta_{j,k}$ has to be zero, and so $2 \in \mathcal{S}$.

[3] There is some question of convention in the definition of versal torsors which leads us to use the opposite of the projection map.

PROPOSITION 4.6. *Let $\boldsymbol{m}$ belong to Σ. The variety $\mathcal{T}_{\boldsymbol{m}}$ is invariant under the action of T_{NS} on $\mathbf{A}_{\boldsymbol{\Delta}}$, and the variety $\mathcal{T}_{\boldsymbol{m}}$ equipped with the map $\pi_{\boldsymbol{m}} : \mathcal{T}_{\boldsymbol{m}} \to S$ and this action of T_{NS} is a versal torsor above S.*

Proof. The description of the kernel of the morphism pr (see (2.2), (2.3)) give the following equations for T_{NS}:

$$Z_j^+ Z_j^- = Z_k^+ Z_k^- \tag{4.6}$$

for $j,\, k \in \{1,2,3,4\}$ and

$$Z_0^+ Z_j^+ Z_k^+ = Z_0^- Z_l^- Z_m^- \tag{4.7}$$

if $\{j,k,l,m\} = \{1,2,3,4\}$. Equations (4.2) are invariant under the action of T_{NS} thanks to (4.6) as are inequalities (4.3). Therefore the action of T_{NS} on $\mathbf{A}_{\boldsymbol{\Delta}}$ induces a natural action of T_{NS} on $\mathcal{T}_{\boldsymbol{m}}$. This description of T_{NS} also implies that $\pi_{\boldsymbol{m}}$ is invariant under the action of T_{NS} on $\mathcal{T}_{\boldsymbol{m}}$. Indeed let $\mathbf{K}$ be an extension of $\mathbf{Q}$, let t belong to $T_{\mathrm{NS}}(\mathbf{K})$, and $\boldsymbol{z}$ to $\mathcal{T}_{\boldsymbol{m}}(\mathbf{K})$. We put $\boldsymbol{z}' = t\boldsymbol{z}$. It follows from (4.4) and (4.6) that $\boldsymbol{z}$ and $\boldsymbol{z}'$ define the same point $(u : v) \in \mathbf{P}^1(\mathbf{K})$ and from (4.5), (4.6), and (4.7) that $\boldsymbol{z}$ and $\boldsymbol{z}'$ give the same point $(x : y : tv^2)$ (resp. $(x : y : tu^2)$ in $\mathbf{P}^2(\mathbf{K})$).

We note that for any extension K of $\mathbf{Q}$, if $R \in \mathcal{T}_{\boldsymbol{m}}(K)$, then $\pi_{\boldsymbol{m}}^{-1}(\pi_{\boldsymbol{m}}(R))$ coincides with the orbit of R under the action of T_{NS}. Indeed if $R' \in \mathcal{T}_{\boldsymbol{m}}(K)$ satisfies $\pi_{\boldsymbol{m}}(R') = \pi_{\boldsymbol{m}}(R)$, then there exists a unique $\boldsymbol{z} \in T_{\boldsymbol{\Delta}}(\mathbf{K})$ such that $R' = \boldsymbol{z}R$. Let us write $\boldsymbol{z} = (z_\delta)_{\delta \in \boldsymbol{\Delta}}$. Using (4.4) and (4.5) and the description of the action of $\mathbf{G}_m^2(K)$ on $\mathscr{T}_{\mathrm{spl}}$, we get that $z_i^+ z_i^- = z_j^+ z_j^-$ if $1 \leqslant i < j \leqslant 4$, and

$$z_0^+ z_0^- (z_k^+ z_k^-)^2 = (z_0^+)^2 \prod_{j=1}^4 z_j^+ = (z_0^-)^2 \prod_{j=1}^4 z_j^-$$

for $k \in \{1,2,3,4\}$. We deduce from these equations that $\boldsymbol{z} \in T_{\mathrm{NS}}(K)$.

It is enough to prove the result over $\overline{\mathbf{Q}}$. By choosing square roots α_j of m_j such that $\prod_{j=1}^4 \alpha_j = \alpha_{\boldsymbol{m}}$, and using a change of variable of the form $Z_j^{\varepsilon\prime} = \alpha_j Z_j^{\varepsilon}$ for $\varepsilon \in \{+1,-1\}$ and $j \in \{1,2,3,4\}$ we may assume that $\boldsymbol{m} = (1,1,1,1)$. Note that for any δ in $\boldsymbol{\Delta}$, the variety $\pi_{\boldsymbol{m}}^{-1}(E_{\boldsymbol{\Delta}})$ is the subvariety of $\mathcal{T}_{\boldsymbol{m}}$ defined by $Z_\delta = 0$. If $\varepsilon \in \{+1,-1\}$, we consider the open subset

$$U_\varepsilon = S - E^\varepsilon - \bigcup_{j=1}^4 E_j^\varepsilon$$

of S and for $j \in \{1,2,3,4\}$, we put

$$U_j = S - E^+ - E^- - \bigcup_{k \neq j} (E_k^+ \cup E_k^-).$$

The open subsets U_1, U_2, U_3, U_4, U_+, and U_- form an open covering of S. If $\varepsilon \in \{+1,-1\}$, we consider that $X + \varepsilon iY = 1$ on U_ε, and we define a section s_ε^1

(resp. s_ε^2) of $\pi_{\mathbf{1}}$ over $U_\varepsilon \cap S_1$ (resp. $U_\varepsilon \cap S_2$) by $Z_0^\varepsilon = Z_1^\varepsilon = Z_2^\varepsilon = Z_3^\varepsilon = Z_4^\varepsilon = 1$, $Z_0^{-\varepsilon} = t$ and $Z_j^{-\varepsilon} = L_j(U,1)$ (resp. $Z_j^{-\varepsilon} = L_j(1,V)$) for $j \in \{1,2,3,4\}$. Similarly, for $j \in \{1,2,3,4\}$, fix k,l,m so that $\{j,k,l,m\} = \{1,2,3,4\}$. On U_j, we may consider that $L_k(U,V) = 1$ and $T = 1$. We may then define a section s_j of $\pi_{\mathbf{1}}$ over U_j by $Z_k^+ = Z_k^- = Z_0^+ = Z_0^- = Z_l^+ = Z_m^+ = 1$ and

$$Z_l^- = L_l(U,V), \quad Z_m^- = L_m(U,V), \quad Z_j^+ = \frac{X+iY}{\prod_{r\neq j} Z_r^+}, \quad \text{and} \quad Z_j^- = \frac{X-iY}{\prod_{r\neq j} Z_r^+}.$$

Condition (4.3) ensures that, for any point $P \in \mathcal{T}_{\mathbf{1}}(\overline{\mathbf{Q}})$, the stabilizer of P in $T_{\mathrm{NS}}(\overline{\mathbf{Q}})$ is trivial. Using the action of T_{NS} on $\mathcal{T}_{\mathbf{1}}$ we then get an equivariant isomorphism from $T_{\mathrm{NS}} \times U$ to $\pi_{\mathbf{1}}^{-1}(U)$ for each open subset U described above. This proves that $\mathcal{T}_{\boldsymbol{m}}$ is a T_{NS}-torsor over S.

It remains to prove that the endomorphism of $\operatorname{Pic}(\overline{S})$ defined by this torsor is the identity map. Let us first recall how this endomorphism may be defined. If L is a line bundle over $\overline{S}$, then the class of L defines a morphism of Galois lattices $\mathbf{Z} \to \operatorname{Pic}(\overline{S})$ and therefore a morphism of algebraic tori $\phi_L : T_{\mathrm{NS}} \to \mathbf{G}_m$ and an action of T_{NS} on $\mathbf{G}_m$. The restricted product $\mathcal{T} \times^{T_{\mathrm{NS}}} \mathbf{G}_m$ is a $\mathbf{G}_m$-torsor over $\overline{S}$ which defines an element of $\operatorname{Pic}(\overline{S})$. For any δ in $\boldsymbol{\Delta}$, the function Z_δ on $\mathcal{T}_{\boldsymbol{m}}$ is invariant under the action of the kernel of the map $\phi_\delta : T_{\mathrm{NS}} \to \mathbf{G}_m$ defined by the class of δ in $\operatorname{Pic}(\overline{S})$. Therefore this function defines an antiequivariant map from $\mathcal{T}_{\boldsymbol{m}} \times^{T_{\mathrm{NS}}} \mathbf{G}_m$ to $\mathbf{A}^1$ which vanishes with multiplicity one over $\pi_{\boldsymbol{m}}^{-1}(\delta)$. Thus the endomorphism defined by $\mathcal{T}_{\boldsymbol{m}}$ on $\operatorname{Pic}(\overline{S})$ sends the class of δ to itself for any $\delta \in \boldsymbol{\Delta}$. This proves that $\mathcal{T}_{\boldsymbol{m}}$ is a versal torsor over S. □

To conclude these constructions it remains to prove that the set of rational points $S(\mathbf{Q})$ is the disjoint union of the sets $\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}))$ where $\boldsymbol{m}$ runs over the set Σ.

Lemma 4.7. *For any $P \in S(\mathbf{Q})$, we have*

$$\sharp(\pi_{\mathrm{spl}}^{-1}(P) \cap \mathscr{T}_{\mathrm{spl}}(\mathbf{Z})) = \sharp \mathbf{G}_m^2(\mathbf{Q})_{\mathrm{tors}} = 2^2.$$

Proof. Let us start with a point $P = ((x_0 : y_0 : t_0), u_0)$ in $S_1(\mathbf{Q})$. We then have the relation

$$x_0^2 + y_0^2 = t_0^2 \prod_{j=1}^{4} L_i(u_0, 1).$$

We may write $u_0 = u/v$ with $u, v \in \mathbf{Z}$ and $\gcd(u,v) = 1$. Then we may find an element λ of $\mathbf{Q}$ such that the rational numbers $x = \lambda x_0$, $y = \lambda y_0$ and $t = \lambda t_0 / v^2$ are coprime integers and we have

$$x^2 + y^2 = t^2 \prod_{j=1}^{4} L_j(u,v).$$

The same construction works for any point of $S_2(\mathbf{Q})$, and if P belongs to $S_1(\mathbf{Q}) \cap S_2(\mathbf{Q})$, the elements of $\mathbf{Z}^5$ thus obtained coincide up to multiplication of the first three or the last two coordinates by -1. $\square$

Remark 4.8. Note that if we impose conditions like

$$t > 0, \quad L_1(u,v) \geqslant 0 \quad \text{and} \quad \prod_{j=2}^{4} L_j(u,v) \geqslant 0,$$

the lifting of P is unique.

PROPOSITION 4.9. *Let P belong to $S(\mathbf{Q})$. Then there exists a unique $\boldsymbol{m}$ in Σ such that P belongs to $\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}))$.*

Proof. Let $Q = (x, y, t, u, v) \in \mathscr{T}_{\mathrm{spl}}(\mathbf{Z})$ be such that $\pi_{\mathrm{spl}}(Q) = P$. Without loss of generality we may assume that $Q = (x, y, t, u, v) \in \mathbf{Z}^5$ is such that

$$\begin{cases} x^2 + y^2 = t^2 \prod_{j=1}^{4} L_j(u,v), \\ \gcd(x,y,t) = 1, \ \gcd(u,v) = 1, \\ t > 0, \ L_1(u,v) \geqslant 0, \ \text{and} \ \prod_{j=2}^{4} L_j(u,v) \geqslant 0. \end{cases} \tag{4.8}$$

The fact that $t^2 \prod_{j=1}^{4} L_j(u,v)$ is the sum of two squares implies that

$$\prod_{j=1}^{4} L_j(u,v) \geqslant 0 \tag{4.9}$$

and, if $\prod_{j=1}^{4} L_j(u,v) \neq 0$, for any prime p congruent to 3 modulo 4,

$$\sum_{j=1}^{4} v_p(L_j(u,v)) \equiv 0 \bmod 2. \tag{4.10}$$

Let j belong to $\{1,2,3,4\}$. If $L_j(u,v) \neq 0$, we denote by $\epsilon_j \in \{-1,+1\}$ the sign of $L_j(u,v)$ and by $\Sigma_j(Q)$ the set of prime numbers p which are congruent to 3 modulo 4 and such that $v_p(L_j(u,v))$ is odd. We then put

$$m_j = \epsilon_j \times \prod_{p \in \Sigma_j(Q)} p.$$

If $L_j(u,v) = 0$, we define m_j as the only integer in Σ_j such that $\prod_{k=1}^{4} m_k$ is a square. By construction, we have $m_j \mid L_j(u,v)$ and the quotient $L_j(u,v)/m_j$ is the sum of two squares.

Let us now check that $\boldsymbol{m} = (m_1, m_2, m_3, m_4)$ belongs to Σ. According to (4.10), if a prime number belongs to $\Sigma_j(Q)$ for some $j \in \{1,2,3,4\}$, then there exists $k \in \{1,2,3,4\}$ with $k \neq j$ such that $p \in \Sigma_k(Q)$. In particular, p divides both $L_j(u,v)$ and $L_k(u,v)$ as well as

$$\Delta_{j,k} u = b_k L_j(u,v) - b_j L_k(u,v)$$

and $\Delta_{j,k}v$. Since $\gcd(u,v)=1$, we get $p \mid \Delta_{j,k}$. Thus $\boldsymbol{m} \in \prod_{j=1}^{4} \Sigma_j$. But combining (4.9), (4.10), and the definition of $\boldsymbol{m}$ we get that $\prod_{j=1}^{4} m_j$ is a square. If d divides all the m_j, it divides $\gcd_{1\leqslant j<k\leqslant 4}(\Delta_{j,k})$ which is equal to 1 since $\Delta_{1,2}=1$ under condition (3.1). Finally $m_1>0$ since $L_1(u,v)>0$ or $\prod_{j=2}^{4} L_j(u,v)>0$. Thus, $\boldsymbol{m}$ belongs to Σ.

We now wish to prove that Q belongs to $\hat{\pi}_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}))$. By construction of $\boldsymbol{m}$, for any j in $\{1,2,3,4\}$, the integer $L_j(u,v)/m_j$ is the sum of two squares. Moreover if p is a prime number, congruent to 3 modulo 4, then p generates a prime ideal of $\mathbf{Z}[i]$. From relations (4.8), if $p \mid t$, then $p \mid (x+iy)(x-iy)$. In that case we have $p \mid x$ and $p \mid y$, which contradicts the fact that $\gcd(x,y,t)=1$. As $t>0$, we get that t may also be written as the sum of two squares.

If $\prod_{j=1}^{4} L_j(u,v) \neq 0$, we choose for $j \in \{1,2,3\}$ an element $z_j^+ \in \mathbf{Z}[i]$ such that $L_j(u,v)/m_j = z_j^+ \overline{z_j^+}$ and an element $z_0^+ \in \mathbf{Z}[i]$ such that $t = z_0^+ \overline{z_0^+}$. Then we get the relation

$$L_4(u,v)/m_4 = \left(\frac{x+iy}{\alpha_{\boldsymbol{m}}(z_0^+)^2 \prod_{j=1}^{3} z_j^+}\right) \overline{\left(\frac{x+iy}{\alpha_{\boldsymbol{m}}(z_0^+)^2 \prod_{j=1}^{3} z_j^+}\right)},$$

and we put $z_4^+ = (x+iy)/(\alpha_{\boldsymbol{m}}(z_0^+)^2 \prod_{j=1}^{3} z_j^+) \in \mathbf{Q}[i]$. If $\prod_{j=1}^{4} L_j(u,v)=0$, we choose z_1^+, z_2^+, z_3^+, z^+ as above and $z_4^+ \in \mathbf{Z}[i]$ such that $L_4(u,v)/m_4 = z_4^+\overline{z_4^+}$. In both cases, we put $z_j^- = \overline{z_j^+}$ for $j \in \{1,2,3,4\}$ and $z_0^- = \overline{z_0^+}$.

The family so constructed satisfy relations (4.5) and (4.8), from which it follows that the corresponding family $(z_\delta)_{\delta\in\boldsymbol{\Delta}}$ is a solution to the systems (4.2) and (4.3). Thus we obtain a point R in $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q})$ such that $\pi_{\boldsymbol{m}}(R)=P$.

Let $\boldsymbol{m}'$ belong to Σ and assume that the point P belongs to the set $\pi_{\boldsymbol{m}'}(\mathcal{T}_{\boldsymbol{m}'}(\mathbf{Q}))$ as well. Then by (4.8), for any prime number p, we have

$$v_p(m'_j) - v_p(m'_k) = v_p(L_j(u,v)) - v_p(L_k(u,v)) = v_p(m_j) - v_p(m_k)$$

for any j,k in $\{1,2,3,4\}$ such that $L_j(u,v)L_k(u,v) \neq 0$. Similarly, denoting by $\operatorname{sgn}(m)$ the sign of an integer m, we have

$$\operatorname{sgn}(m'_j)/\operatorname{sgn}(m'_k) = \operatorname{sgn}(m_j)/\operatorname{sgn}(m_k).$$

These relations between $\boldsymbol{m}$ and $\boldsymbol{m}'$ remain valid if $L_j(u,v)L_k(u,v)=0$ since the products $\prod_{j=1}^{4} m_j$ and $\prod_{j=1}^{4} m'_j$ are squares. But, by definition of Σ, we have

$$m'_1 > 0 \quad \text{and} \quad \min_{1\leqslant j\leqslant 4} v_p(m'_j) = 0$$

for any prime number p, and similarly for $\boldsymbol{m}$. We obtain that $\boldsymbol{m} = \boldsymbol{m}'$. $\square$

5. **Jumping up**

Having constructed the required versal torsors explicitly, we now wish to lift our initial counting problem to these torsors. In order to do this, we shall define an adelic domain $\mathscr{D}_{\boldsymbol{m}}$ in the adelic space $\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})$ so that for any $P \in \pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}))$, the cardinality of $\pi_{\boldsymbol{m}}^{-1}(P) \cap \mathscr{D}_{\boldsymbol{m}}$ is $\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}$.

5.1. *Idelic preliminaries.* We first need to gather a few facts about the adelic space $T_{\mathrm{NS}}(\boldsymbol{A}_{\mathbf{Q}})$.

Notation 5.1. Let A be a commutative ring. We may identify the A-points of $\mathbf{A}_{\boldsymbol{\Delta}}$ with the elements of the invariant ring

$$A_{\boldsymbol{\Delta}} = \Big(\prod_{\delta \in \boldsymbol{\Delta}} A \otimes_{\mathbf{Z}} \mathbf{Z}[i]\Big)^{\mathscr{G}}.$$

Let $\mathscr{P}$ be the set of prime numbers.

Let $p \in \mathscr{P}$. We put $\mathcal{S}_p = \mathrm{Spec}(\mathbf{Q}_p \otimes_{\mathbf{Z}} \mathbf{Z}[i])$ which we may identify with the set of places of $\mathbf{Q}[i]$ above p. If $\boldsymbol{a} = (a_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{S}_p}$ and $\boldsymbol{b} = (b_{\mathfrak{p}})_{\mathfrak{p} \in \mathcal{S}_p}$ belong to $\mathbf{Z}^{\mathcal{S}_p}$, we write $\boldsymbol{a} \geqslant \boldsymbol{b}$ if $a_{\mathfrak{p}} \geqslant b_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathcal{S}_p$ and $\min(\boldsymbol{a}, \boldsymbol{b}) = (\min(a_{\mathfrak{p}}, b_{\mathfrak{p}}))_{\mathfrak{p} \in \mathcal{S}_p}$. The valuations induce a map

$$\widehat{v}_p : \mathbf{Q}_p \otimes_{\mathbf{Z}} \mathbf{Z}[i] \longrightarrow (\mathbf{Z} \cup \{\infty\})^{\mathcal{S}_p}.$$

Thus we get a natural map

$$(\mathbf{Q}_p \otimes_{\mathbf{Z}} \mathbf{Z}[i])^{\boldsymbol{\Delta}} \longrightarrow (\mathbf{Z} \cup \{\infty\})^{\mathcal{S}_p \times \boldsymbol{\Delta}}.$$

The action of $\mathscr{G}$ on $\mathcal{S}_p$ and $\boldsymbol{\Delta}$ induces an action of $\mathscr{G}$ on the set on the right-hand side so that the above map is $\mathscr{G}$-equivariant. Denoting by $\overline{\Gamma}_p$ the set of invariants in $(\mathbf{Z} \cup \{\infty\})^{\mathcal{S}_p \times \boldsymbol{\Delta}}$ and by Γ_p its intersection with $\mathbf{Z}^{\mathcal{S}_p \times \boldsymbol{\Delta}}$, we get a map

$$\log_p : \mathbf{A}_{\boldsymbol{\Delta}}(\mathbf{Q}_p) \longrightarrow \overline{\Gamma}_p$$

whose restriction to $T_{\boldsymbol{\Delta}}(\mathbf{Q}_p)$ is a morphism from this group to the group Γ_p and $\log_p$ is compatible with the action of $T_{\boldsymbol{\Delta}}(\mathbf{Q}_p)$ on the left and the action of Γ_p on the right. We denote by Ξ_p the set of elements $(r_{\mathfrak{p},\delta})$ of Γ_p such that $r_{\mathfrak{p},\delta} \geqslant 0$ for any $\mathfrak{p} \in \mathcal{S}_p$ and any $\delta \in \boldsymbol{\Delta}$.

If T is an algebraic torus over $\mathbf{Q}$ which splits over $\mathbf{Q}(i)$, then $X^*(T)$ denotes the group of characters of T over $\mathbf{Q}(i)$ and $X_*(T) = \mathrm{Hom}(X^*(T), \mathbf{Z})$ its dual, that is the group of cocharacters of T. We denote by $\langle\cdot,\cdot\rangle$ the natural pairing $X^*(T) \times X_*(T) \to \mathbf{Z}$. For any place v of $\mathbf{Q}$, we denote by $X_*(T)_v$ the group of cocharacters of T over $\mathbf{Q}_v$, which may be described as $X_*(T)^{\mathrm{Gal}(\overline{\mathbf{Q}}_v/\mathbf{Q}_v)}$. We also consider the groups $X_*(T)_{\mathbf{Q}} = X_*(T)^{\mathscr{G}}$ and $X^*(T)_{\mathbf{Q}} = X^*(T)^{\mathscr{G}}$. The group Γ_p may then be seen as the group $X_*(T_{\boldsymbol{\Delta}})_p$. The restriction of $\log_p$ from $T_{\boldsymbol{\Delta}}(\mathbf{Q}_p)$ to Γ_p is then the natural morphism defined in [Ono61, §2.1]. For any $(\boldsymbol{r}_\delta)_{\delta \in \boldsymbol{\Delta}} \in \Gamma_p$, we put $\boldsymbol{r}_j^{\pm} = \boldsymbol{r}_{D_j^{\pm}}$ for $j \in \{1,2,3,4\}$ and $\boldsymbol{r}_0^{\pm} = \boldsymbol{r}_{E^{\pm}}$. The group $X_*(T_{\mathrm{NS}})_p$ is then the subgroup of Γ_p given by the equations

$$\boldsymbol{r}_j^{+} + \boldsymbol{r}_j^{-} = \boldsymbol{r}_l^{+} + \boldsymbol{r}_l^{-}$$

for $1 \leqslant j < l \leqslant 4$ and

$$\boldsymbol{r}_0^+ + \boldsymbol{r}_j^+ + \boldsymbol{r}_l^+ = \boldsymbol{r}_0^- + \boldsymbol{r}_m^- + \boldsymbol{r}_n^-$$

if $\{j, l, m, n\} = \{1, 2, 3, 4\}$.

Remarks 5.2. (i) If $p \equiv 3 \bmod 4$ or $p = 2$, then there exists a unique element $\mathfrak{p}$ in $\mathcal{S}_p$. Thus Γ_p is canonically isomorphic to $\mathbf{Z}^{\boldsymbol{\Delta}_\mathbf{Q}}$. If $p \equiv 1 \bmod 4$, then choosing an element $\mathfrak{p} \in \mathcal{S}_p$, we get an isomorphism from $\mathbf{Z}^{\boldsymbol{\Delta}}$ to Γ_p.

(ii) We may note that an element $Q \in \mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ belongs to $\mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p)$ if and only if $\log_p(Q)$ belongs to Ξ_p.

LEMMA 5.3. *For any prime* p, *the morphism* $\log_p$ *induces an isomorphism from the quotient* $T_{\mathrm{NS}}(\mathbf{Q}_p)/T_{\mathrm{NS}}(\mathbf{Z}_p)$ *to* $X_*(T_{\mathrm{NS}})_p$ *and there is an exact sequence*

$$1 \longrightarrow T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}} \longrightarrow T_{\mathrm{NS}}(\mathbf{Q}) \longrightarrow \bigoplus_{p \in \mathscr{P}} X_*(T_{\mathrm{NS}})_p \longrightarrow 0.$$

Proof. By [Dra71, p. 449], the kernel of the map $\log_p$ from $T_{\mathrm{NS}}(\mathbf{Q}_p)$ to $X_*(T_{\mathrm{NS}})_p$ coincides with $T_{\mathrm{NS}}(\mathbf{Z}_p)$ for any prime p. Let us prove that the map $\bigoplus_p \log_p$ from $T_{\mathrm{NS}}(\mathbf{Q})$ to $\bigoplus_p X_*(T_{\mathrm{NS}})_p$ is surjective. We first assume that $p \neq 2$. If $p \equiv 1 \bmod 4$, we choose an element $\varpi \in \mathbf{Z}[i]$ such that $p = \varpi\overline{\varpi}$ and identify $\mathcal{S}_p$ with $\{\varpi, \overline{\varpi}\}$. If $\boldsymbol{r} \in \Gamma_p$, we then define

$$\exp_\varpi(\boldsymbol{r}) = (\varpi^{r_{\varpi,\delta}}\overline{\varpi}^{r_{\overline{\varpi},\delta}})_{\delta \in \boldsymbol{\Delta}}.$$

If $p \equiv 3 \bmod 4$, then we put $\varpi = p$ and for $\boldsymbol{r} \in \Gamma_p$, we define $\exp_\varpi(\boldsymbol{r})$ to be $(\varpi^{r_{p,\delta}})_{\delta \in \boldsymbol{\Delta}}$. By construction, $\exp_\varpi$ is a morphism from Γ_p to $T_{\boldsymbol{\Delta}}(\mathbf{Q})$ and satisfies $\log_p \circ \exp_\varpi = \mathrm{Id}_{\Gamma_p}$ and $\log_\ell \circ \exp_\varpi = 0$ for any prime $\ell \neq p$. Moreover we have

$$\chi(\exp_\varpi(\boldsymbol{r})) = p^{\langle \chi, \boldsymbol{r} \rangle} \tag{5.1}$$

for any $\chi \in X^*(T_{\boldsymbol{\Delta}})_{\mathbf{Q}}$ and any $\boldsymbol{r} \in \Gamma_p$. Therefore, if $\boldsymbol{r}$ belongs to $X_*(T_{\mathrm{NS}})_p$, then $\exp_\varpi(\boldsymbol{r})$ belongs to $T_{\mathrm{NS}}(\mathbf{Q})$. It remains to prove a similar result for $p = 2$, although there is no morphism which satisfies (5.1). Let $\boldsymbol{r}$ belong to $X_*(T_{\mathrm{NS}})_2$. Let us write $r_j = r_j^+ = r_j^-$ for j in $\{0, \dots, 4\}$. Since $\boldsymbol{r}$ belong to $X_*(T_{\mathrm{NS}})_2$, we have $r_1 = r_2 = r_3 = r_4$. We put $z_j^+ = (1+i)^{r_j}$ for $j \in \{0, 1, 2, 3\}$ and $z_4^+ = (-i)^{r_0 + 2r_1}(1+i)^{r_0}$ and $z_j^- = \overline{z}_j^+$ for $j \in \{0, \dots, 4\}$. Then $\log_2(\boldsymbol{z}) = \boldsymbol{r}$ and $\boldsymbol{z}$ satisfies equation (4.6). Moreover if $\{j, k, l, m\} = \{1, 2, 3, 4\}$, then one has

$$z_0^+ z_j^+ z_k^+ / (z_0^- z_l^- z_m^-) = \frac{(1+i)^{r_0 + 2r_1}}{(1-i)^{r_0 + 2r_1}} (-i)^{r_0 + 2r_1} = 1$$

which proves that $\boldsymbol{z}$ satisfies (4.7).

If $\boldsymbol{z}$ belongs to the kernel of the map $\bigoplus_p \log_p$, then its coordinates are invertible elements in $\mathbf{Z}[i]$. Thus $\boldsymbol{z}$ is a torsion element of $T_{\mathrm{NS}}(\mathbf{Q})$. □

5.2. *Local domains.* To construct $\mathscr{D}_{\boldsymbol{m}}$, for any prime p and any $\boldsymbol{m} \in \Sigma$ we shall define a fundamental domain in $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ under the action of $T_{\mathrm{NS}}(\mathbf{Q}_p)$ modulo $T_{\mathrm{NS}}(\mathbf{Z}_p)$. In other words, we want an open domain $\mathscr{D}_{\boldsymbol{m},p} \subset \mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ such that:

(i) The open set $\mathscr{D}_{\boldsymbol{m},p}$ is stable under the action of $T_{\mathrm{NS}}(\mathbf{Z}_p)$.
(ii) For any t in $T_{\mathrm{NS}}(\mathbf{Q}_p) - T_{\mathrm{NS}}(\mathbf{Z}_p)$, one has $t.\mathscr{D}_{\boldsymbol{m},p} \cap \mathscr{D}_{\boldsymbol{m},p} = \emptyset$.
(iii) For any x in $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$, there exists an element t in $T_{\mathrm{NS}}(\mathbf{Q}_p)$ such that x belongs to $t.\mathscr{D}_{\boldsymbol{m},p}$.

LEMMA 5.4. *For any prime number p, the domain $\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)$ is a fundamental domain in $\mathscr{T}_{\mathrm{spl}}(\mathbf{Q}_p)$ under the action of $T_{\mathrm{spl}}(\mathbf{Q}_p)$ modulo $T_{\mathrm{spl}}(\mathbf{Z}_p)$.*

Proof. As in the proof of Lemma 4.7, if P belongs to $S(\mathbf{Q}_p)$, then there exists a point $Q = (x, y, t, u, v) \in \mathscr{T}_{\mathrm{spl}}(\mathbf{Q}_p)$ such that $\pi_{\mathrm{spl}}(Q) = P$ and

$$\min(v_p(x), v_p(y), v_p(t)) = \min(v_p(u), v_p(v)) = 0.$$

The last condition is equivalent to $Q \in \mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)$. The lemma then follows from the facts that the action of $T_{\mathrm{spl}}(\mathbf{Q}_p)$ on $\mathscr{T}_{\mathrm{spl}}(\mathbf{Q}_p)$ is given by

$$((\lambda, \mu), (x, y, t, u, v)) \mapsto (\lambda x, \lambda y, \mu^{-2}\lambda t, \mu u, \mu v)$$

and $T_{\mathrm{spl}}(\mathbf{Q}_p)$-orbits are the fibers of the projection $\pi_{\mathrm{spl}} : \mathscr{T}_{\mathrm{spl}}(\mathbf{Q}_p) \to S(\mathbf{Q}_p)$. $\square$

LEMMA 5.5. *Two elements of $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ belong to the same orbit under the action of $T_{\mathrm{NS}}(\mathbf{Z}_p)$ if and only if they have the same image by $\pi_{\boldsymbol{m}}$ and $\log_p$.*

Proof. According to Proposition 4.6, two elements of $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ belong to the same orbit under the action of $T_{\mathrm{NS}}(\mathbf{Q}_p)$ if and only if their image by $\pi_{\boldsymbol{m}}$ coincide. On the other hand, $T_{\mathrm{NS}}(\mathbf{Z}_p) = T_{\mathrm{NS}}(\mathbf{Q}_p) \cap T_{\boldsymbol{\Delta}}(\mathbf{Z}_p)$ is the set of elements of $\mathbf{A}_{\boldsymbol{\Delta}}(\mathbf{Q}_p)$ which are sent to the origin of Γ_p by $\log_p$. Therefore if two elements of $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ belong to the same orbit for $T_{\mathrm{NS}}(\mathbf{Z}_p)$, their image in $\overline{\Gamma}_p$ coincides. Conversely, let x and y be elements of $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ which have the same image by $\pi_{\boldsymbol{m}}$ and $\log_p$. Then there exists an element $t \in T_{\mathrm{NS}}(\mathbf{Q}_p)$ such that $y = tx$. Since $\log_p(x) = \log_p(y)$, if a coordinate z_δ of x is different from 0, the corresponding component of $\log_p(t)$ is 0. Taking into account conditions (4.3) and equations (4.6) and (4.7) which define T_{NS}, this implies that $\log_p(t)$ is the unit element and thus $t \in T_{\mathrm{NS}}(\mathbf{Z}_p)$. $\square$

Remark 5.6. The idea behind the construction of $\mathscr{D}_{\boldsymbol{m},p}$ is first to consider the intersection

$$\widehat{\pi}_m^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)) \cap \mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p),$$

which is stable under the action of $T_{\mathrm{NS}}(\mathbf{Z}_p)$. For all primes p for which there is good reduction, this intersection coincides with $\mathscr{T}_{\boldsymbol{m}}(\mathbf{Z}_p)$. More generally, if p is good or if $p \not\equiv 1 \bmod 4$, this intersection satisfies conditions (i)–(iii) and yields the wanted domain. On the other hand, if p is a prime dividing one of the $\Delta_{j,k}$ and such that $p \equiv 1 \bmod 4$, then for any $Q \in \mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p) \cap \widehat{\pi}_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p))$, the intersection

$$\widehat{\pi}_{\boldsymbol{m}}^{-1}(Q) \cap \mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p)$$

is the union of a finite number of $T_{\mathrm{NS}}(\mathbf{Z}_p)$-orbits. We then select a total order on Γ_p and choose the minimal element in the image of the last intersection by ϕ_p. In that way, we construct the wanted domain.

To better understand the construction, we describe the conditions satisfied by $\log_p(R)$ for a lifting R of a point $Q \in \mathcal{T}_{\mathrm{spl}}(\mathbf{Q}_p)$. Let $R = (z_\delta)_{\delta \in \boldsymbol{\Delta}} \in \mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ and let $Q = (x, y, t, u, v) = \widehat{\pi}_{\boldsymbol{m}}(R)$. Let us denote by $(\boldsymbol{r}_\delta)_{\delta \in \boldsymbol{\Delta}} \in \overline{\Gamma}_p$ the image of R by $\log_p$. We also put $\boldsymbol{n}_j = \widehat{v}_p(L_j(u,v)/m_j)$ for $j \in \{1,2,3,4\}$, $\boldsymbol{n}_0 = \widehat{v}_p(t)$, and $\boldsymbol{n}^{\pm} = \widehat{v}_p((x \pm iy)/\alpha_{\boldsymbol{m}})$. Then we have the relations

$$\boldsymbol{n}_j = \boldsymbol{r}_j^+ + \boldsymbol{r}_j^- \tag{5.2}$$

for $j \in \{0, \dots, 4\}$, and

$$\boldsymbol{n}^{\pm} = 2\boldsymbol{r}_0^{\pm} + \sum_{j=1}^{4} \boldsymbol{r}_j^{\pm}. \tag{5.3}$$

Lemma 5.7. *Let p be a prime number and let $\boldsymbol{m}$ belong to Σ. Let Q belong to the intersection $\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p) \cap \pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p))$ and let $(\boldsymbol{n}_j)_{j \in \{0,\dots,4\}}$ and $\boldsymbol{n}^+, \boldsymbol{n}^-$ be the corresponding elements of $\mathbf{Z}^{\mathcal{S}_p}$ defined in Remark 5.6.*

(a) *One has $\boldsymbol{n}_j \geqslant 0$ for $j \in \{0, \dots, 4\}$, $\boldsymbol{n}^+ \geqslant 0$ and $\boldsymbol{n}^- \geqslant 0$.*
(b) *If $p \notin \mathcal{S}$, then $\min(\boldsymbol{n}_i, \boldsymbol{n}_j) = 0$ if $1 \leqslant i < j \leqslant 4$.*
(c) *If $p \not\equiv 1 \bmod 4$, then $\boldsymbol{n}_0 = 0$.*
(d) *One has $\min(\boldsymbol{n}_0, \boldsymbol{n}^+, \boldsymbol{n}^-) = 0$.*
(e) *There exists a solution in Ξ_p to equations (5.2) and (5.3).*
(f) *The number of such solutions is finite.*
(g) *There exists a unique solution to these equations in Ξ_p if $p \notin \mathcal{S}$ or if $p \not\equiv 1 \bmod 4$.*

Proof. We write $\boldsymbol{m} = (m_1, \dots, m_4)$ and $Q = (x, y, t, u, v)$. As Q belongs to the set $\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p))$, one has that $p | m_i$ if and only if $p \equiv 3 \bmod 4$ and $v_p(L_i(u,v))$ is odd. If these conditions are verified, $v_p(\alpha_{\boldsymbol{m}}) = 1$ and $\alpha_{\boldsymbol{m}} | L_i(u,v)$. Similarly, using equation (4.1), we have that $\alpha_{\boldsymbol{m}} | x \pm iy$ and this concludes the proof of a).

We now assume that $p \notin \mathcal{S}$. Let i, j be such that $1 \leqslant i < j \leqslant 4$. Thus p does not divide $\Delta_{i,j}$. This implies that $\min(v_p(L_i(u,v)), v_p(L_j(u,v))) = 0$ and so $\min(\boldsymbol{n}_i, \boldsymbol{n}_j) = 0$.

We now prove assertion (c). If $p | t$, then by equation (4.1), it follows that $p^2 | x^2 + y^2$. If we assume that $p = 2$ or $p \equiv 3 \bmod 4$, then this implies that $p | x$ and $p | y$ which contradicts the fact that $\min(v_p(x), v_p(y), v_p(t)) = 0$.

Let $\mathfrak{p} \in \mathcal{S}_p$. If $\mathfrak{p}$ divides $x+iy$, $x-iy$, and t, then p divides x, y and t. This proves assertion (d).

Since Q belongs to $\pi_{\boldsymbol{m}}(\mathcal{T}(\mathbf{Q}_p))$, equations (5.2) and (5.3) have a solution in Γ_p. If $p \equiv 3 \bmod 4$ or $p=2$, then the integers $r_j^{\pm} \in \mathbf{Z}$ are such that $r_j^+ = r_j^-$ for $j \in \{0,\dots,4\}$. Therefore the equations in (5.2) have a unique solution in Γ_p. By (a) the coordinates of this solution are positive. If $p \equiv 1 \bmod 4$, then by choosing an element $\mathfrak{p} \in \mathcal{S}_p$ we are reduced to solving the equations

$$n_j = r_j^+ + r_j^-$$

for $j \in \{0,\dots,4\}$, and

$$n^{\pm} = 2r_0^{\pm} + \sum_{j=1}^{4} r_j^{\pm}$$

in $\mathbf{Z}^{\boldsymbol{\Delta}}$, where $n_j \geqslant 0$ for $j \in \{0,\dots,4\}$, $n^+ \geqslant 0$ and $n^- \geqslant 0$. Since we have the relation $2n_0 + \sum_{j=1}^4 n_j = n^+ + n^-$, we may write $n^+ = 2a_0^+ + \sum_{j=1}^4 a_j^+$ where $0 \leqslant a_j^+ \leqslant n_j$ for $j \in \{0,\dots,4\}$. Then we put $a_j^- = n_j - a_j^+$ for $j \in \{0,\dots,4\}$ to get a solution with nonnegative coordinates.

Assertion (f) follows from the fact that there is only a finite number of nonnegative integral solutions to an equation of the form $n = k^+ + k^-$.

If $p \equiv 3 \bmod 4$ or $p = 2$, we have already seen that the solution to the system of equations is unique. If $p \notin \mathcal{S}$ and $p \equiv 1 \bmod 4$, then it follows from assertions (b) and (d) that $r_j^{\pm} = \min(n_j, n^{\pm})$, which implies that the solution is unique. □

LEMMA 5.8. *If p is a prime number such that $p \equiv 1 \bmod 4$ or $p \notin \mathcal{S}$, then for $\boldsymbol{m} \in \Sigma$, the set $\mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p) \cap \widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p))$ satisfies the conditions* (i)–(iii) *and defines a fundamental domain in $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ under the action of $T_{\mathrm{NS}}(\mathbf{Z}_p)$.*

Proof. To prove the lemma it is sufficient to prove that the intersection of any nonempty fiber of $\pi_{\boldsymbol{m}}$ with $\mathscr{T}_{\boldsymbol{m}}(\mathbf{Z}_p)$ is not empty and is an orbit under the action of $T_{\mathrm{NS}}(\mathbf{Z}_p)$. Let P belong to the set $\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p))$. By Lemma 5.4 we may lift P to a point Q which belongs to $\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)$. According to Lemma 5.7(e), we may find an element $\boldsymbol{r} \in \Xi_p$ which is a solution to equations (5.2) and (5.3). Let R' be any lifting of P to $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ and let $\boldsymbol{r}' = \log_p(R')$. The difference $\boldsymbol{r}'-\boldsymbol{r}$ belongs to $X_*(T_{\mathrm{NS}})_p$. According to Lemma 5.3, there exists $t \in T_{\mathrm{NS}}(\mathbf{Q}_p)$ such that $\log_p(t) = \boldsymbol{r} - \boldsymbol{r}'$. Then the point $R = t.R' \in \mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ satisfies $\log_p(R) = \boldsymbol{r}$ and R belongs to $\mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p) \cap \widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p))$.

It remains to prove that if two element R and R' of $\mathscr{T}_{\boldsymbol{m}}(\mathbf{Z}_p)$ are in the same fibre for $\pi_{\boldsymbol{m}}$, then they belong to the same orbit under the action of $T_{\mathrm{NS}}(\mathbf{Z}_p)$. Their images in $\mathscr{T}_{\mathrm{spl}}(\mathbf{Q}_p)$ belong to $\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)$ and therefore are contained in the same orbit for the action of $T_{\mathrm{spl}}(\mathbf{Z}_p)$, which means that the equations described in Remark 5.6 for $\log_p(R)$ and $\log_p(R')$ are exactly the same. We then apply assertion (g) of Lemma 5.7 and Lemma 5.5. □

LEMMA 5.9. *If the prime number* p *does not belong to* $\mathcal{S}$, *then for* $\boldsymbol{m} \in \Sigma$, *we have*

$$\mathscr{T}_{\boldsymbol{m}}(\mathbf{Z}_p) = \mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p) \cap \widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)).$$

Proof. We keep the notation used in the proof of the previous lemma. Using Lemma 5.7(b) and (d), and the positivity of the coefficients in $\boldsymbol{r}$, we get that $\min(\boldsymbol{r}_{\delta_1}, \boldsymbol{r}_{\delta_2}) = 0$ whenever $\delta_1 \cap \delta_2 = \emptyset$, which means that R belongs to $\mathscr{T}_{\boldsymbol{m}}(\mathbf{Z}_p)$. □

Definition 5.10. Let $\boldsymbol{m}$ belong to Σ. If $p \notin \mathcal{S}$, we put $\mathscr{D}_{\boldsymbol{m},p} = \mathscr{T}_{\boldsymbol{m}}(\mathbf{Z}_p)$. If $p \in \mathcal{S}$ and $p \not\equiv 1 \bmod 4$, we put

$$\mathscr{D}_{\boldsymbol{m},p} = \mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p) \cap \widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)).$$

It remains to define the domain for the primes $p \in \mathcal{S}$ such that $p \equiv 1 \bmod 4$.

Notation 5.11. We put $\mathcal{S}' = \{p \in \mathcal{S},\ p \equiv 1 \bmod 4\}$. For any $p \in \mathcal{S}'$, we fix in the remainder of this text a decomposition $p = \varpi_p \overline{\varpi_p}$ for an irreducible element $\varpi_p \in \mathbf{Z}[i]$. We may then write $\mathcal{S}_p = \{\varpi_p, \overline{\varpi_p}\}$. The group Γ_p is isomorphic to $\mathbf{Z}^{\boldsymbol{\Delta}}$ through the map ϕ_p which applies a family $(r_{\mathfrak{p},\delta})_{(\mathfrak{p},\delta) \in \mathcal{S}_p \times \boldsymbol{\Delta}}$ onto the family $(r_{\varpi_p,\delta})_{\delta \in \boldsymbol{\Delta}}$. Let $j \neq k$ be two elements of $\{1,2,3,4\}$ such that $p | \Delta_{j,k}$. We then define $\boldsymbol{f}_{j,k} = (f_\delta)_{\delta \in \Delta} \in \mathbf{Z}^{\boldsymbol{\Delta}}$ by

$$f_\delta = \begin{cases} 1 \text{ if } \delta \in \{D_j^-, D_k^+\}, \\ 0 \text{ otherwise.} \end{cases}$$

We put $\boldsymbol{e}_{j,k} = \phi_p^{-1}(\boldsymbol{f}_{j,k})$ and consider the set

$$\Lambda_p = \Xi_p - \bigcup_{\{(j,k) \in \{1,2,3,4\} | j<k \text{ and } p | \Delta_{j,k}\}} \boldsymbol{e}_{j,k} + \Xi_p. \tag{5.4}$$

Definition 5.12. Let $\boldsymbol{m}$ belong to Σ. If $p \in \mathcal{S}$ and $p \equiv 1 \bmod 4$, then we define $\mathscr{D}_{\boldsymbol{m},p}$ to be the set of $R \in \widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p))$ such that $\log_p(R) \in \Lambda_p$.

Remark 5.13. In particular, one has $\mathscr{D}_{\boldsymbol{m},p} \subset \mathscr{Y}_{\boldsymbol{m}}(\mathbf{Z}_p)$ for any prime number p.

LEMMA 5.14. *If* $p \in \mathcal{S}$ *and* $p \equiv 1 \bmod 4$, *then for* $\boldsymbol{m} \in \Sigma$, *the set* $\mathscr{D}_{\boldsymbol{m},p}$ *satisfies conditions* (i)–(iii) *and defines a fundamental domain in* $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ *under the action of* $T_{\mathrm{NS}}(\mathbf{Z}_p)$.

Proof. According to Lemma 5.5 and Lemma 5.7(e), we have only to prove that for any $Q \in \mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p) \cap \widehat{\pi}_{\boldsymbol{m}}(\mathcal{T}_p)$, there exist a unique solution of equations (5.2) and (5.3) which belongs to Λ_p. Among the solutions in Ξ_p, there is a unique solution such that if $\boldsymbol{s} = \phi_p(\boldsymbol{r})$, the quadruple $(s_1^+, s_2^+, s_3^+, s_4^+)$ is maximal for the lexicographic order. It remains to prove that the solution satisfies this last condition if and only if $\boldsymbol{r}$ belongs to Λ_p. Let $\boldsymbol{r}$ be the solution for which the above quadruple is maximal and $\widetilde{\boldsymbol{r}}$ be any solution in Ξ_p and $\widetilde{\boldsymbol{s}} = \phi_p(\widetilde{\boldsymbol{r}})$. If $\boldsymbol{r} \neq \widetilde{\boldsymbol{r}}$, then we consider the smallest $j \in \{1,2,3,4\}$ such that $s_j^+ > \widetilde{s}_j^+$. With the notation of Remark 5.6, this implies that $\boldsymbol{n}_j \neq 0$, $\boldsymbol{n}^+ \neq 0$, and $\boldsymbol{n}^- \neq 0$. Therefore $\boldsymbol{n}_0 = 0$ and there exists $k > j$ such that $s_k^+ < \widetilde{s}_k^+$. Since $s_j^- < \widetilde{s}_j^-$, we may conclude that $\widetilde{\boldsymbol{r}} \in \boldsymbol{e}_{j,k} + \Xi_p$. Moreover $p \mid \Delta_{j,k}$. Conversely if $\widetilde{\boldsymbol{r}}$ belongs to $\boldsymbol{e}_{j,k} + \Xi_p$ for some $j,k \in \{1,2,3,4\}$ such that $j < k$, then $\widetilde{\boldsymbol{r}} - \boldsymbol{e}_{j,k} + \boldsymbol{e}_{k,j}$ is another solution to system of equations which gives a bigger quadruple for the lexicographic order. □

5.3. *Adelic domains and lifting of the points.*

Definition 5.15. Let $\boldsymbol{m} \in \Sigma$. We define the open subset $\mathscr{D}_{\boldsymbol{m}}$ of $\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})$ as the product $\mathcal{T}_{\boldsymbol{m}}(\mathbf{R}) \times \prod_{p \in \mathscr{P}} \mathscr{D}_{\boldsymbol{m},p}$.

PROPOSITION 5.16. *The set $\mathscr{D}_{\boldsymbol{m}}$ is a fundamental domain in $\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})$ under the action of $T_{\mathrm{NS}}(\mathbf{Q})$ modulo $T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}$. In other words*:

(i) *The open set $\mathscr{D}_{\boldsymbol{m}}$ is stable under the action of $T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}$.*
(ii) *For any t in $T_{\mathrm{NS}}(\mathbf{Q}) - T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}$, one has $t.\mathscr{D}_{\boldsymbol{m}} \cap \mathscr{D}_{\boldsymbol{m}} = \emptyset$.*
(iii) *For any x in $\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})$, there exists an element t in $T_{\mathrm{NS}}(\mathbf{Q})$ such that x belongs to $t.\mathscr{D}_{\boldsymbol{m}}$.*

Proof. Assertion (i) followssince $\mathscr{D}_{\boldsymbol{m},p}$ is stable under $T_{\mathrm{NS}}(\mathbf{Z}_p)$ for any prime number p. If t belongs to $T_{\mathrm{NS}}(\mathbf{Q}) - T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}$, then, by Lemma 5.3, there exists a prime number p such that $\log_p(t) \neq 0$. Thus $t.\mathscr{D}_{\boldsymbol{m},p} \cap \mathscr{D}_{\boldsymbol{m},p} = \emptyset$, which proves (ii). Let x belong to $\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})$. For any prime number p, there exists an element $t_p \in T_{\mathrm{NS}}(\mathbf{Q}_p)$ such that $t_p.x \in \mathscr{D}_{\boldsymbol{m},p}$. By Lemma 5.3, there exists an element $t \in T_{\mathrm{NS}}(\mathbf{Q})$ such that $\log_p(t) = \log_p(t_p)$ for any prime number p and $t.x \in \mathscr{D}_{\boldsymbol{m}}$. □

COROLLARY 5.17. *Let P belong to $S(\mathbf{Q})$ and let $\boldsymbol{m}$ be the unique element of Σ such that $P \in \pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}))$. Then*

$$\sharp(\pi_{\boldsymbol{m}}^{-1}(P) \cap \mathscr{D}_{\boldsymbol{m}}) = \sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}} = 2^8.$$

Proof. This corollary follows from the last proposition and the fact that $\pi_{\boldsymbol{m}}^{-1}(x)$ is an orbit under the action of $T_{\mathrm{NS}}(\mathbf{Q})$. □

Let us now lift the heights to the versal torsors.

Definition 5.18. As in Notation 3.2 we put $C = \sqrt{\prod_{j=1}^4 |a_j| + |b_j|}$. Let w be a place of $\mathbf{Q}$. We define a function H_w on $\mathbf{Q}_w^5$ by

$$H_w(x,y,t,u,v) = \begin{cases} \max(\frac{|x|_w}{C}, \frac{|y|_w}{C}, \max(|u|_w, |v|_w)^2 |t|_w) & \text{if } w = \infty, \\ \max(|x|_w, |y|_w, \max(|u|_w, |v|_w)^2 |t|_w) & \text{otherwise} \end{cases}$$

for any $(x,y,t,u,v)\in\mathbf{Q}_w^5$. If $\boldsymbol{m}\in\Sigma$, we shall also denote by $H_w:\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_w)\to\mathbf{R}$ the composite function $H_w\circ\widehat{\pi}_{\boldsymbol{m}}$. We then define $H:\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})\to\mathbf{R}$ by $H=\prod_{w\in\mathrm{Val}(\mathbf{Q})}H_w$.

Remarks 5.19. (i) The line bundle ω_S^{-1} defines a character χ_ω on the torus $T_{\mathrm{spl}}=\mathbf{G}_{m,\mathbf{Q}}^2$ simply given by $(\lambda,\mu)\mapsto\lambda$, and we have the relation

$$H_w(t.R)=|\chi_\omega(t)|_w H_w(R) \tag{5.5}$$

for any $t\in T_{\mathrm{spl}}(\mathbf{Q}_w)$ and any $R\in T_{\mathrm{spl}}(\mathbf{Q}_w)$. A similar assertion is true on $\mathcal{T}_{\boldsymbol{m}}$ for $\boldsymbol{m}\in\Sigma$.

(ii) As a point $Q=(x:y:t:u:v)$ in $\mathscr{T}_{\mathrm{spl}}(\mathbf{R})$ satisfies equation (4.1), we have that

$$\max(|x|,|y|)^2\leqslant\prod_{j=1}^{4}(|a_j|+|b_j|)\max(|u|,|v|)^4|t|^2,$$

and it follows that

$$H_\infty(Q)=\max(|u|,|v|)^2|t|.$$

PROPOSITION 5.20. *Let* $\boldsymbol{m}\in\Sigma$. *For any* $R\in\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q})$, *one has*

$$H(\pi_{\boldsymbol{m}}(R))=H(R).$$

Proof. We may define a map $\widehat{\psi}:\mathbf{Q}^5\to\mathbf{Q}^5$ by

$$(x,y,t,u,v)\mapsto(v^2t:uvt:u^2t:x:y).$$

The restriction of the map $\widehat{\psi}$ from $\mathscr{T}_{\mathrm{spl}}$ to $\mathbf{A}_{\mathbf{Q}}^5-\{0\}$ is a lifting of the map $\psi:S\to S'$. On S', the height H_4 is given by

$$H_4(x_0:\cdots:x_4)=\max\left(|x_0|_\infty,|x_1|_\infty,|x_2|_\infty,\frac{|x_3|_\infty}{C},\frac{|x_4|_\infty}{C}\right)\times\prod_{p\in\mathscr{P}}\max_{0\leqslant j\leqslant 4}(|x_j|_p)$$

for any $(x_0,\ldots,x_4)\in\mathbf{Q}^5$. This formula implies the statement of the lemma. □

COROLLARY 5.21. *For any real number* B, *we have*

$$N(B)=\frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}}\sum_{\boldsymbol{m}\in\Sigma}\sharp\{R\in\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q})\cap\mathscr{D}_{\boldsymbol{m}},\ H(R)\leqslant B\}.$$

Proof. This corollary follows from Propositions 4.9, 4.6, 5.20, and Corollary 5.17. □

Remark 5.22. For any prime number p and any $\boldsymbol{m}\in\Sigma$, we have $\mathscr{D}_{\boldsymbol{m},p}$ belonging to $\widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p))$. Therefore, for any $R=(R_w)_{w\in\mathrm{Val}(\mathbf{Q})}$ belonging to $\mathscr{D}_{\boldsymbol{m}}$, we have $H(R)=H_\infty(R_\infty)$.

Notation 5.23. For any real number B, and any $\boldsymbol{m}\in\Sigma$, we denote by $\mathscr{D}_{\boldsymbol{m},\infty}(B)$ the set of $R\in\mathcal{T}_{\boldsymbol{m}}(\mathbf{R})$ such that the point $Q=(x,y,t,u,v)=\widehat{\pi}_{\boldsymbol{m}}(R)$

satisfies the conditions

$$H_\infty(Q) \leqslant B \quad \text{and} \quad H_\infty(Q) \geqslant \max(|u|,|v|)^2 \geqslant 1. \tag{5.6}$$

We define $\mathscr{D}_{\boldsymbol{m}}(B)$ as the product $\mathscr{D}_{\boldsymbol{m},\infty}(B) \times \prod_{p\in\mathscr{P}} \mathscr{D}_{\boldsymbol{m},p}$.

Remark 5.24. Let F be a fiber of the morphism $\pi : S \to \mathbf{P}^1_{\mathbf{Q}}$. Then the Picard group of S is a free $\mathbf{Z}$-module with a basis given by the pair $([F],[\omega_S^{-1}])$. According to formula (5.5), the function H_∞ corresponds to $[\omega_S^{-1}]$. In a similar way the map applying (x,y,t,u,v) to $\max(|u|,|v|)$ corresponds to $[F]$. On the other hand, the cone of effective divisors in $\mathrm{Pic}(S)$ is the cone generated by $[F]$ and $[E^+]+[E^-]=[\omega_S^{-1}]-2[F]$. But, by the preceding remark, the function

$$Q=(x,y,t,u,v) \longmapsto \frac{H_\infty(Q)}{\max(|u|,|v|)^2}$$

corresponds to $[E^+]+[E^-]$. Thus the lower bounds imposed in the definition of $\mathscr{D}_{\boldsymbol{m},\infty}(B)$ correspond to condition (3.9) of [Pey01, p. 268]. These lower bounds are automatically satisfied by any point R in $\mathscr{D}_{\boldsymbol{m}} \cap \mathcal{T}_{\boldsymbol{m}}(\mathbf{Q})$. Indeed $Q=\widehat{\pi}_{\boldsymbol{m}}(R)$ belongs to $\mathscr{T}_{\mathrm{spl}}(\mathbf{Z})$, and writing $Q=(x,y,t,u,v)$ we get that $\max(|u|,|v|)\geqslant 1$. Since $(x,y,t)\neq 0$, by equation (4.1), we also have that $t \neq 0$ and therefore $|t|\geqslant 1$ which yields the second inequality.

Corollary 5.25. *For any real number B, we have*

$$N(B)=\frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\boldsymbol{m}\in\Sigma} \sharp(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}) \cap \mathscr{D}_{\boldsymbol{m}}(B)).$$

Proof. This follows from the last remark and the preceding corollary. □

5.4. *Moebius inversion formula and change of variables.* As is usual with these type of problems, we now wish to use a Moebius inversion formula to replace the coprimality conditions by divisibility conditions.

5.4.1. *First inversion.* The first inversion corresponds to the conditions imposed at the places $p \in \mathcal{S}$ with $p \equiv 1 \bmod 4$.

Notation 5.26. Let $\mathrm{N}(\mathfrak{a}) = \#(\mathbf{Z}[i]/\mathfrak{a})$ denote the norm of an ideal $\mathfrak{a}$ of the ring of Gaussian integers $\mathbf{Z}[i]$. We define

$$\widehat{\mathfrak{D}} = \{\mathfrak{b} \subset \mathbf{Z}[i],\ \mathrm{N}(\mathfrak{b}) \in \mathfrak{D}\},$$

where

$$\mathfrak{D} = \{d \in \mathbf{Z}_{>0},\ p \mid d \Rightarrow p \equiv 1 \bmod 4\}. \tag{5.7}$$

Let A be a commutative ring. Let $\boldsymbol{\mathfrak{b}} = (\mathfrak{b}_\delta)_{\delta\in\boldsymbol{\Delta}}$ be a family of ideals of $A \otimes_{\mathbf{Z}} \mathbf{Z}[i]$ such that $\mathfrak{b}_{\overline{\delta}} = \overline{\mathfrak{b}_\delta}$ for any $\delta \in \boldsymbol{\Delta}$. Then $(\prod_{\delta\in\boldsymbol{\Delta}} \mathfrak{b}_\delta)^{\mathscr{G}}$ is an ideal of $A_{\boldsymbol{\Delta}}$

and for any $\boldsymbol{n}\in\mathbf{Z}^4$, we define

$$\mathscr{Y}_{\boldsymbol{n}}(\mathfrak{b})=\mathscr{Y}_{\boldsymbol{n}}(A)\cap\Big(\prod_{\delta\in\boldsymbol{\Delta}}\mathfrak{b}_\delta\Big)^{\mathscr{G}}.$$

We define $\mathscr{I}_{\boldsymbol{\Delta}}(A)$ as the set of such families of ideals. For any p, the map $\log_p$ induces a map from $\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$ to $\overline{\Gamma}_p$. If $\log_2(\mathfrak{a})=0$, then we define

$$\boldsymbol{\lambda}(\mathfrak{a})=\prod_{p\in\mathscr{P}-\{2\}}\exp_{\varpi_p}(\log_p(\mathfrak{a})).$$

For any $\mathfrak{a}\in\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$, we also put $\mathrm{N}(\mathfrak{a})=(\mathrm{N}(\mathfrak{a}_j^+))_{1\leqslant j\leqslant 4}\in\mathbf{Z}^4_{\geqslant 0}$.

If $\boldsymbol{\lambda}=(\lambda_\delta)_{\delta\in\boldsymbol{\Delta}}$ belongs to $T_{\boldsymbol{\Delta}}(\mathbf{Q})\cap\mathbf{Z}_{\boldsymbol{\Delta}}$, then we put $\mathrm{N}(\boldsymbol{\lambda})=(\lambda_j^+\lambda_j^-)_{1\leqslant j\leqslant 4}$ belonging to $\mathbf{Z}^4_{>0}$ and define a morphism $m_{\boldsymbol{\lambda}}:\mathscr{Y}_{\mathrm{N}(\boldsymbol{\lambda})\boldsymbol{n}}\to\mathscr{Y}_{\boldsymbol{n}}$ using the action of the torus $T_{\boldsymbol{\Delta}}$ on $\mathbf{A}_{\boldsymbol{\Delta}}$. For any commutative ring A, we may define an element $\boldsymbol{\lambda}A_{\boldsymbol{\Delta}}\in\mathscr{I}_\Delta(A)$ by taking the family of ideals $(\lambda_\delta A)_{\delta\in\boldsymbol{\Delta}}$. If $\mathfrak{a}\in\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$ satisfies $\log_2(\mathfrak{a})=0$, then $\mathfrak{a}=\boldsymbol{\lambda}(\mathfrak{a})\mathbf{Z}_{\boldsymbol{\Delta}}$. For any $\mathfrak{a}\in\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$, we similarly define $\mathfrak{a}A_{\boldsymbol{\Delta}}$ as $(\mathfrak{a}_\delta A)_{\delta\in\boldsymbol{\Delta}}\in\mathscr{I}_{\boldsymbol{\Delta}}(A)$.

Let $\boldsymbol{m}\in\Sigma$ and let $\mathfrak{a}=(\mathfrak{a}_j)_{1\leqslant j\leqslant 4}\in\widehat{\mathfrak{D}}^4$. We may see $\mathfrak{a}$ as an element of $\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$ by putting $\mathfrak{a}_j^+=\mathfrak{a}_j$ and $\mathfrak{a}_j^-=\overline{\mathfrak{a}}_j$ for $j\in\{1,2,3,4\}$ and $\mathfrak{a}_0^+=\mathfrak{a}_0^-=\mathbf{Z}[i]$. Let $\boldsymbol{n}=\boldsymbol{m}\mathrm{N}(\mathfrak{a})=(m_j\mathrm{N}(\mathfrak{a}_j))_{1\leqslant j\leqslant 4}$. Recall that $\alpha_{\boldsymbol{m}}$ is the positive square root of $\prod_{j=1}^4 m_j$. We put

$$\alpha_{\boldsymbol{m},\mathfrak{a}}=\alpha_{\boldsymbol{m}}\times\prod_{j=1}^4\lambda(\mathfrak{a})_j^+.$$

Note that $\prod_{j=1}^4 n_j=N(\alpha_{\boldsymbol{m},\mathfrak{a}})$. We then define a map $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}:\mathscr{Y}_{\boldsymbol{n}}\to\mathbf{A}^5_{\mathbf{Z}}$ as follows. Thanks to equations (4.2) and the fact that, by (3.1), the family $(a_j,b_j)_{1\leqslant j\leqslant 4}$ generates $\mathbf{Z}^2$, the system of equations

$$L_j(U,V)=n_j(X_j^2+Y_j^2)\tag{5.8}$$

in the variables U and V has a unique solution in the ring of functions on $\mathscr{Y}_{\boldsymbol{n}}$. We also define $T=X_0^2+Y_0^2$ and define X and Y by the relation

$$X+iY=\alpha_{\boldsymbol{m},\mathfrak{a}}(X_0+iY_0)^2\prod_{j=1}^4(X_j+iY_j).$$

The morphism $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}$ is then defined by the family of functions (X,Y,T,U,V). Since these functions satisfy the relation

$$X^2+Y^2=T^2\prod_{j=1}^4 L_j(U,V),$$

the image of $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}$ is contained in the Zariski closure $\mathscr{Y}_{\mathrm{spl}}$ of $\mathscr{T}_{\mathrm{spl}}$ in $\mathbf{A}^5_{\mathbf{Z}}$.

Let $\boldsymbol{m}\in\Sigma$ and $\mathfrak{a}\in\widehat{\mathfrak{D}}^4$. For any prime number p, we define $\mathscr{D}^1_{\boldsymbol{m},\mathfrak{a},p}$ as $\mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)\cap\widehat{\pi}^{-1}_{\boldsymbol{m},\mathfrak{a}}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p))$ where $\boldsymbol{n}=\boldsymbol{m}\mathrm{N}(\mathfrak{a})$. For any real number B, we also define $\mathscr{D}^1_{\boldsymbol{m},\mathfrak{a},\infty}(B)$ as the set of $R\in\mathscr{Y}_{\boldsymbol{n}}(\mathbf{R})$ such that $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}(R)$ satisfies conditions (5.6). We then put $\mathscr{D}^1_{\boldsymbol{m},\mathfrak{a}}(B) = \mathscr{D}^1_{\boldsymbol{m},\mathfrak{a},\infty}(B) \times \prod_{p\in\mathscr{P}} \mathscr{D}^1_{\boldsymbol{m},\mathfrak{a},p}$. When $\mathfrak{a}_j = \mathbf{Z}[i]$ for $j \in \{1,2,3,4\}$, we shall forget $\mathfrak{a}$ in the notation.

Let $\mathcal{S}'$ be the set of $p \in \mathcal{S}$ such that $p \equiv 1 \bmod 4$. For any $p \in \mathcal{S}'$, we consider the set $\mathscr{E}_p$ of subsets I of $\Delta - \{E^+, E^-\}$ such that:

(i) if $\delta_j^+ \in I$, then there exists $k < j$ such that $\delta_k^- \in I$;
(ii) if $\delta_k^- \in I$, then there exists $j > k$ such that $\delta_j^+ \in I$;
(iii) if $\delta_j^+ \in I$ and $\delta_k^- \in I$ with $j \neq k$, then $p \mid \Delta_{j,k}$.

For any $I \in \mathscr{E}_p$, we define $\boldsymbol{f}_I = (f_\delta)_{\delta\in\boldsymbol{\Delta}} \in \mathbf{Z}^{\boldsymbol{\Delta}}$ by

$$f_\delta = \begin{cases} 1 & \text{if } \delta \in I, \\ 0 & \text{otherwise.} \end{cases}$$

Using Notation 5.11, we then consider

$$\boldsymbol{e}_I = \varphi_p^{-1}(\boldsymbol{f}_I) \text{ and } \Sigma'_p = \left\{ \exp_{\varpi_p}(\boldsymbol{e}_I),\ I \in \mathscr{E}_p \right\}.$$

We define Σ' as the subset of $\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$ defined by

$$\Sigma' = \left\{ \left(\prod_{p\in\mathcal{S}'} \boldsymbol{\lambda}_p \right) \mathbf{Z}_{\boldsymbol{\Delta}},\ (\boldsymbol{\lambda}_p)_{p\in\mathcal{S}'} \in \prod_{p\in\mathcal{S}'} \Sigma'_p \right\}.$$

An element $\mathfrak{a} \in \Sigma'$ is determined by the quadruple $(\mathfrak{a}_j^+)_{1\leqslant j\leqslant 4}$, and we shall also consider Σ' as a subset of $\widehat{\mathfrak{D}}^4$. For $p \in \mathcal{S}'$, we define a map $\mu_p : \mathscr{E}_p \to \mathbf{Z}$ by the conditions

$$\mu_p(\emptyset) = 1 \quad \text{and} \quad \sum_{J\subset I} \mu_p(J) = 0 \text{ if } I \neq \emptyset.$$

The map $\mu : \Sigma' \to \mathbf{Z}$ is defined by $\mu(\mathfrak{a}) = \prod_{p\in\mathcal{S}'} \mu_p(I_p(\mathfrak{a}))$.

We shall denote by $\boldsymbol{A}_{f,\infty}$ the ring $\mathbf{R} \times \prod_{p\in\mathscr{P}} \mathbf{Z}_p$.

Remarks 5.27. (i) Let $\boldsymbol{\lambda} = (\lambda_\delta)_{\delta\in\boldsymbol{\Delta}} \in T_{\boldsymbol{\Delta}}(\mathbf{Q}) \cap \mathbf{Z}_{\boldsymbol{\Delta}}$. Let A be a commutative ring. Then $m_{\boldsymbol{\lambda}}$ is a bijection from the set $\mathscr{Y}_{\mathrm{N}(\boldsymbol{\lambda})\boldsymbol{n}}(A)$ to the set $\mathscr{Y}_{\boldsymbol{n}}(\boldsymbol{\lambda} A_{\boldsymbol{\Delta}})$.

(ii) With the same notation, for the ring $A = \mathbf{Z}_p$, the set $\mathscr{Y}_{\boldsymbol{n}}(\mathfrak{d})$ is the inverse image by $\log_p$ of the set $\log_p(\boldsymbol{\lambda}) + \Xi_p$.

LEMMA 5.28. *Let $p \in \mathcal{S}'$. For any subset K of Γ_p, we denote by $\mathbf{1}_K$ its characteristic function. Then*

$$\mathbf{1}_{\Lambda_p} = \sum_{I\in\mathscr{E}_p} \mu_p(I) \mathbf{1}_{\boldsymbol{e}_I + \Xi_p}.$$

Proof. For any j, k in $\{1,2,3,4\}$ such that $j < k$ and $p \mid \Delta_{j,k}$, we put $I_{j,k} = \{\delta_j^-, \delta_k^+\}$. Let K be a subset of

$$\{(j,k) \in \{1,2,3,4\}^2,\ j < k \text{ and } p \mid \Delta_{j,k}\}.$$

Let $I = \bigcup_{(j,k)\in K} I_{j,k}$. Then we have

$$\bigcap_{(j,k)\in K} (\boldsymbol{e}_{j,k} + \Xi_p) = \boldsymbol{e}_I + \Xi_p.$$

On the other hand, a subset I of $\boldsymbol{\Delta}$ belongs to $\mathscr{E}_p$ if and only if it is the union of subsets $I_{j,k}$ with $j < k$ and $p \mid \Delta_{j,k}$. The lemma then follows from equation (5.4) which defines Λ_p and the fact that the map $I \mapsto \boldsymbol{e}_I + \Xi_p$ reverses the inclusions. $\square$

LEMMA 5.29. *Let $\mathfrak{a} \in \Sigma'$ and let B be a positive real number. The multiplication by $\boldsymbol{\lambda}(\mathfrak{a}) \in T_{\boldsymbol{\Delta}}(\mathbf{Q})$ maps $\mathscr{D}^1_{\boldsymbol{m},\mathfrak{a}}(B)$ onto $\mathscr{D}^1_{\boldsymbol{m}}(B) \cap \mathscr{Y}_{\boldsymbol{m}}(\mathfrak{a}(\boldsymbol{A}_{f,\infty})_{\boldsymbol{\Delta}})$.*

Proof. By Remark 5.27(i), the map $m_{\boldsymbol{\lambda}(\mathfrak{a})}$ is a bijection from the set $\mathscr{Y}_{\mathrm{N}(\mathfrak{a})\boldsymbol{m}}(\boldsymbol{A}_{f,\infty})$ onto the set $\mathscr{Y}_{\boldsymbol{m}}(\mathfrak{a}(\boldsymbol{A}_{f,\infty})_{\boldsymbol{\Delta}})$. Let us now compare the maps $\widehat{\pi}_{\boldsymbol{m}} \circ m_{\boldsymbol{\lambda}(\mathfrak{a})}$ and $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}$. The map $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}$ is given by the relations

$$\begin{cases} L_j(U,V) = \mathrm{N}(\mathfrak{a}_j^+) m_i (X_j^2 + Y_j^2) \text{ for } j \in \{1,2,3,4\}, \\ T = X_0^2 + Y_0^2, \\ X + iY = \alpha_{\boldsymbol{m},\mathfrak{a}} (X_0 + iY_0)^2 \prod_{j=1}^4 (X_j + iY_j), \end{cases}$$

whereas $\widehat{\pi}_{\boldsymbol{m}} \circ m_{\boldsymbol{\lambda}(\mathfrak{a})}$ is given by

$$\begin{cases} L_j(U,V) = \lambda(\mathfrak{a})_j^+ \lambda(\mathfrak{a})_j^- m_i (X_j^2 + Y_j^2) \text{ for } j \in \{1,2,3,4\}, \\ T = X_0^2 + Y_0^2, \\ X + iY = \alpha_{\boldsymbol{m}} \left(\prod_{j=1}^4 \lambda(\mathfrak{a})_j^+ \right) (X_0 + iY_0)^2 \prod_{j=1}^4 (X_j + iY_j). \end{cases}$$

Therefore $\widehat{\pi}_{\boldsymbol{m}} \circ m_{\boldsymbol{\lambda}(\mathfrak{a})}$ coincides with $\widehat{\pi}_{\boldsymbol{m},\mathfrak{a}}$. This proves that for any prime number p, the map $m_{\lambda(\mathfrak{a})}$ maps $\widehat{\pi}^{-1}_{\boldsymbol{m},\mathfrak{a}}(\mathbf{Z}_p)$ onto $\widehat{\pi}^{-1}_{\boldsymbol{m}}(\mathbf{Z}_p)$. Moreover $m_{\boldsymbol{\lambda}(\mathfrak{a})}$ sends the set $\mathscr{D}^1_{\boldsymbol{m},\mathfrak{a},\infty}(B)$ onto $\mathscr{D}^1_{\boldsymbol{m},\infty}(B)$. $\square$

PROPOSITION 5.30. *For any real number B, we have*

$$N(B) = \frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\boldsymbol{m}\in\Sigma} \sum_{\mathfrak{a}\in\Sigma'} \mu(\mathfrak{a}) \sharp(\mathcal{T}_{\mathrm{N}(\mathfrak{a})\boldsymbol{m}}(\mathbf{Q}) \cap \mathscr{D}^1_{\boldsymbol{m},\mathfrak{a}}(B)).$$

Proof. Proposition 5.30 follows from Lemma 5.28, the definition of $\mathscr{D}_{\boldsymbol{m}}(B)$, and Lemma 5.29. $\square$

5.4.2. *Second inversion.* The inversion we shall now perform corresponds to the condition $\gcd(x,y,t) = 1$.

Notation 5.31. The map $\mu : \widehat{\mathfrak{O}} \to \mathbf{Z}$ is the multiplicative function such that

$$\mu(\mathfrak{p}^k) = \begin{cases} 1 & \text{if } k = 0, \\ -1 & \text{if } k = 1, \\ 0 & \text{otherwise} \end{cases}$$

for any prime ideal $\mathfrak{p}$ in $\widehat{\mathfrak{O}}$ and any integer $k \geqslant 0$.

Let $\boldsymbol{m} \in \Sigma$ and $\boldsymbol{\mathfrak{a}} \in \Sigma' \subset \widehat{\mathfrak{O}}^4$. Let $\boldsymbol{\mathfrak{b}} = (\mathfrak{b}_j)_{j \in \{1,2,3,4\}} \in \widehat{\mathfrak{O}}^4$. We put $\boldsymbol{n} = \mathrm{N}(\boldsymbol{\mathfrak{a}}\boldsymbol{\mathfrak{b}})\boldsymbol{m}$ and $\mu(\boldsymbol{\mathfrak{b}}) = \prod_{j=1}^4 \mu(\mathfrak{b}_j)$. Let B be a real number. Let p be a prime number. If R belongs to $\mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)$, we denote by X, Y, T, U, and V the functions on $\mathscr{Y}_{\boldsymbol{n}}$ which define $\widehat{\pi}_{\boldsymbol{m},\boldsymbol{\mathfrak{a}}\boldsymbol{\mathfrak{b}}}$. The local domain $\mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}},p}$ is then defined as follows:

- If $p \equiv 3 \bmod 4$ or $p = 2$, then $\mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}},p}$ is the set of $R \in \mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)$ such that $T(R) \in \mathbf{Z}_p^*$ and $\min(v_p(U(R)), v_p(V(R))) = 0$.
- If $p \equiv 1 \bmod 4$, then $\mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}},p}$ is the set of $R = (z_\delta)_{\delta \in \boldsymbol{\Delta}} \in \mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)$ such that z_0^- belongs to $\bigcap_{j=1}^4 \mathfrak{b}_j$, with $\min\bigl(v_p(T(R)), v_p\bigl(\prod_{j=1}^4 \mathrm{N}(\mathfrak{a}_j)\bigr)\bigr) = 0$ and $\min(v_p(U(R)), v_p(V(R))) = 0$.

We also put $\mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}},\infty}(B) = \mathscr{D}^1_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\infty}(B)$ and

$$\mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}}}(B) = \mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}},\infty}(B) \times \prod_{p \in \mathscr{P}} \mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}},p}.$$

PROPOSITION 5.32. *For any real number B, we have the relation*

$$N(B) = \frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\boldsymbol{m} \in \Sigma} \sum_{\boldsymbol{\mathfrak{a}} \in \Sigma'} \sum_{\boldsymbol{\mathfrak{b}} \in \widehat{\mathfrak{O}}^4} \mu(\boldsymbol{\mathfrak{a}})\mu(\boldsymbol{\mathfrak{b}})\sharp(\mathcal{T}_{\mathrm{N}(\boldsymbol{\mathfrak{a}})\mathrm{N}(\boldsymbol{\mathfrak{b}})\boldsymbol{m}}(\mathbf{Q}) \cap \mathscr{D}^2_{\boldsymbol{m},\boldsymbol{\mathfrak{a}},\boldsymbol{\mathfrak{b}}}(B)).$$

Proof. Let $\boldsymbol{m} \in \Sigma$, let $\boldsymbol{\mathfrak{a}} \in \Sigma'$ and let p be a prime number.

Let us first assume that $p \not\equiv 1 \bmod 4$. By Lemma 5.7(c), we have $v_p(t) = 0$ for any $(x, y, t, u, v) \in \mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p)$. Conversely, let R belong to $\mathscr{Y}_{\boldsymbol{m}\mathrm{N}(\boldsymbol{\mathfrak{a}})}(\mathbf{Z}_p)$. If $v_p(T(R)) = 0$, then $\min(v_p(X(R)), v_p(Y(R)), v_p(T(R))) = 0$.

We now assume that $p \equiv 1 \bmod 4$. For any $R = (z_\delta)_{\delta \in \boldsymbol{\Delta}} \in \mathscr{Y}_{\boldsymbol{m}\mathrm{N}(\boldsymbol{\mathfrak{a}})}(\mathbf{Q}_p)$, we have the relations

$$T(R) = z_0^+ z_0^- \quad \text{and} \quad X(R) + iY(R) = \alpha_{\boldsymbol{m},\boldsymbol{\mathfrak{a}}} (z_0^+)^2 \prod_{j=1}^4 z_j^+.$$

Note that if $\varpi_p | \alpha_{\boldsymbol{m},\boldsymbol{\mathfrak{a}}}$ for any prime $p \equiv 1 \bmod 4$, then $p | \alpha_{\boldsymbol{m},\boldsymbol{\mathfrak{a}}}$. Therefore we have the relation $\gcd(X(R), Y(R), T(R)) = 1$ in $\mathbf{Z}_p$ if and only if R satisfies the following two conditions:

(i) One has $\min(v_p(T(R)), v_p(\mathrm{N}(\prod_{j=1}^4 \mathfrak{a}_j))) = 0$.

(ii) There is no $j \in \{1, 2, 3, 4\}$ and no $\varpi \in \mathcal{S}_p$ such that $z_j^+ \in \varpi$ and $z_0^+ \in \overline{\varpi}$.

We denote by $\widehat{\mathfrak{b}}$ the unique element of $\mathscr{I}_{\boldsymbol{\Delta}}(\mathbf{Z})$ such that $\widehat{\mathfrak{b}}_j^+ = \mathfrak{b}_j$ for j belonging to $\{1,2,3,4\}$ and $\widehat{\mathfrak{b}}_0^- = \bigcap_{j=1}^4 \mathfrak{b}_j$. A classical Moebius inversion yields that the characteristic function of the set of the elements R in $\mathscr{Y}_{\boldsymbol{m}\mathrm{N}(\mathfrak{a})}(\mathbf{Z}_p)$ which satisfy condition (ii) is equal to

$$\sum_{\mathfrak{b}\in\widehat{\mathfrak{D}}^4} \mu(\mathfrak{b}) \mathbf{1}_{\mathscr{Y}_{\boldsymbol{m}\mathrm{N}(\mathfrak{a})}\left(\widehat{\mathfrak{b}}(\mathbf{Z}_p)_{\boldsymbol{\Delta}}\right)}.$$

By Remark 5.27(i), the multiplication map $m_{\boldsymbol{\lambda}(\mathfrak{b})}$ maps $\mathscr{Y}_{\boldsymbol{m}\mathrm{N}(\mathfrak{a})}\left(\widehat{\mathfrak{b}}(\mathbf{Z}_p)_{\boldsymbol{\Delta}}\right)$ onto the set of $(z_\delta)_{\delta\in\boldsymbol{\Delta}}$ in $\mathscr{Y}_{\boldsymbol{m}\mathrm{N}(\mathfrak{a}\mathfrak{b})}(\mathbf{Z}_p)$ such that z_0^- belongs to $\bigcap_{j=1}^4 \mathfrak{b}_j$. The rest of the proof is similar to the proof of Lemma 5.29. □

5.4.3. *Third inversion.* The last inversion corresponds to the condition $\gcd(u,v)=1$, in which it will prove nonetheless useful to retain the fact that u, v cannot both be even.

Notation 5.33. Let $\boldsymbol{m}\in\Sigma$ and $\mathfrak{a}\in\Sigma'$. Let $\mathfrak{b}=(\mathfrak{b}_j)_{j\in\{1,2,3,4\}}\in\widehat{\mathfrak{D}}^4$. We put $\boldsymbol{n}=\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})\boldsymbol{m}$. Let ℓ be an odd integer. Let p be a prime number. The local domain $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}$ is then defined as follows:

- If $p=2$, then $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}$ is the set of $R\in\mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)$ such that $T(R)\in\mathbf{Z}_p^*$ and $\min(v_p(U(R)), v_p(V(R)))=0$.
- If $p\equiv 3 \bmod 4$, then $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}$ is the set of $R\in\mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)$ such that $T(R)\in\mathbf{Z}_p^*$ and ℓ divides $U(R)$ and $V(R)$.
- If $p\equiv 1 \bmod 4$, then $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}$ is the set of $R=(z_\delta)_{\delta\in\boldsymbol{\Delta}}\in\mathscr{Y}_{\boldsymbol{n}}(\mathbf{Z}_p)$ such that z_0^- belongs to $\bigcap_{j=1}^4 \mathfrak{b}_j$, with $\min\left(v_p(T(R)), v_p\left(\prod_{j=1}^4 \mathrm{N}(\mathfrak{a}_j)\right)\right)=0$ and and such that ℓ divides $U(R)$ and $V(R)$.

We define $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,\infty}(B)=\mathscr{D}^2_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\infty}(B)$ and

$$\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell}(B)=\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,\infty}(B)\times\prod_{p\in\mathscr{P}}\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}.$$

PROPOSITION 5.34. *For any positive real number B, we have that $N(B)$ is equal to*

$$\frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}}\sum_{\boldsymbol{m}\in\Sigma}\sum_{\mathfrak{a}\in\Sigma'}\sum_{\mathfrak{b}\in\widehat{\mathfrak{D}}^4}\sum_{\substack{\ell=1\\2\nmid\ell}}^{\infty}\mu(\mathfrak{a})\mu(\mathfrak{b})\mu(\ell)\sharp(\mathcal{T}_{\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b})\boldsymbol{m}}(\mathbf{Q})\cap\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell}(B)).$$

6. Formulation of the counting problem

We are now ready to begin the analytic part of the proof of Theorem 3.3. Let us recall that the linear forms that we are working with take the shape

$$L_1(U,V)=U,\ \ L_2(U,V)=V,\ \ L_3(U,V)=a_3U+b_3V,\ \ L_4(U,V)=a_4U+b_4V,$$

with integers a_3, b_3, a_4, b_4 such that $\gcd(a_3, b_3) = \gcd(a_4, b_4) = 1$ and

$$\Delta = a_3 b_3 a_4 b_4 (a_3 b_4 - a_4 b_3) \neq 0. \tag{6.1}$$

It is clear that the forms involved are all pairwise nonproportional. In this section we will further translate our counting problem in terms of the familiar multiplicative arithmetic function

$$r(n) = \sharp\{(x, y) \in \mathbf{Z}^2,\ x^2 + y^2 = n\} = 4 \sum_{d|n} \chi(d),$$

where χ is the real nonprincipal character modulo 4. It is to this expression that we will be able to direct the full force of analytic number theory.

In what follows we will allow the implied constant in any estimate to depend arbitrarily upon the coefficients of the linear forms involved. Furthermore, we will reserve j for an arbitrary index from the set $\{1, 2, 3, 4\}$. Finally, many of our estimates will involve a small parameter $\varepsilon > 0$, and it will ease notation if we also permit the implied constants to depend on the choice of ε. We will follow common practice and allow ε to take different values at different parts of the argument.

Recall the definitions of Σ, Σ' from Sections 4 and 5 respectively. In particular we have $m_j N(\mathfrak{a}_j^+) = O(1)$ whenever $\boldsymbol{m} \in \Sigma$ and $\boldsymbol{\mathfrak{a}} \in \Sigma'$.

PROPOSITION 6.1. *For $B \geqslant 1$, we have*

$$N(B) = \frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\substack{\boldsymbol{m} \in \Sigma \\ \boldsymbol{\mathfrak{a}} \in \Sigma'}} \mu(\boldsymbol{\mathfrak{a}}) \sum_{\substack{\ell = 1 \\ 2 \nmid \ell}}^{\infty} \mu(\ell) \sum_{\boldsymbol{\mathfrak{b}} \in \widehat{\mathfrak{D}}^4} \mu(\boldsymbol{\mathfrak{b}}) \sum_{\substack{t \in \mathfrak{D} \\ \gcd(t, \mathrm{N}(\boldsymbol{\mathfrak{a}})) = 1 \\ \mathrm{N}(\bigcap \mathfrak{b}_j) | t}} r\Big(\frac{t}{\mathrm{N}(\bigcap \mathfrak{b}_j)}\Big) \mathscr{U}\Big(\frac{B}{t}\Big),$$

where

$$\mathscr{U}(T) = \sum_{\substack{(u,v) \in \mathbf{Z}^2 \cap \sqrt{T} \mathscr{R}_{\boldsymbol{m}} \\ \ell | u, v \\ 2 \nmid \gcd(u,v) \\ m_j \mathrm{N}(\mathfrak{a}_j^+ \mathfrak{b}_j) | L_j(u,v)}} \prod_{j=1}^{4} r\Big(\frac{L_j(u,v)}{m_j \mathrm{N}(\mathfrak{a}_j^+ \mathfrak{b}_j)}\Big)$$

and

$$\mathscr{R}_{\boldsymbol{m}} = \Big\{(u, v) \in \mathbf{R}^2,\ 0 < |u|, |v| \leqslant 1,\ m_j L_j(u, v) > 0 \textit{ for } j \in \{1, 2, 3, 4\}\Big\}. \tag{6.2}$$

Proof. We apply Proposition 5.34. Let $\boldsymbol{m} \in \Sigma$, $\boldsymbol{\mathfrak{a}} \in \Sigma'$, and $\boldsymbol{\mathfrak{b}} \in \widehat{\mathscr{D}}^4$. We wish to express $\sharp(\mathcal{T}_{\mathrm{N}(\boldsymbol{\mathfrak{a}})\mathrm{N}(\boldsymbol{\mathfrak{b}})\boldsymbol{m}}(\mathbf{Q}) \cap \mathscr{D}^3_{\boldsymbol{m}, \boldsymbol{\mathfrak{a}}, \boldsymbol{\mathfrak{b}}, \ell}(B))$ in terms of the function r. But given $(t, u, v) \in \mathbf{Z}^3$, the number of elements R in that intersection such that $(T(R), U(R), V(R)) = (t, u, v)$ is 0 if (t, u, v) does not satisfy the conditions

$$\gcd(t, \mathrm{N}(\boldsymbol{\mathfrak{a}})) = 1,\ \ N(\textstyle\bigcap \mathfrak{b}_j) | t,\ \ \ell | u, v,\ \ 2 \nmid t \gcd(u, v) \text{ and } m_j \mathrm{N}(\mathfrak{a}_j^+ \mathfrak{b}_j) \mid L_j(u, v)$$

and is equal to

$$r\left(\frac{t}{\mathrm{N}(\bigcap \mathfrak{b}_j)}\right)\prod_{j=1}^{4} r\left(\frac{L_j(u,v)}{m_j\mathrm{N}(\mathfrak{a}_j^+\mathfrak{b}_j)}\right)$$

otherwise. $\square$

Let us set

$$d_j = m_j\mathrm{N}(\mathfrak{a}_j^+)\mathrm{N}(\mathfrak{b}_j), \quad D_j = \begin{cases} [d_j,\ell] & \text{if } j=1 \text{ or } 2,\\ d_j & \text{if } j=3 \text{ or } 4,\end{cases} \tag{6.3}$$

where $[d_j,\ell]$ is the least common multiple of d_j,ℓ. Then d_j, D_j are odd positive integers such that $d_j \mid D_j$. We may write

$$\mathscr{U}(T) = \sum_{\substack{(u,v)\in\Gamma_{\mathbf{D}}\cap\sqrt{T}\mathscr{R}_{\boldsymbol{m}}\\ 2\nmid\gcd(u,v)}} \prod_{j=1}^{4} r\Big(\frac{L_j(u,v)}{d_j}\Big), \tag{6.4}$$

where

$$\Gamma_{\mathbf{D}} = \{(u,v)\in\mathbf{Z}^2,\ D_j \mid L_j(u,v)\}. \tag{6.5}$$

Before passing to a detailed analysis of the sum $\mathscr{U}(T)$ and its effect on the behaviour of the counting function $N(B)$, we will first corral together some of the technical tools that will prove useful to us. It is clear that $\Gamma_{\mathbf{D}}$ defines a sublattice of $\mathbf{Z}^2$ of rank 2, since it is closed under addition and contains the vector $D_1D_2D_3D_4(u,v)$ for any $(u,v)\in\mathbf{Z}^2$. Let us write

$$\varrho(\mathbf{D}) = \det\Gamma_{\mathbf{D}}, \tag{6.6}$$

for the determinant. It follows from the Chinese remainder theorem that there is a multiplicativity property $\varrho(g_1h_1,\dots,g_4h_4) = \varrho(g_1,\dots,g_4)\varrho(h_1,\dots,h_4)$, whenever $g_1\cdots g_4$ and $h_1\cdots h_4$ are coprime. Recall the definition (6.1) of Δ. Then [HB03, eq. (3.12)] shows that

$$\varrho(p^{e_1},\dots,p^{e_4}) = p^{\max_{i<j}\{e_i+e_j\}} \tag{6.7}$$

for any prime $p\nmid\Delta$. Likewise, when $p\mid\Delta$ one has

$$\varrho(p^{e_1},\dots,p^{e_4}) \asymp p^{\max_{i<j}\{e_i+e_j\}}, \tag{6.8}$$

whence

$$\varrho(\mathbf{D}) \asymp [D_1D_2, D_1D_3, D_1D_4, D_2D_3, D_2D_4, D_3D_4], \tag{6.9}$$

where the symbol $\asymp$ means that the two quantities involved have the same order of magnitude.

7. Estimating $\mathscr{U}(T)$: an upper bound

Our goal in this section is to provide an upper bound for $\mathscr{U}(T)$ that is uniform in the various parameters. This will allow us to reduce the range of summation for the various parameters appearing in our expression for $N(B)$. Our main tool will be previous work of the first two authors [dlBB06], which is concerned with the average order of arithmetic functions ranging over the values taken by binary forms.

Throughout this section we continue to adhere to the convention that all of our implied constants are allowed to depend upon the coefficients of the forms L_j. Recall the expression for $\mathscr{U}(T)$ given in (6.4), with d_j, D_j given by (6.3). We then have the following result.

Lemma 7.1. *Let $\varepsilon > 0$, let $T \geqslant 1$, and write $d = d_1d_2d_3d_4$. Then we have*

$$\mathscr{U}(T) \ll (d\ell)^\varepsilon \Big(\frac{T}{[D_1D_2, \dots, D_3D_4]} + \frac{T^{1/2+\varepsilon}}{\ell} \Big).$$

Proof. Since we are only concerned with providing an upper bound for $\mathscr{U}(T)$, we may drop any of the conditions in the summation over (u,v) that we care to choose. Thus it follows that

$$\mathscr{U}(T) \leqslant \sum_{(u,v)\in \Gamma_{\mathbf{D}} \cap (0,\sqrt{T}]^2} \prod_{j=1}^4 r\Big(\frac{|L_j(u,v)|}{d_j}\Big),$$

where $\Gamma_{\mathbf{D}}$ is the lattice defined in (6.5).

Let $\mathbf{e}_1, \mathbf{e}_2$ be a minimal basis for $\Gamma_{\mathbf{D}}$. This is constructed by taking $\mathbf{e}_1 \in \Gamma_{\mathbf{D}}$ to be any nonzero vector for which $|\mathbf{e}_1|$ is least, and then choosing $\mathbf{e}_2 \in \Gamma_{\mathbf{D}}$ to be any vector not proportional to $\mathbf{e}_1$, for which $|\mathbf{e}_2|$ is least. The successive minima of $\Gamma_{\mathbf{D}}$ are the numbers $s_i = |\mathbf{e}_i|$ for $i = 1, 2$. We claim that one has $s_1 \geqslant \min\{D_1, D_2\} \geqslant \ell$. For this we recall definition (6.3) of D_1, D_2 and note that $\Gamma_{\mathbf{D}} \subseteq \Lambda = \{(u,v) \in \mathbf{Z}^2,\ D_1 \mid u,\ D_2 \mid v\}$, where $\Lambda \subseteq \mathbf{Z}^2$ is a sublattice of rank 2, with smallest successive minimum $\min\{D_1, D_2\}$. The desired inequalities are now obvious, and we conclude that

$$\ell \leqslant s_1 \leqslant s_2, \quad s_1s_2 \ll \varrho(\mathbf{D}) \leqslant s_1s_2, \tag{7.1}$$

where ϱ is defined in (6.6).

Write $M_j(X,Y)$ for the linear form obtained from $d_j^{-1}L_j(U,V)$ via the change of variables $(U,V) \mapsto X\mathbf{e}_1 + Y\mathbf{e}_2$. Each M_j has integer coefficients of size $O(\varrho(\mathbf{D}))$. Furthermore, it follows from work of Davenport [Dav63, Lemma 5] that $x \ll \max\{|u|,|v|\}/s_1$ and $y \ll \max\{|u|,|v|\}/s_2$ whenever one writes $(u,v) \in \Gamma_{\mathbf{D}}$ as $(u,v) = x\mathbf{e}_1 + y\mathbf{e}_2$, with $x, y \in \mathbf{Z}$. Let $T_1 = s_1^{-1}\sqrt{T}$ and

$T_2 = s_2^{-1}\sqrt{T}$, so that in particular $T_1 \geqslant T_2 > 0$. Then we may deduce that

$$\mathscr{U}(T) \leqslant \sum_{x \ll T_1, y \ll T_2} \prod_{j=1}^{4} r(|M_j(x,y)|).$$

Suppose that $M_j(X,Y) = a_{j1}X + a_{j2}Y$, with coefficients $a_{ji} = O(\varrho(\mathbf{D}))$. We proceed to introduce a multiplicative function $r_1(n)$, via

$$r_1(p^\nu) = \begin{cases} 1+\chi(p), & \nu = 1 \text{ and } p \nmid 6d\ell \prod a_{ji}, \\ (1+\nu)^4, & \text{otherwise}, \end{cases}$$

where $d = d_1d_2d_3d_4$. Then $r(n_1)r(n_2)r(n_3)r(n_4) \leqslant 2^8 r_1(n_1n_2n_3n_4)$, and one checks that r_1 belongs to the class of nonnegative arithmetic functions considered previously by the first two authors [dlBB06]. An application of [dlBB06, Cor. 1] now reveals that

$$\mathscr{U}(T) \ll (d\ell)^\varepsilon (T_1T_2 + T_1^{1+\varepsilon}) \ll (d\ell)^\varepsilon \Big(\frac{T}{s_1s_2} + \frac{T^{1/2+\varepsilon}}{s_1}\Big)$$

for any $\varepsilon > 0$. Combining (7.1) with (6.9) we therefore conclude the proof of the lemma. □

The main purpose of Lemma 7.1 is to reduce the range of summation of the various parameters appearing in Proposition 6.1. Let us write $E_0(B)$ for the overall contribution to the summation from values of $\mathfrak{b}_j, \ell$ such that

$$\max \mathrm{N}(\mathfrak{b}_j) > \log(B)^D \quad \text{or} \quad \ell > \log(B)^L \tag{7.2}$$

for parameters $D, L > 0$ to be selected in due course. We will denote by $N_1(B)$ the remaining contribution, so that

$$N(B) = N_1(B) + E_0(B). \tag{7.3}$$

Henceforth, the implied constants in our estimates will be allowed to depend on D and L, in addition to ε and the coefficients of the linear forms L_j. We have the following result.

Lemma 7.2. *We have* $E_0(B) \ll B\log(B)^{1-\min\{D/4, L/2\}+\varepsilon}$ *for any* $\varepsilon > 0$.

Proof. We begin observing that $\mathscr{U}(B/t) = 0$ in $E_0(B)$, unless $D_j \leqslant \sqrt{B/t}$, in the notation of (6.3). But then it follows that we must have

$$t \leqslant \frac{B}{\sqrt{D_1D_2D_3D_4}} \leqslant \frac{B\sqrt{\gcd(\mathrm{N}(\mathfrak{b}_1),\ell)\gcd(\mathrm{N}(\mathfrak{b}_2),\ell)}}{\ell\sqrt{\mathrm{N}(\mathfrak{b}_1)\cdots\mathrm{N}(\mathfrak{b}_4)}} = B_0,$$

say, in the summation over t. Here we have used the fact that $m_jN(\mathfrak{a}_j^+) = O(1)$ whenever $\boldsymbol{m} \in \Sigma$ and $\mathfrak{a} \in \Sigma'$. It will be convenient to set $K = \mathrm{N}(\mathfrak{b}_1)\cdots\mathrm{N}(\mathfrak{b}_4)$.

We now apply Lemma 7.1 to bound $\mathscr{U}(B/t)$, giving

$$E_0(B) \ll \sum_{\substack{\boldsymbol{m}\in\Sigma\\ \mathfrak{a}\in\Sigma'}} \sum_{\ell} \ell^{\varepsilon} \sum_{\mathfrak{b}_1,\dots,\mathfrak{b}_4} K^{\varepsilon} \sum_{\substack{t\leqslant B_0\\ \mathrm{N}(\bigcap \mathfrak{b}_j)\mid t}} r\Big(\frac{t}{\mathrm{N}(\bigcap \mathfrak{b}_j)}\Big)\Big(\frac{B}{t[D_1D_2,\dots,D_3D_4]}+\frac{B^{1/2+\varepsilon}}{t^{1/2+\varepsilon}\ell}\Big)$$

for any $\varepsilon>0$, where the summations over ℓ and $\mathfrak{b}_j$ are subject to (7.2). In view of the elementary estimates

$$\sum_{n\leqslant x}\frac{r(n)}{n^{\theta}} \ll \begin{cases}\log(2x) & \text{if } \theta\geqslant 1,\\ x^{1-\theta} & \text{if } 0\leqslant\theta<1,\end{cases} \tag{7.4}$$

we easily conclude that

$$E_0(B) \ll \sum_{\substack{\boldsymbol{m}\in\Sigma\\ \mathfrak{a}\in\Sigma'}} \sum_{\ell} \ell^{\varepsilon} \sum_{\mathfrak{b}_1,\dots,\mathfrak{b}_4} \frac{K^{\varepsilon}}{\mathrm{N}(\bigcap \mathfrak{b}_j)}\Big(\frac{B\log(B)}{[D_1D_2,\dots,D_3D_4]}+\frac{B^{1/2+\varepsilon}B_0^{1/2-\varepsilon}}{\ell}\Big).$$

The second term in the inner bracket is

$$\ll B\cdot\frac{\gcd(\mathrm{N}(\mathfrak{b}_1),\ell)^{1/4}\gcd(\mathrm{N}(\mathfrak{b}_2),\ell)^{1/4}}{\ell^{3/2-\varepsilon}K^{1/4-\varepsilon}}.$$

Similarly rapid consultation with (6.3) reveals that the first term in the inner bracket is

$$\ll \frac{B\log(B)}{(D_1D_2)^{3/4}(D_3D_4)^{1/4}} \ll B\log(B)\cdot\frac{\gcd(\mathrm{N}(\mathfrak{b}_1),\ell)^{1/4}\gcd(\mathrm{N}(\mathfrak{b}_2),\ell)^{1/4}}{\ell^{3/2}K^{1/4}}.$$

Bringing these estimates together we may now conclude that

$$E_0(B) \ll B\log(B)\sum_{\ell}\sum_{\mathfrak{b}_1,\dots,\mathfrak{b}_4}\frac{1}{\mathrm{N}(\bigcap \mathfrak{b}_j)}\cdot\frac{\gcd(\mathrm{N}(\mathfrak{b}_1),\ell)^{1/4}\gcd(\mathrm{N}(\mathfrak{b}_2),\ell)^{1/4}}{\ell^{3/2-\varepsilon}K^{1/4-\varepsilon}},$$

where the sums are over $\ell\in\mathbf{Z}_{>0}$ and $\mathfrak{b}_1,\dots,\mathfrak{b}_4\subseteq\widehat{\mathfrak{D}}$ such that (7.2) holds.

For fixed $\ell\in\mathbf{Z}_{>0}$, and $\varepsilon>0$ we proceed to estimate the sum

$$S_\ell(T)=\sum_{\substack{\mathfrak{b}_1,\dots,\mathfrak{b}_4\subseteq\mathbf{Z}[i]\\ \max\mathrm{N}(\mathfrak{b}_j)\geqslant T}}\frac{\gcd(\mathrm{N}(\mathfrak{b}_1),\ell)^{1/4}\gcd(\mathrm{N}(\mathfrak{b}_2),\ell)^{1/4}}{\mathrm{N}(\bigcap \mathfrak{b}_j)K^{1/4-\varepsilon}},$$

using Rankin's trick and the observation that $\mathrm{N}(\mathfrak{a})\mid\mathrm{N}(\mathfrak{a}\cap\mathfrak{b})$ for any $\mathfrak{a},\mathfrak{b}\subseteq\mathbf{Z}[i]$. Thus it follows that $\mathrm{N}(\bigcap\mathfrak{b}_j)\geqslant[\mathrm{N}(\mathfrak{b}_1),\dots,\mathrm{N}(\mathfrak{b}_4)]$, whence

$$\begin{aligned}
S_\ell(T) &\leqslant \frac{1}{T^{\delta}}\sum_{\mathfrak{b}_1,\dots,\mathfrak{b}_4\subseteq\mathbf{Z}[i]}\frac{\gcd(\mathrm{N}(\mathfrak{b}_1),\ell)^{1/4}\gcd(\mathrm{N}(\mathfrak{b}_2),\ell)^{1/4}}{[\mathrm{N}(\mathfrak{b}_1),\dots,\mathrm{N}(\mathfrak{b}_4)]^{1-\delta}K^{1/4-\varepsilon}}\\
&\ll \frac{1}{T^{\delta}}\sum_{b_1,\dots,b_4=1}^{\infty}\frac{\gcd(b_1,\ell)^{1/4}\gcd(b_2,\ell)^{1/4}}{[b_1,\dots,b_4]^{1-\delta}b_1^{1/4-\varepsilon}\cdots b_4^{1/4-\varepsilon}}\\
&\ll_\delta \ell^{\varepsilon}T^{-\delta},
\end{aligned}$$

provided that $\delta<1/4$, as is obvious from the corresponding Euler product.

Armed with this we see that the overall contribution to the above estimate for $E_0(B)$ arising from $\ell, \mathfrak{b}_1, \dots, \mathfrak{b}_4$ for which $\ell > \log(B)^L$ is

$$\ll B \log(B) \sum_{\ell > \log(B)^L} \ell^{-3/2+\varepsilon} S_\ell(1) \ll B \log(B)^{1-L/2+\varepsilon},$$

which is satisfactory. In a similar fashion the overall contribution arising from $\ell, \mathfrak{b}_1, \dots, \mathfrak{b}_4$ for which $\max \mathrm{N}(\mathfrak{b}_j) > \log(B)^D$ is

$$\ll B \log(B) \sum_{\ell} \ell^{-3/2+\varepsilon} S_\ell(\log(B)^D) \ll B \log(B)^{1-D/4+\varepsilon},$$

which is also satisfactory. The statement of Lemma 7.2 is now obvious. □

8. Estimating $\mathscr{U}(T)$: an asymptotic formula

In view of our work in the previous section it remains to estimate $N_1(B)$, which we have defined as the contribution to $N(B)$ from values of $\mathfrak{b}_j, \ell$ for which (7.2) fails. Thus

$$N_1(B) = \frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\substack{\boldsymbol{m} \in \Sigma \\ \mathfrak{a} \in \Sigma'}} \mu(\mathfrak{a}) \sum_{\substack{\ell \leqslant \log(B)^L \\ 2 \nmid \ell}} \mu(\ell) \times \sum_{\substack{\mathfrak{b}_1, \dots, \mathfrak{b}_4 \in \widehat{\mathfrak{D}} \\ \mathrm{N}(\mathfrak{b}_j) \leqslant \log(B)^D}} \prod_{j=1}^{4} \mu(\mathfrak{b}_j) \sum_{\substack{t \in \mathfrak{D} \cap [1,B] \\ \gcd(t, \mathrm{N}(\mathfrak{a}))=1 \\ \mathrm{N}(\bigcap \mathfrak{b}_j) \mid t}} r\Big(\frac{t}{\mathrm{N}(\bigcap \mathfrak{b}_j)}\Big) \mathscr{U}\Big(\frac{B}{t}\Big).$$

Here we have inserted the condition $t \leqslant B$ in the summation over t, since the innermost summand is visibly zero otherwise. Whereas the previous section was primarily concerned with a uniform upper bound for the sum $\mathscr{U}(T)$ defined in (6.4), our work in the present section will revolve around a uniform asymptotic formula for $\mathscr{U}(T)$. The error term that arises in our analysis will involve the real number

$$\eta = 1 - \frac{1 + \log(\log(2))}{\log(2)}, \tag{8.1}$$

which has numerical value $0.086071\dots$.

Before revealing our result for $\mathscr{U}(T)$, we must first introduce some notation for certain local densities that emerge in the asymptotic formula. In fact estimating $\mathscr{U}(T)$ boils down to counting integer points on the affine variety

$$L_j(U, V) = d_j(S_j^2 + T_j^2), \quad (1 \leqslant j \leqslant 4), \tag{8.2}$$

in $\mathbf{A}^{10}_{\mathbf{Q}}$, with U, V restricted to lie in a lattice depending on $\mathbf{D}$. Thus the expected leading constant admits an interpretation as a product of local densities.

Given a prime $p > 2$ and $\mathbf{d}, \mathbf{D}$ as in (6.3), let

$$N_{\mathbf{d},\mathbf{D}}(p^n) = \sharp\Big\{(u, v, \mathbf{s}, \mathbf{t}) \in (\mathbf{Z}/p^n\mathbf{Z})^{10}, \quad \begin{array}{l} L_j(u,v) \equiv d_j(s_j^2 + t_j^2) \bmod p^n \\ D_j \mid L_j(u,v) \end{array} \Big\}.$$

The p-adic density on (8.2) is defined to be

$$\omega_{\mathbf{d},\mathbf{D}}(p) = \lim_{n\to\infty} p^{-6n-\lambda_1-\cdots-\lambda_4} N_{\mathbf{d},\mathbf{D}}(p^n) \tag{8.3}$$

when $p > 2$, where

$$\boldsymbol{\lambda} = \big(v_p(d_1), \ldots, v_p(d_4)\big), \quad \boldsymbol{\mu} = \big(v_p(D_1), \ldots, v_p(D_4)\big). \tag{8.4}$$

When $\mathbf{d}, \mathbf{D}$ are as in (6.3) and $p > 2$, we will set

$$\sigma_p(\mathbf{d}, \mathbf{D}) = \omega_{\mathbf{d},\mathbf{D}}(p). \tag{8.5}$$

Turning to the case $p = 2$, we define

$$\sigma_2(\mathbf{d}, \mathbf{D}) = \lim_{n\to\infty} 2^{-6n} N_{\mathbf{d},\mathbf{D}}(2^n), \tag{8.6}$$

where

$$N_{\mathbf{d},\mathbf{D}}(2^n) = \sharp\Big\{(u, v, \mathbf{s}, \mathbf{t}) \in (\mathbf{Z}/2^n\mathbf{Z})^{10}, \quad \begin{array}{l} L_j(u,v) \equiv d_j(s_j^2 + t_j^2) \bmod 2^n \\ 2 \nmid \gcd(u,v) \end{array} \Big\}.$$

Finally, we let $\omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty)$ denote the usual archimedean density of solutions to the system of equations (8.2), with $(u, v, \mathbf{s}, \mathbf{t}) \in \mathscr{R}_{\boldsymbol{m}} \times \mathbf{R}^8$ and $\mathscr{R}_{\boldsymbol{m}}$ defined in (6.2). We are now ready to record our main estimate for $\mathscr{U}(T)$.

LEMMA 8.1. *Let $\mathbf{d}, \mathbf{D}$ be as in* (6.3). *Then for any $\varepsilon > 0$ and $T \geqslant 2$ we have*

$$\mathscr{U}(T) = c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}} T + O\Big(\frac{(d_1d_2d_3d_4\ell)^{\varepsilon} T}{\log(T)^{\eta-\varepsilon}}\Big),$$

where

$$c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}} = \omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty) \prod_{p\in\mathscr{P}} \sigma_p(\mathbf{d}, \mathbf{D}). \tag{8.7}$$

Proof. Our primary tool in estimating $\mathscr{U}(T)$ asymptotically is the subject of allied work of the first two authors [dlBB08]. We begin by bringing our expression for $\mathscr{U}(T)$ into a form that can be tackled by the main results there. According to (6.1) we may assume that the binary linear forms L_j are pairwise nonproportional and primitive. Furthermore, the region $\mathscr{R}_{\boldsymbol{m}} \subset \mathbf{R}^2$ defined in (6.2) is open, bounded, and convex, with a piecewise continuously differentiable boundary such that $m_jL_j(u, v) > 0$ for each $(u, v) \in \mathscr{R}_{\boldsymbol{m}}$.

A key step in applying the work of [dlBB08] consists in checking that the "normalisation hypothesis" $\mathsf{NH}_2(\mathbf{d})$ is satisfied in the present context. In fact it is easy to see that $L_j, \mathscr{R}_{\boldsymbol{m}}$ will satisfy $\mathsf{NH}_2(\mathbf{d})$ provided that

$$L_1(U, V) \equiv d_1U \pmod 4, \quad L_2(U, V) \equiv V \pmod 4.$$

The second congruence is automatic since $L_2(U,V) = V$. Recalling that $L_1(U,V) = U$, we therefore conclude that $\mathsf{NH}_2(\mathbf{d})$ holds if $d_1 \equiv 1 \bmod 4$. Alternatively, if $d_1 \equiv 3 \bmod 4$, we make the unimodular change of variables $(U,V) \mapsto (-U,V)$ to place ourselves in the setting of $\mathsf{NH}_2(\mathbf{d})$. We leave the reader to check that this ultimately leads to an identical estimate in the ensuing argument. Thus, for the purposes of our exposition here, we may freely assume that $L_j, \mathscr{R}_{\boldsymbol{m}}$ satisfy $\mathsf{NH}_2(\mathbf{d})$ in $\mathscr{U}(T)$.

We proceed by writing

$$\mathscr{U}(T) = U_1(T) + U_2(T) + U_3(T), \tag{8.8}$$

where $U_1(T)$ denotes the contribution to $\mathscr{U}(T)$ from (u,v) such that $2 \nmid uv$, $U_2(T)$ denotes the contribution from (u,v) such that $2 \nmid u$ and $2 \mid v$, and finally $U_3(T)$ is the contribution from (u,v) such that $2 \mid u$ and $2 \nmid v$. For each $1 \leqslant i \leqslant 3$, we will establish an estimate of the form

$$U_i(T) = c_i T + O\Big(\frac{(d\ell)^{\varepsilon} T}{\log(T)^{\eta-\varepsilon}}\Big), \tag{8.9}$$

where $d = d_1 d_2 d_3 d_4$.

Beginning with the case $i = 1$, we observe that $U_1(T) = S_1(\sqrt{T}, \mathbf{d}, \mathsf{\Gamma}_{\mathbf{D}})$, in the notation of [dlBB08, eq. (1.9)]. An application of [dlBB08, Ths. 3 and 4] with $(j,k) = (1,2)$ therefore reveals that (8.9) holds with

$$c_1 = \omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty)\omega_{1,\mathbf{d}}(2) \prod_{p>2} \omega_{\mathbf{d},\mathbf{D}}(p).$$

Here $\omega_{\mathbf{d},\mathbf{D}}(p)$ is given by (8.3) for $p > 2$ and $\omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty)$ is defined prior to the statement of the lemma. Finally, for $i \in \{0,1\}$, the corresponding 2-adic density is given by

$$\omega_{i,\mathbf{d}}(2) = \lim_{n\to\infty} 2^{-6n} \sharp\Big\{(u,v,\mathbf{s},\mathbf{t}) \in (\mathbf{Z}/2^n\mathbf{Z})^{10}, \begin{array}{l} L_j(u,v) \equiv d_j(s_j^2 + t_j^2) \bmod 2^n \\ u \equiv 1 \bmod 4,\ v \equiv i \bmod 2 \end{array}\Big\}.$$

Note that the notation introduced in [dlBB08] involves an additional subscript in $\omega_{i,\mathbf{d}}(2)$ whose presence indicates which of the various normalisation hypotheses the $L_j, \mathscr{R}_{\boldsymbol{m}}$ are assumed to satisfy. Since we have placed ourselves in the context of $\mathsf{NH}_2(\mathbf{d})$ in each case, we have found it reasonable to suppress mentioning this here. Let us now shift to a consideration of the sum $U_2(T)$ in (8.8), for which one finds that $U_2(T) = S_0(\sqrt{T}, \mathbf{d}, \mathsf{\Gamma}_{\mathbf{D}})$. Applying [dlBB08, Ths. 3 and 4] with $(j,k) = (0,2)$ therefore yields (8.9) with $i = 2$ and

$$c_2 = \omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty)\omega_{0,\mathbf{d}}(2) \prod_{p>2} \omega_{\mathbf{d},\mathbf{D}}(p).$$

Finally we turn to the sum $U_3(T)$ in (8.8). Making the unimodular change of variables $(U,V) \mapsto (V,U)$, one now sees that $U_3(T) = S_0(\sqrt{T}; \mathbf{d}, \mathsf{\Gamma}_{\mathbf{D}}^{\flat})$, where the underlying region is $\mathscr{R}_{\boldsymbol{m}}^{\flat} = \{(u,v) \in \mathbf{R}^2,\ (v,u) \in \mathscr{R}_{\boldsymbol{m}}\}$ and $\mathsf{\Gamma}_{\mathbf{D}}^{\flat}$ is defined as for $\Gamma_{\mathbf{D}}$, but with the linear forms $L_j(U,V)$ replaced by $L_j(V,U)$. Thus an application of [dlBB08, Ths. 3 and 4] with $(j,k)=(0,2)$ produces (8.9) with $i=3$, and

$$c_3 = \omega_{\mathscr{R}_m^\flat}(\infty)\omega_{0,\mathbf{d}}^\flat(2)\prod_{p>2}\omega_{\mathbf{d},\mathbf{D}}^\flat(p) = \omega_{\mathscr{R}_m}(\infty)\omega_{0,\mathbf{d}}^\flat(2)\prod_{p>2}\omega_{\mathbf{d},\mathbf{D}}(p).$$

Here the superscripts $\flat$ indicate that the local densities are taken with respect to the linear forms $L_j(V,U)$.

We are now ready to bring together our various estimates for $U_1(T), U_2(T)$ and $U_3(T)$ in (8.8). This leads to the asymptotic formula in the statement of the lemma, with leading constant

$$c_{\mathbf{d},\mathbf{D},\mathscr{R}_m} = \omega_{\mathscr{R}_m}(\infty)\Big(\omega_{1,\mathbf{d}}(2)+\omega_{0,\mathbf{d}}(2)+\omega_{0,\mathbf{d}}^\flat(2)\Big)\prod_{p>2}\omega_{\mathbf{d},\mathbf{D}}(p).$$

The statement of the lemma easily follows with recourse to definitions (8.5) and (8.6) of the local densities $\sigma_p(\mathbf{d},\mathbf{D})$. □

We will need to consider the effect of the error term in Lemma 8.1 on the quantity $N_1(B)$ that was described at the start of the section. Accordingly, let us write

$$N_1(B) = N_2(B) + E_1(B), \tag{8.10}$$

where $N_2(B)$ denotes the overall contribution from the main term in Lemma 8.1 and $E_1(B)$ denotes the contribution from the error term.

Lemma 8.2. *We have $E_1(B) \ll B\log(B)^{1+L-\eta+\varepsilon}$ for any $\varepsilon>0$.*

Proof. Inserting the error term in Lemma 8.1 into our expression for $N_1(B)$, we obtain

$$\begin{aligned} E_1(B) &\ll B\log(B)^{\varepsilon}\sum_{\ell\leqslant \log(B)^L}\sum_{\substack{\mathfrak{b}_1,\dots,\mathfrak{b}_4\in\widehat{\mathfrak{D}}\\ \mathrm{N}(\mathfrak{b}_j)\leqslant\log(B)^D}}\sum_{\substack{t\leqslant B\\ \mathrm{N}(\bigcap\mathfrak{b}_j)\mid t}} r\Big(\frac{t}{\mathrm{N}(\bigcap\mathfrak{b}_j)}\Big)\cdot\frac{1}{t\log(2B/t)^\eta}\\ &\ll B\log(B)^{L+\varepsilon}\sum_{\substack{\mathfrak{b}_1,\dots,\mathfrak{b}_4\in\widehat{\mathfrak{D}}\\ \mathrm{N}(\mathfrak{b}_j)\leqslant\log(B)^D}}\frac{1}{\mathrm{N}(\bigcap\mathfrak{b}_j)}\sum_{t\leqslant B_1}\frac{r(t)}{t\log(2B_1/t)^\eta}, \end{aligned}$$

where we have written $B_1 = B/\mathrm{N}(\bigcap\mathfrak{b}_j)$, for ease of notation. Combining the familiar (7.4) with partial summation, we therefore conclude that

$$E_1(B) \ll B\log(B)^{1+L-\eta+\varepsilon}\sum_{\substack{\mathfrak{b}_1,\dots,\mathfrak{b}_4\in\widehat{\mathfrak{D}}\\ \mathrm{N}(\mathfrak{b}_j)\leqslant\log(B)^D}}\frac{1}{\mathrm{N}(\bigcap\mathfrak{b}_j)} \ll B\log(B)^{1+L-\eta+\varepsilon}.$$

This concludes the proof of the lemma. □

Let $\epsilon \in \{-1,+1\}$ and $|z|<1$. To proceed further we will need to calculate expressions for the geometric series

$$S^{\epsilon}(z)=\sum_{\mathbf{n}\in\mathbf{Z}_{\geqslant 0}^4}\epsilon^{n_1+n_2+n_3+n_4}z^{m(\mathbf{n})}, \tag{8.11}$$

where $m(\mathbf{n})=\max_{i\neq j}\{n_i+n_j\}$. We claim that

$$S^{-1}(z)=\frac{(1-z)^2}{(1+z)^2(1+z^2)},\quad S^{+1}(z)=\frac{1+2z+6z^2+2z^3+z^4}{(1-z)^4(1+z)^2}. \tag{8.12}$$

A similar calculation can be found in [HB03, §8] and so we shall be brief. The key idea is to observe that

$$S^{\epsilon}(z)=S_0^{\epsilon}(z)+2S_1^{\epsilon}(z)+z^2S^{\epsilon}(z),$$

where for any $\epsilon\in\{-1,+1\}$, $S_0^{\epsilon}(z)$ (resp. $S_1^{\epsilon}(z)$) denotes the contribution from $\mathbf{n}$ such that $\min\{n_1,n_2\}=\min\{n_3,n_4\}=0$ (resp. $\min\{n_1,n_2\}\geqslant 1$ and $\min\{n_3,n_4\}=0$). The calculation of $S_0^{\epsilon}(z)$ and $S_1^{\epsilon}(z)$ is straightforward and readily confirms the expressions for $S^{\epsilon}(z)$ in (8.12).

We now have the tools in place with which to produce a uniform upper bound for the constant (8.7) appearing in Lemma 8.1. This is achieved in the following result.

Lemma 8.3. *Let $\varepsilon>0$. Then we have*

$$c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}}\ll\frac{(D_1D_2D_3D_4)^{\varepsilon}}{[D_1D_2,\dots,D_3D_4]},$$

where $\mathbf{d},\mathbf{D}$ are given by (6.3).

Proof. It follows from [dlBB08, Th. 4] that $\omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty)=\pi^4\operatorname{Vol}(\mathscr{R}_{\boldsymbol{m}})\ll 1$. Similarly, we have $\sigma_2(\mathbf{d},\mathbf{D})\leqslant 2^4$, since for any $A\in\mathbf{Z}$ there are at most 2^{n+1} solutions of the congruence $s^2+t^2\equiv A \bmod 2^n$ by [dlBB08, eq. (2.5)]. Thus we have

$$c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}}\ll\prod_{p>2}|\sigma_p(\mathbf{d},\mathbf{D})|,$$

where $\sigma_p(\mathbf{d},\mathbf{D})$ is given by (8.5). For $p>2$, an application of [dlBB08, Th. 4] yields

$$\sigma_p(\mathbf{d},\mathbf{D})=\Big(1-\frac{\chi(p)}{p}\Big)^4\sum_{\nu_1,\dots,\nu_4=0}^{\infty}\frac{\chi(p)^{\nu_1+\nu_2+\nu_3+\nu_4}}{\varrho(p^{\max\{\mu_1,\lambda_1+\nu_1\}},\dots,p^{\max\{\mu_4,\lambda_4+\nu_4\}})},$$

where ϱ is the determinant given in (6.6) and $\boldsymbol{\lambda},\boldsymbol{\mu}$ are given by (8.4). Using the multiplicativity of ϱ we may clearly write

$$\prod_{p>2}|\sigma_p(\mathbf{d},\mathbf{D})|=\frac{1}{\varrho(\mathbf{D})}\prod_{p>2}|\sigma_p'(\mathbf{d},\mathbf{D})|,$$

where now

$$\sigma'_p(\mathbf{d},\mathbf{D}) = \Big(1-\frac{\chi(p)}{p}\Big)^4 \sum_{\nu_1,\dots,\nu_4=0}^{\infty} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3+\nu_4}\varrho(p^{\mu_1},\dots,p^{\mu_4})}{\varrho(p^{\max\{\mu_1,\lambda_1+\nu_1\}},\dots,p^{\max\{\mu_4,\lambda_4+\nu_4\}})}.$$

In view of (6.9), it will suffice to show that

$$\prod_{p>2}|\sigma'_p(\mathbf{d},\mathbf{D})| \ll (D_1D_2D_3D_4)^{\varepsilon} \tag{8.13}$$

in order to complete the proof of the lemma.

Recall definition (6.1) of Δ and write $D = D_1D_2D_3D_4$. For any $\mathbf{n}\in\mathbf{Z}^4_{\geqslant 0}$, let $m(\mathbf{n}) = \max_{i\neq j}\{n_i+n_j\}$. Then for $p\nmid \Delta D$, it follows from (6.7) that

$$\sigma'_p(\mathbf{d},\mathbf{D}) = \Big(1-\frac{\chi(p)}{p}\Big)^4 \sum_{\nu_1,\dots,\nu_4=0}^{\infty} \frac{\chi(p)^{\nu_1+\nu_2+\nu_3+\nu_4}}{p^{m(\boldsymbol{\nu})}}.$$

In the notation of (8.11) we deduce from (8.12) that

$$\sigma'_p(\mathbf{d},\mathbf{D}) = \Big(1-\frac{1}{p}\Big)^4 S^{+1}(1/p) = \frac{1+2/p+6/p^2+2/p^3+1/p^4}{(1+1/p)^2},$$

if $p\equiv 1 \bmod 4$, and

$$\sigma'_p(\mathbf{d},\mathbf{D}) = \Big(1+\frac{1}{p}\Big)^4 S^{-1}(1/p) = \frac{(1-1/p^2)^2}{(1+1/p^2)},$$

if $p\equiv 3 \bmod 4$. Thus $\sigma'_p(\mathbf{d},\mathbf{D}) = 1+O(1/p^2)$ for $p\nmid\Delta D$.

Suppose now that $p\mid \Delta D$. Then (6.8) implies that

$$\sigma'_p(\mathbf{d},\mathbf{D}) \ll \sum_{\nu_1,\dots,\nu_4=0}^{\infty} \frac{1}{p^{m(\mathbf{n})-m(\boldsymbol{\mu})}} \ll 1,$$

where $\mathbf{n} = (\max\{\mu_1,\lambda_1+\nu_1\},\dots,\max\{\mu_4,\lambda_4+\nu_4\})$. Putting this together with our treatment of the factors corresponding to $p\nmid\Delta D$, we are easily led to the desired upper bound in (8.13). This therefore concludes the proof of the lemma. □

9. The dénouement

Let $\varepsilon>0$. Take $D=4$ and $L=2\eta/3$ in Lemmata 7.2 and 8.2. We therefore deduce that

$$N(B) = N_2(B) + O\Big(B\log(B)^{1-\eta/3+\varepsilon}\Big)$$

via (7.3) and (8.10), where $N_2(B)$ is equal to

$$\frac{B}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\substack{\boldsymbol{m}\in\Sigma\\ \mathfrak{a}\in\Sigma'}} \mu(\mathfrak{a}) \sum_{\substack{\ell\leqslant \log(B)^{2\eta/3}\\ 2\nmid \ell}} \mu(\ell)$$

$$\times \sum_{\substack{\mathfrak{b}_1,\dots,\mathfrak{b}_4\in\widehat{\mathfrak{D}}\\ \mathrm{N}(\mathfrak{b}_j)\leqslant \log(B)^4}} \prod_{j=1}^{4} \mu(\mathfrak{b}_j) c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}} \sum_{\substack{t\in\mathfrak{D}\cap[1,B]\\ \gcd(t,\mathrm{N}(\mathfrak{a}))=1\\ \mathrm{N}(\bigcap \mathfrak{b}_j)\mid t}} \frac{r(t/\mathrm{N}(\bigcap\mathfrak{b}_j))}{t}.$$

Here $c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}}$ is given by (8.7), with $\mathbf{d},\mathbf{D}$ being given by (6.3) and $\mathscr{R}_{\boldsymbol{m}}$ given by (6.2). The following simple result is classical and allows us to carry out the inner summation over t. The proof follows from a routine analysis of the corresponding Dirichlet series and will not be presented here.

Lemma 9.1. *Let $m\in\mathbf{Z}_{>0}$ and let $T\geqslant 1$. Then for any $\varepsilon>0$, we have*

$$\sum_{\substack{t\in\mathfrak{D}\cap[1,T]\\ \gcd(t,m)=1}} \frac{r(t)}{t} = C_m\log(T) + O(m^{\varepsilon}),$$

where

$$C_m = 2L(1,\chi)\prod_{p\equiv 3 \bmod 4}\Big(1-\frac{1}{p^2}\Big)\prod_{\substack{p\mid m\\ p\equiv 1 \bmod 4}}\Big(1-\frac{1}{p}\Big)^2.$$

Making the obvious change of variables it now follows from Lemma 9.1 that

$$\sum_{\substack{t\in\mathfrak{D}\cap[1,B]\\ \gcd(t,\mathrm{N}(\mathfrak{a}))=1\\ \mathrm{N}(\bigcap \mathfrak{b}_j)\mid t}} \frac{r(t/\mathrm{N}(\bigcap\mathfrak{b}_j))}{t} = \frac{c_{\mathfrak{a},\mathfrak{b}}\log(B)}{\mathrm{N}(\bigcap\mathfrak{b}_j)} + O(1),$$

where

$$c_{\mathfrak{a},\mathfrak{b}} = \begin{cases} C_{\mathrm{N}(\mathfrak{a})} & \text{if } \gcd(\mathrm{N}(\bigcap\mathfrak{b}_j),\mathrm{N}(\mathfrak{a}))=1,\\ 0 & \text{otherwise.}\end{cases}$$

In particular it is clear that $c_{\mathfrak{a},\mathfrak{b}}=O(1)$. Applying Lemma 8.3 it is easy to conclude that the overall contribution to $N_2(B)$ from the error term in this estimate is

$$\begin{aligned} &\ll B\sum_{\ell\leqslant\log(B)^{2\eta/3}} \ell^{\varepsilon} \sum_{\mathrm{N}(\mathfrak{b}_j)\leqslant\log(B)^4} \frac{(\mathrm{N}(\mathfrak{b}_1)\cdots\mathrm{N}(\mathfrak{b}_4))^{\varepsilon}}{[\mathrm{N}(\mathfrak{b}_1)\mathrm{N}(\mathfrak{b}_2),\dots,\mathrm{N}(\mathfrak{b}_3)\mathrm{N}(\mathfrak{b}_4)]}\\ &\ll B\log(B)^{2\eta/3+\varepsilon}\prod_{p\leqslant\log(B)^4} S^{+1}(1/p)\end{aligned}$$

in the notation of (8.11). This is therefore seen to be $O(B\log(B)^{2\eta/3+\varepsilon})$ via (8.12).

In conclusion, we may write

$$N(B) = N_3(B) + O\Big(B\log(B)^{1-\eta/3+\varepsilon}\Big),$$

where now $N_3(B)$ is given by

$$\frac{B\log(B)}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}}\sum_{\substack{\boldsymbol{m}\in\Sigma\\ \mathfrak{a}\in\Sigma'}}\mu(\mathfrak{a})\sum_{\substack{\ell\leqslant\log(B)^{2\eta/3}\\ 2\nmid\ell}}\mu(\ell)\sum_{\substack{\mathfrak{b}_1,\dots,\mathfrak{b}_4\in\widehat{\mathfrak{D}}\\ \mathrm{N}(\mathfrak{b}_j)\leqslant\log(B)^4}}\frac{c_{\mathfrak{a},\mathfrak{b}}c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}}}{\mathrm{N}(\bigcap\mathfrak{b}_j)}\prod_{j=1}^{4}\mu(\mathfrak{b}_j).$$

Here we have used (8.1) to observe that $1-\eta/3 > 2\eta/3$. Finally, through a further application of Lemma 8.3, it is now a trivial matter to re-apply the proof of Lemma 7.2 to show that the summations over ℓ and $\mathfrak{b}_j$ can be extended to infinity with error $O(B\log(B)^{1-\eta/3+\varepsilon})$. This therefore leads to the final outcome that

$$N(B) = cB\log(B) + O\Big(B\log(B)^{1-\eta/3+\varepsilon}\Big)$$

for any $\varepsilon > 0$, where if $c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}}$ is given by (8.7) and $\mathbf{d},\mathbf{D}$ are given by (6.3), then

$$c = \frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}}\sum_{\substack{\boldsymbol{m}\in\Sigma\\ \mathfrak{a}\in\Sigma'}}\mu(\mathfrak{a})\sum_{\substack{\ell=1\\ 2\nmid\ell}}^{\infty}\mu(\ell)\sum_{\mathfrak{b}_1,\dots,\mathfrak{b}_4\in\widehat{\mathfrak{D}}}\frac{c_{\mathfrak{a},\mathfrak{b}}c_{\mathbf{d},\mathbf{D},\mathscr{R}_{\boldsymbol{m}}}}{\mathrm{N}(\bigcap\mathfrak{b}_j)}\prod_{j=1}^{4}\mu(\mathfrak{b}_j). \tag{9.1}$$

10. **Jumping down**

We shall now relate the constant c defined by equation (9.1) with the one expected, as required to complete the proof of Theorem 3.3.

10.1. *Expression in terms of volumes.* Let us first recall that the adelic set $\mathcal{T}_{\boldsymbol{n}}(\boldsymbol{A}_{\mathbf{Q}})$ comes with a canonical measure which is defined as follows. The canonical line bundle on $\omega_{\mathcal{T}_{\boldsymbol{n}}}$ is trivial [Pey01, lemme 3.1.12] and the invertible functions on $\mathcal{T}_{\boldsymbol{n}}$ are constant. Therefore up to multiplication by a constant there exists a unique section $\breve{\omega}_{\mathcal{T}_{\boldsymbol{n}}}$ of $\omega_{\mathcal{T}_{\boldsymbol{n}}}$ which does not vanish. By [Wei82, §2], this form defines a measure $\boldsymbol{\omega}_{\mathcal{T}_{\boldsymbol{n}},v}$ on $\mathcal{T}_{\boldsymbol{n}}(\mathbf{Q}_v)$ for any place v of $\mathbf{Q}$. According to [Pey01, lemme 3.1.14], the product $\prod_v \boldsymbol{\omega}_{\mathcal{T}_{\boldsymbol{n}},v}$ converges and defines a measure on $\mathcal{T}_{\boldsymbol{n}}(\boldsymbol{A}_{\mathbf{Q}})$. By the product formula, this measure does not depend on the choice of the section $\breve{\omega}_{\mathcal{T}_{\boldsymbol{n}}}$. Let us now describe explicitly how to construct such a section $\breve{\omega}_{\mathcal{T}_{\boldsymbol{n}}}$.

Notation 10.1. Let $\mathscr{X}_{\boldsymbol{n}}$ be the subscheme of

$$\mathbf{A}^8_{\mathbf{Z}} = \mathrm{Spec}(\mathbf{Z}[X_j, Y_j, 1\leqslant j\leqslant 4])$$

defined by equations (4.2). Then $\mathscr{Y}_{\boldsymbol{n}}$ is the product $\mathscr{X}_{\boldsymbol{n}}\times\mathbf{A}^2_{\mathbf{Z}}$. We denote by $\mathscr{X}^\circ_{\boldsymbol{n}}$ the complement of the origin in $\mathscr{X}_{\boldsymbol{n}}$. For three distinct elements j,k,l of

$\{1, 2, 3, 4\}$, let us denote by $P_{j,k,l}$ the quadratic form

$$\Delta_{j,k} n_l (X_l^2 + Y_l^2) + \Delta_{k,l} n_j (X_j^2 + Y_j^2) + \Delta_{l,j} n_k (X_k^2 + Y_k^2).$$

Then we have the relations

$$\begin{aligned} a_j P_{k,l,m} + a_k P_{l,m,j} + a_l P_{m,j,k} + a_m P_{j,k,l} = 0, \\ b_j P_{k,l,m} + b_k P_{l,m,j} + b_l P_{m,j,k} + b_m P_{j,k,l} = 0 \end{aligned}$$

whenever $\{j, k, l, m\} = \{1, 2, 3, 4\}$. Since $\Delta_{1,2} = 1$, the scheme $\mathscr{X}_{\boldsymbol{n}}^{\circ}$ is the complete intersection in $\mathbf{A}_{\mathbf{Z}}^8 - \{0\}$ of the quadrics defined by $P_{1,2,3}$ and $P_{1,2,4}$. Therefore the corresponding Leray form is a nonzero section of the canonical line bundle $\omega_{\mathscr{X}_{\boldsymbol{n},\mathbf{Q}}^{\circ}}$. On $\mathbf{A}_{\mathbf{Z}}^2$, we may take the natural form $\frac{\partial}{\partial X_0} \wedge \frac{\partial}{\partial Y_0}$. The exterior product of these forms gives a form on an open subset of $\mathscr{Y}_{\boldsymbol{n}}$, and by restriction, a form $\breve{\omega}_{\mathcal{T}_{\boldsymbol{n}}}$ on $\mathcal{T}_{\boldsymbol{n}}$ which does not vanish. We denote by $\boldsymbol{\omega}_{\boldsymbol{n},v}$ the corresponding measure on $\mathscr{Y}_n(\mathbf{Q}_v)$ for $v \in \mathrm{Val}(\mathbf{Q})$.

LEMMA 10.2. *Let $\boldsymbol{m} \in \Sigma$ and $\mathfrak{a} \in \Sigma'$. Let $\mathfrak{b} = (\mathfrak{b}_j)_{j \in \{1,2,3,4\}}$ belong to $\widehat{\mathfrak{D}}^4$. Let ℓ be an odd integer. Let d_j and D_j be defined by formula* (6.3). *Then for any prime number p, we have*

$$\boldsymbol{\omega}_{\boldsymbol{n},p}(\mathscr{D}_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}^3) = \beta_p p^{-v_p\left(\mathrm{N}\left(\bigcap_j \mathfrak{b}_j\right)\right)} \lim_{n \to \infty} p^{-6n} N_{\mathbf{d},\mathbf{D}}(p^n),$$

where

$$\beta_p = \begin{cases} \frac{1}{2} & \text{if } p = 2, \\ 1 - \frac{1}{p^2} & \text{if } p \equiv 3 \bmod 4, \\ \left(1 - \frac{1}{p}\right)^2 & \text{if } p \mid \prod_j \mathrm{N}(\mathfrak{a}_j^+) \text{ and } p \equiv 1 \bmod 4, \\ 0 & \text{if } p \mid \prod_j \mathrm{N}(\mathfrak{a}_j^+) \text{ and } p \mid \prod_j \mathrm{N}(\mathfrak{b}_j), \\ 1 & \text{otherwise.} \end{cases}$$

Proof. In the product $\mathscr{X}_{N(\mathfrak{a}\mathfrak{b})\boldsymbol{m}} \times \mathbf{A}_{\mathbf{Z}}^2$, the domain $\mathscr{D}_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,p}^3$ decomposes as a product. The projection onto the eight coordinates X_j, Y_j, where j belonging to $\{1, 2, 3, 4\}$, gives an isomorphism from the complete intersection in $\mathbf{A}_{\mathbf{Z}}^{10} - \{0\}$ given by the equations

$$L_j(U, V) = n_j(X_j^2 + Y_j^2)$$

for $j \in \{1, 2, 3, 4\}$ to the scheme $\mathscr{X}_{\boldsymbol{n}}^{\circ}$. Moreover this isomorphism map is compatible with the respective Leray forms. Since the measure defined by the Leray measure coincides with the counting measure (see, e.g., [Lac82, Prop. 1.14]), the volume of the first component is equal to $\lim_{n \to \infty} p^{-6n} N_{\mathbf{d},\mathbf{D}}(p^n)$. The measure on $\mathbf{A}_{\mathbf{Z}}^2$ is the standard Haar measure. On the other hand, the image of the domain in $\mathbf{Z}_p^2$ may be described as follows:

- It is $\mathbf{Z}[i]_{1+i} - (1 + i)\mathbf{Z}[i]_{1+i}$ if $p = 2$.
- It is $\mathbf{Z}_p^2 - p\mathbf{Z}_p^2$ if $p \equiv 3 \bmod 4$.

- It is the set of $(x, y) \in \mathbf{Z}_p^2$ such that p does not divide $\mathrm{N}(x+iy)$ if $p \mid \prod_j \mathrm{N}(\mathfrak{a}_j^+)$, the prime p does not divide $\mathrm{N}(\bigcap_j \mathfrak{b}_j)$, and $p \equiv 1 \bmod 4$.
- It is empty if $p \mid \prod_j \mathrm{N}(\mathfrak{a}_j^+)$ and $p \mid \prod_j \mathrm{N}(\mathfrak{b}_j)$.
- It is $(\bigcap_j \mathfrak{b}_j)\mathbf{Z}_p[i]$ otherwise.

Therefore $\beta_p p^{-v_p\left(\mathrm{N}\left(\bigcap_j \mathfrak{b}_j\right)\right)}$ is the volume of this component. □

LEMMA 10.3. *Let* $\boldsymbol{m} \in \Sigma$ *and* $\mathfrak{a} \in \Sigma'$. *Let* $\mathfrak{b} = (\mathfrak{b}_j)_{j \in \{1,2,3,4\}}$ *belong to* $\widehat{\mathfrak{D}}^4$. *We put* $\boldsymbol{n} = \mathrm{N}(\mathfrak{a}\mathfrak{b})\boldsymbol{m}$. *Let* ℓ *be an odd integer. For any real number* B, *we have*

$$\boldsymbol{\omega}_{\boldsymbol{n},\infty}(\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,\infty}(B)) = \frac{4L(1,\chi)\pi^4}{\prod_{j=1}^4 n_j} \operatorname{Vol}(\mathscr{R}_{\boldsymbol{m}}) f(B),$$

where $f(B) = \int_0^{\log(B)} u e^u \,\mathrm{d}u = B\log(B) - B + 1$.

Proof. The functions U and V on $\mathscr{Y}_{\boldsymbol{n}} = \mathscr{X}_{\boldsymbol{n}} \times \mathbf{A}^2$ are induced by functions on $\mathscr{X}_{\boldsymbol{n}}$ which we shall also denote by U and V. Let $H_{F,\infty} : \mathscr{X}_{\boldsymbol{n}}(\mathbf{R}) \to \mathbf{R}$ and $H_{E,\infty} : \mathbf{R}^2 \to \mathbf{R}$ be defined by

$$H_{F,\infty}(R) = \max(|U(R)|, |V(R)|) \quad \text{and} \quad H_{E,\infty}(x_0, y_0) = x_0^2 + y_0^2.$$

Then the domain $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,\infty}(B)$ is the set of $(R, (x_0, y_0)) \in \mathscr{X}_{\boldsymbol{n}}(\mathbf{R}) \times \mathbf{R}^2$ such that

$$H_{F,\infty}(R) \geqslant 1, \quad H_{E,\infty}(x_0, y_0) \geqslant 1, \quad \text{and} \quad H_{F,\infty}(R)^2 H_{E,\infty}(x_0, y_0) \leqslant B.$$

Let us denote by $v_{\boldsymbol{n},1}(t)$ (resp. $v_2(t)$) the volume of the set of $R \in \mathscr{X}_{\boldsymbol{n}}(\mathbf{R})$ (resp. $(x_0, y_0) \in \mathbf{R}^2$) such that $H_{F,\infty}(R) \leqslant t$ (resp. $H_{E,\infty}(x_0, y_0) \leqslant t$). Then the functions $v_{\boldsymbol{n},1}$ and v_2 are monomials of respective degrees 2 and 1. Therefore the volume of the domain $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell,\infty}(B)$ is given by

$$v_{\boldsymbol{n},1}(1)v_2(1) \int_{\substack{t \geqslant 1, u \geqslant 1 \\ t^2 u \leqslant B}} 2t \,\mathrm{d}u \,\mathrm{d}t = v_{\boldsymbol{n},1}(1)v_2(1)f(B).$$

To compute the value of $v_{\boldsymbol{n},1}(1)$, we may use the change of variables $x'_j = \sqrt{|n_j|}x_j$ and $y'_j = \sqrt{|n_j|}y_j$. Since the Leray form may be locally described as

$$\begin{vmatrix} \frac{\partial P_{1,2,3}}{\partial X_1} & \frac{\partial P_{1,2,3}}{\partial X_2} \\ \frac{\partial P_{1,2,4}}{\partial X_1} & \frac{\partial P_{1,2,4}}{\partial X_2} \end{vmatrix}^{-1} \mathrm{d}X_3 \,\mathrm{d}X_4 \prod_{j=1}^4 \mathrm{d}Y_j = (4\Delta_{3,4}X_1X_2)^{-1} \,\mathrm{d}X_3 \,\mathrm{d}X_4 \prod_{j=1}^4 \mathrm{d}Y_j,$$

we get that $v_{\boldsymbol{n},1}(1) = v_{\boldsymbol{\varepsilon},1}(1) \prod_{j=1}^4 n_j^{-1}$, where $\varepsilon_j = \operatorname{sgn}(n_j) = \operatorname{sgn}(m_j)$. It follows that $v_{\boldsymbol{n},1}(1) = (\prod_{j=1}^4 n_j)^{-1}\pi^4 \operatorname{Vol}(\mathscr{R}_{\boldsymbol{m}})$. We conclude the proof with the equalities $v_2(1) = \pi = 4L(1,\chi)$. □

PROPOSITION 10.4. *Let $\boldsymbol{m} \in \Sigma$ and $\mathfrak{a} \in \Sigma'$. Let $\mathfrak{b} = (\mathfrak{b}_j)_{j\in\{1,2,3,4\}}$ belong to $\widehat{\mathfrak{D}}^4$. Let ℓ be an odd integer. Then*

$$\frac{c_{\mathfrak{a},\mathfrak{b}} c_{\mathbf{d},\mathbf{D},\mathscr{R}}}{\mathrm{N}(\bigcap \mathfrak{b}_j)} f(B) = \mathrm{Vol}(\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell}(B)),$$

where $f(B) = B\log(B) - B + 1$.

Proof. This follows from Lemmata 10.2 and 10.3; indeed, by [dlBB08, eq. (2.8)], we have $\omega_{\mathscr{R}_{\boldsymbol{m}}}(\infty) = \pi^4 \mathrm{Vol}(\mathscr{R}_{\boldsymbol{m}})$ and

$$\prod_{p\in\mathscr{P}} \sigma_p(\mathbf{d},\mathbf{D}) = \frac{1}{\prod_{j=1}^4 n_j} \prod_{p\in\mathscr{P}} \lim_{k\to\infty} p^{-6k} N_{\mathbf{d},\mathbf{D}}(p^k),$$

where $\boldsymbol{n} = N(\mathfrak{a}\mathfrak{b})\boldsymbol{m}$. □

10.2. *Moebius reversion.*

PROPOSITION 10.5. *Let B be a real number and $\boldsymbol{m}$ belong to Σ. Then*

$$\mathrm{Vol}(\mathscr{D}_{\boldsymbol{m}}(B)) = \sum_{\mathfrak{a}\in\Sigma'} \sum_{\mathfrak{b}\in\widehat{\mathfrak{D}}^4} \sum_{\ell\,\mathrm{odd}} \mu(\mathfrak{a})\mu(\mathfrak{b})\mu(\ell)\,\mathrm{Vol}(\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell}(B)).$$

Proof. For any $\boldsymbol{\lambda} \in T_{\boldsymbol{\Delta}}(\mathbf{Q}) \cap \mathbf{Z}_{\boldsymbol{\Delta}}$ and any $\boldsymbol{n} \in \mathbf{Z}^4$, the multiplication by $\boldsymbol{\lambda}$ defines an isomorphism from $\mathscr{Y}_{N(\boldsymbol{\lambda})\boldsymbol{n}}$ to $\mathscr{Y}_{\boldsymbol{n}}$. Therefore it sends the canonical form on the adelic set $\mathscr{Y}_{N(\boldsymbol{\lambda})\boldsymbol{n}}(\boldsymbol{A}_{\mathbf{Q}})$ onto the canonical form on $\mathscr{Y}_{\boldsymbol{n}}(\boldsymbol{A}_{\mathbf{Q}})$. Therefore the volume of $\mathscr{D}^3_{\boldsymbol{m},\mathfrak{a},\mathfrak{b},\ell}(B)$ coincides with the volume of its image in $\mathscr{Y}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}})$. The formula then follows from Lemma 5.28 and the proofs of Propositions 5.32 and 5.34. □

10.3. *The constant.*

PROPOSITION 10.6. *We have*

$$C_H(S)B\log(B) = \frac{1}{\sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}} \sum_{\boldsymbol{m}\in\Sigma} \mathrm{Vol}(\mathscr{D}_{\boldsymbol{m}}(B)) + O(B).$$

Proof. The following proof is based upon the ideas of P. Salberger [Sal98], as described in [Pey01, §5.3].

We may identify ω_S^{-1} with $\mathscr{O}_{S'}(1)$ (see Lemma 2.2). This enables us to define an adelic metric on ω_S^{-1} by

$$\|y\|_v = \begin{cases} \min\left(\left|\frac{y}{X_0(x)}\right|, \left|\frac{y}{X_1(x)}\right|, \left|\frac{y}{X_2(x)}\right|, C\left|\frac{y}{X_3(x)}\right|, C\left|\frac{y}{X_4(x)}\right|\right) & \text{if } v = \infty, \\ \min_{0\leqslant i\leqslant 4}\left(\left|\frac{y}{X_i(x)}\right|_v\right) & \text{otherwise} \end{cases}$$

for $x \in S'(\mathbf{Q}_v)$ and y in the corresponding fiber $\mathscr{O}_{S'}(1)_x \otimes \mathbf{Q}_v$, with the constant C defined in Notation 3.2. This adelic metric defines the height used throughout the text. Let v be a place of $\mathbf{Q}$. We denote by $\boldsymbol{\omega}_{H,v}$ the measure on $S(\mathbf{Q}_v)$ corresponding to the adelic metric on ω_S^{-1} (see [Pey95, §2]). Let us recall that on a split torus $\mathbf{G}_m^n$, the form $\bigwedge_{j=1}^n \xi_j^{-1} d\xi_j$, where $(\xi_j)_{1\leqslant j\leqslant n}$ is a basis of $X^*(\mathbf{G}_m^n)$, up to sign does not depend on the choice of the basis. Therefore there is a canonical Haar measure on $T_{\mathrm{NS}}(\mathbf{Q}_v)$ which we shall denote by $\boldsymbol{\omega}_{T_{\mathrm{NS}},v}$. Let $\boldsymbol{m}$ be an element of Σ. The functions H_w defined in Definition 5.18 may been seen as the composite of the metrics on ω_S^{-1} with the natural morphism from the universal torsor $\mathcal{T}_{\boldsymbol{m}}$ to the line bundle ω_S^{-1}. Let $U \neq \emptyset$ be an open subset of $\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_v))$. According to [Pey01, lemme 3.1.14] and [Pey98, §4.4], if $s : U \to \mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_v)$ is a continuous section of $\pi_{\boldsymbol{m}}$, then the measure $\boldsymbol{\omega}_{\boldsymbol{m},v}$ is characterised by the relation

(10.1)

$$\int_{\pi_{\boldsymbol{m}}^{-1}(U)} f(y)\boldsymbol{\omega}_{\boldsymbol{m},v}(y) = \int_U \int_{T_{\mathrm{NS}}(\mathbf{Q}_v)} f(t.s(x))H_v(t.s(x))\boldsymbol{\omega}_{T_{\mathrm{NS}},v}(t)\boldsymbol{\omega}_{H,v}(x)$$

for any continuous function f on $\pi_{\boldsymbol{m}}^{-1}(U)$ with compact support.

By Lemmata 5.8 and 5.14, for any prime number p, $\mathscr{D}_{\boldsymbol{m},p}$ is a fundamental domain in $\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)$ under the action of $T_{\mathrm{NS}}(\mathbf{Q}_p)$ modulo $T_{\mathrm{NS}}(\mathbf{Z}_p)$. Moreover, by definition, we have that $\mathscr{D}_{\boldsymbol{m},p}$ is contained in $\widehat{\pi}_{\boldsymbol{m}}^{-1}(\mathscr{T}_{\mathrm{spl}}(\mathbf{Z}_p))$ and thus H_p is equal to 1 on $\mathscr{D}_{\boldsymbol{m},p}$. Using (10.1), we get that

$$\boldsymbol{\omega}_{\boldsymbol{m},p}(\pi_{\boldsymbol{m}}^{-1}(U) \cap \mathscr{D}_{\boldsymbol{m},p}) = \boldsymbol{\omega}_{T_{\mathrm{NS}},p}(T_{\mathrm{NS}}(\mathbf{Z}_p))\boldsymbol{\omega}_{H,v}(U)$$

for any open subset U of $\pi_{\boldsymbol{m}}(\mathscr{D}_{\boldsymbol{m},p})$.

The maps $\log \circ H_F$, $\log \circ H_E$ define a map $\log_\infty : \mathcal{T}_{\boldsymbol{m}}(\mathbf{R}) \to \mathrm{Pic}(S)^\vee \otimes_{\mathbf{Z}} \mathbf{R}$, and using $\log_\infty \times \pi_{\boldsymbol{m}}$, we get a homeomorphism

$$\mathcal{T}_{\boldsymbol{m}}(\mathbf{R}) \to \mathrm{Pic}(S)^\vee \otimes_{\mathbf{Z}} \mathbf{R} \times \pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{R})).$$

Let

$$T^1_{\mathrm{NS}}(\mathbf{R}) = \{t \in T_{\mathrm{NS}}(\mathbf{R}),\ \forall \chi \in \mathrm{Pic}(S), |\chi(t)| = 1\}.$$

Then for any real number B and any open subset U of $\pi_m(\mathscr{D}_{\boldsymbol{m},\infty}(B)$, we get

$$\begin{aligned}
&\boldsymbol{\omega}_{\boldsymbol{m},\infty}(\pi_{\boldsymbol{m}}^{-1}(U) \cap \mathscr{D}_{\boldsymbol{m},\infty}(B)) \\
&\quad = \int_{\{y \in C_{\mathrm{eff}}(S)^\vee,\ \langle \omega_S^{-1}, y\rangle \leqslant \log(B)\}} e^{\langle \omega_S^{-1}, y\rangle}\, \mathrm{d}y \times \omega_{T_{\mathrm{NS}}}(T^1_{\mathrm{NS}}(\mathbf{R}))\, \omega_{H,\infty}(U) \\
&\quad = \alpha(S)\boldsymbol{\omega}_{T_{\mathrm{NS}},\infty}(T^1_{\mathrm{NS}}(\mathbf{R}))\, \boldsymbol{\omega}_{H,\infty}(U)f(B),
\end{aligned}$$

where $C_{\mathrm{eff}}(S)^\vee$ is the dual to the closed cone in $\mathrm{Pic}(S) \otimes_{\mathbf{Z}} \mathbf{R}$ generated by the effective divisors.

Taking the product over all places of $\mathbf{Q}$, we get the formula
(10.2)

$$\boldsymbol{\omega}_{\boldsymbol{m}}(\mathscr{D}_{\boldsymbol{m}}(B)) = \alpha(S)\boldsymbol{\omega}_{T_{\mathrm{NS}},\infty}(T^1_{\mathrm{NS}}(\mathbf{R}))\boldsymbol{\omega}_{H,\infty}(\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{R}))) \int_0^{\log(B)} ue^u \,\mathrm{d}u$$
$$\times \left(\prod_{p\in\mathscr{P}} L_p(1,\mathrm{Pic}(\overline{S}))\boldsymbol{\omega}_{T_{\mathrm{NS}},p}(T_{\mathrm{NS}}(\mathbf{Z}_p))\right)$$
$$\times \left(\prod_{p\in\mathscr{P}} L_p(1,\mathrm{Pic}(\overline{S}))^{-1}\boldsymbol{\omega}_{H,p}(\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\mathbf{Q}_p)))\right).$$

By Lemma 5.3, the map from $T_{\mathrm{NS}}(\mathbf{Q})$ to $\bigoplus_{p\in\mathscr{P}} X_*(T_{\mathrm{NS}})_p$ is surjective. It follows that

$$T^1_{\mathrm{NS}}(\boldsymbol{A}_{\mathbf{Q}}) = (T^1_{\mathrm{NS}}(\mathbf{R}) \times \prod_{p\in\mathscr{P}} T_{\mathrm{NS}}(\mathbf{Z}_p)).T_{\mathrm{NS}}(\mathbf{Q}),$$

and we get an exact sequence

$$1 \longrightarrow T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}} \longrightarrow T^1_{\mathrm{NS}}(\mathbf{R}) \times \prod_{p\in\mathscr{P}} T_{\mathrm{NS}}(\mathbf{Z}_p) \longrightarrow T^1_{\mathrm{NS}}(\boldsymbol{A}_{\mathbf{Q}})/T_{\mathrm{NS}}(\mathbf{Q}) \longrightarrow 1.$$

Combining this with formula (10.2) and the definitions of the adelic measures, we get the formula

$$\boldsymbol{\omega}_{\boldsymbol{m}}(\mathscr{D}_{\boldsymbol{m}}(B)) = \sharp T_{\mathrm{NS}}(\mathbf{Q})_{\mathrm{tors}}\alpha(S)\tau(T_{\mathrm{NS}})\,\boldsymbol{\omega}_H(\pi_m(\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}}))) \int_0^{\log(B)} ue^u \,\mathrm{d}u,$$

where $\tau(T_{\mathrm{NS}})$ denotes the Tamagawa number of T_{NS}. By Ono's main theorem [Ono63, §5], $\tau(T_{\mathrm{NS}})$ is equal to $\sharp H^1(\mathbf{Q},\mathrm{Pic}(\overline{S})/\sharp Ш^1(\mathbf{Q},T_{\mathrm{NS}})$ and using Salberger's argument [Sal98, proof of lemma 6.17] and Proposition 4.9, any point in $S(\boldsymbol{A}_{\mathbf{Q}})^{\mathrm{Br}}$ belongs to exactly $\sharp Ш^1(\mathbf{Q},T_{\mathrm{NS}})$ sets of the form $\pi_{\boldsymbol{m}}(\mathcal{T}_{\boldsymbol{m}}(\boldsymbol{A}_{\mathbf{Q}}))$. This concludes the proof of the proposition. □

References

[BM90] V. V. Batyrev and Y. I. Manin, Sur le nombre des points rationnels de hauteur borné des variétés algébriques, *Math. Ann.* **286** (1990), 27–43. MR 1032922. Zbl 0679.14008. http://dx.doi.org/10.1007/BF01453564.

[BT95] V. V. Batyrev and Y. Tschinkel, Rational points of bounded height on compactifications of anisotropic tori, *Internat. Math. Res. Notices* (1995), 591–635. MR 1369408. Zbl 0890.14008. http://dx.doi.org/10.1155/S1073792895000365.

[dlBB06] R. de la Bretèche and T. D. Browning, Sums of arithmetic functions over values of binary forms, *Acta Arith.* **125** (2006), 291–304. MR 2276196. Zbl 1159.11035. http://dx.doi.org/10.4064/aa125-3-6.

[dlBB08] R. de la Bretèche and T. D. Browning, Binary linear forms as sums of two squares, *Compos. Math.* **144** (2008), 1375–1402. MR 2474314. Zbl 05382617. http://dx.doi.org/10.1112/S0010437X08003692.

[Châ59] F. Châtelet, Points rationnels sur certaines courbes et surfaces cubiques, *Enseignement Math.* **5** (1959), 153–170 (1960). MR 0130218. Zbl 0100.27404.

[Châ66] ———, Points rationnels sur certaines surfaces cubiques, in *Les Tendances Géom. en Algèbre et Théorie des Nombres*, Éditions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 67–75. MR 0213353. Zbl 0178.24101.

[CTS77] J.-L. Colliot-Thélène and J.-J. Sansuc, La descente sur une variété rationnelle définie sur un corps de nombres, *C. R. Acad. Sci. Paris Sér. A-B* **284** (1977), A1215–A1218. MR 0447250. Zbl 0349.14015.

[CTS80] ———, La descente sur les variétés rationnelles, in *Journées de Géometrie Algébrique d'Angers, Juillet* 1979/*Algebraic Geometry, Angers*, 1979, Sijthoff & Noordhoff, Alphen aan den Rijn, 1980, pp. 223–237. MR 0605344. Zbl 0451.14018.

[CTS87] ———, La descente sur les variétés rationnelles. II, *Duke Math. J.* **54** (1987), 375–492. MR 0899402. Zbl 0659.14028. http://dx.doi.org/10.1215/S0012-7094-87-05420-2.

[CTSSD87a] J.-L. Colliot-Thélène, J.-J. Sansuc, and P. Swinnerton-Dyer, Intersections of two quadrics and Châtelet surfaces. I, *J. Reine Angew. Math.* **373** (1987), 37–107. MR 0870307. Zbl 0622.14029.

[CTSSD87b] ———, Intersections of two quadrics and Châtelet surfaces. II, *J. Reine Angew. Math.* **374** (1987), 72–168. MR 0876222. Zbl 0622.14030.

[Coo71] R. J. Cook, Simultaneous quadratic equations, *J. London Math. Soc.* **4** (1971), 319–326. MR 0289406. Zbl 0224.10021.

[CT88] D. F. Coray and M. A. Tsfasman, Arithmetic on singular Del Pezzo surfaces, *Proc. London Math. Soc.* **57** (1988), 25–87. MR 0940430. Zbl 0653.14018. http://dx.doi.org/10.1112/plms/s3-57.1.25.

[Dav63] H. Davenport, Cubic forms in sixteen variables, *Proc. Roy. Soc. Ser. A* **272** (1963), 285–303. MR 0155800. Zbl 0107.04102.

[Dra71] P. K. J. Draxl, *L*-Funktionen algebraischer Tori, *J. Number Theory* **3** (1971), 444–467. MR 0291099. Zbl 0231.12018.

[HB03] D. R. Heath-Brown, Linear relations amongst sums of two squares, in *Number Theory and Algebraic Geometry*, *London Math. Soc. Lecture Note Ser.* **303**, Cambridge Univ. Press, Cambridge, 2003, pp. 133–176. MR 2053459. Zbl 1161.11387.

[HBS02] R. Heath-Brown and A. Skorobogatov, Rational solutions of certain equations involving norms, *Acta Math.* **189** (2002), 161–177. MR 1961196. Zbl 1023.11033. http://dx.doi.org/10.1007/BF02392841.

[Isk71] V. A. Iskovskih, A counterexample to the Hasse principle for systems of two quadratic forms in five variables, *Mat. Zametki* **10** (1971), 253–257. MR 0286743. Zbl 0232.10015.

[Lac82] G. Lachaud, Une présentation adélique de la série singulière et du problème de Waring, *Enseign. Math.* **28** (1982), 139–169. MR 0670501. Zbl 0499.12010.

[Ono61] T. Ono, Arithmetic of algebraic tori, *Ann. of Math.* **74** (1961), 101–139. MR 0124326. Zbl 0119.27801. http://dx.doi.org/10.2307/1970307.

[Ono63] ———, On the Tamagawa number of algebraic tori, *Ann. of Math.* **78** (1963), 47–73. MR 0156851. Zbl 0122.39101. http://dx.doi.org/10.2307/1970502.

[Pey95] E. Peyre, Hauteurs et mesures de Tamagawa sur les variétés de Fano, *Duke Math. J.* **79** (1995), 101–218. MR 1340296. Zbl 0901.14025. http://dx.doi.org/10.1215/S0012-7094-95-07904-6.

[Pey98] ———, Terme principal de la fonction zêta des hauteurs et torseurs universels, in *Nombre et Répartition de Points de Hauteur Bornée*, *Astérisque* **251**, 1998, pp. 259–298. MR 1679842. Zbl 0966.14016.

[Pey01] ———, Torseurs universels et méthode du cercle, in *Rational Points on Algebraic Varieties*, *Progr. Math.* **199**, Birkhäuser, Basel, 2001, pp. 221–274. MR 1875176. Zbl 1092.14506.

[Pey03] ———, Points de hauteur bornée, topologie adélique et mesures de Tamagawa, *J. Théor. Nombres Bordeaux* **15** (2003), 319–349. MR 2019019. Zbl 1057.14031. http://dx.doi.org/10.5802/jtnb.405.

[Sal98] P. Salberger, Tamagawa measures on universal torsors and points of bounded height on Fano varieties, in *Nombre et Répartition de Points de Hauteur Bornée*, **251**, 1998, pp. 91–258. MR 1679841. Zbl 0959.14007.

[Sko01] A. Skorobogatov, *Torsors and Rational Points*, *Cambridge Tracts in Math.* **144**, Cambridge Univ. Press, Cambridge, 2001. MR 1845760. Zbl 0972.14015. http://dx.doi.org/10.1017/CBO9780511549588.

[Wei82] A. Weil, *Adeles and Algebraic Groups*, *Progr. Math.* **23**, Birkhäuser, Mass., 1982. MR 0670072. Zbl 0493.14028.

(Received: February 2, 2010)
(Revised: November 5, 2010)

Institut de Mathématiques de Jussieu, Université Paris 7, Paris, France
E-mail: breteche@math.jussieu.fr

School of Mathematics, University of Bristol, Bristol, England
E-mail: t.d.browning@bristol.ac.uk

Institut Fourier, Université de Grenoble I and
CNRS, Saint-Martin d'Hères, France
E-mail: Emmanuel.Peyre@ujf-grenoble.fr