RATIONAL POINTS ON CUBIC SURFACES

NIKLAS BROBERG

Abstract. Let k be an algebraic number field and $F(x_0, x_1, x_2, x_3)$ a non–singular cubic form with coefficients in k. Suppose that the projective cubic k–surface $X \subset \mathbb{P}^3_k$ given by $F = 0$ contains three coplanar lines defined over k, and let $U(k)$ be the set of k–points on X which does not lie on any line on X. We show that the number of points in $U(k)$, with height at most B, is $O_{F,\varepsilon}(B^{4/3+\varepsilon})$ for any $\varepsilon > 0$.

1. Introduction

It has been known since the 19th century that there are exactly 27 lines on any non–singular projective cubic surface X. If the form F defining X has coefficients in a field k which is not algebraically closed, then some of the lines may not be defined over k. One of the more interesting problems of diophantine geometry is to count the number $n_X(B)$ of rational points of height at most B on such a surface, and to study the asymptotic growth of this counting function as B tends to infinity. It appears that the lines on X defined over k play the dominant role in determining the behaviour of $n_X(B)$. It is known by a theorem of Schanuel [11] that if Z is such a rational line on X and $n_Z(B)$ is the number of rational points on Z of height not exceeding B, then

$$n_Z(B) = cB^2 + O(B \log B)$$

for some positive constant c which depends on k and the choice of coordinates. In this formula, the field k is a finite extension field of $\mathbb{Q}$, and the height function used in the definition of $n_Z(B)$ is the $[k : \mathbb{Q}]$ power of the absolute height on the set of algebraic points $\mathbb{P}^3(\overline{\mathbb{Q}})$ in projective 3–space.

When it comes to the points outside the lines, very little is actually known. It has been conjectured by Manin (see [3], for example) that if U is the open subset of X given by the complement of the 27 lines, then $n_U(B) = O(B^{1+\varepsilon})$ for any $\varepsilon > 0$. In contrast to this hypothesis, the best general result of this kind seems to be $n_U(B) = O(B^{7/3+\varepsilon})$, due to Pila (see [6]). In some special cases, sharper estimates have been established. In the case where all 27 lines are defined over the ground field, it was shown by Manin and Tschinkel [9] that $n_U(B) = O(B^{5/3+\varepsilon})$. Another, much older, result is due to Hooley [7]. He proved, by means of sieve methods, that $n_U(B) = O(B^{5/3+\varepsilon})$ for the surface $x_0^3 + x_1^3 + x_2^3 + x_3^3 = 0$ over $\mathbb{Q}$. This result is not covered by the theorem of Manin and Tschinkel, since 24 of the lines are not defined over $\mathbb{Q}$. A more elementary proof of Hooley's theorem was given by Wooley [14], and the result was improved and generalized by Heath–Brown [5], who

1991 *Mathematics Subject Classification.* 11G35, 11E20.

Key words and phrases. Cubic surfaces, Rational Points, Quadratic Forms.

showed that $n_U(B) = O(B^{4/3+\varepsilon})$ for cubic surfaces over $\mathbb{Q}$ containing three coplanar rational lines.

The aim of this paper is to extend Heath–Brown's estimate to cubic surfaces over arbitrary number fields. In order to achieve this we shall combine Heath–Brown's arguments with arguments from algebraic geometry and the arithmetic of ternary quadratic forms over arbitrary number fields. The main theorem of this paper is the following.

Theorem 1. *Let k be an algebraic number field and $F(x_0, x_1, x_2, x_3)$ a non–singular cubic form with coefficients in k. Suppose that the projective cubic k–surface $X \subset \mathbb{P}^3_k$ given by $F = 0$ contains three coplanar lines defined over k. Then the number of rational points on X, not lying on any line, and with height not exceeding B is $O(B^{4/3+\varepsilon})$.*

The content of the paper is as follows.

In section 2 we fix the notation. We choose normalized absolute values, define height functions, and look briefly at the notion of lattices. We also state some preliminary results, in most cases without proof. One of these results is the adelic version of Minkowski's second theorem about successive minima, due to Bombieri and Vaaler [1].

Section 3, which is the larger part of the paper, is devoted to the arithmetic of ternary quadratic forms. We generalize two theorems of Heath–Brown. Both results give uniform estimates for the number of points of bounded height on a conic. By uniform we mean that the estimates only depend on a few parameters of the form defining the conic.

In section 4 we prove theorem 1. The assumption that X contains three rational coplanar lines makes it possible to define three conic bundle morphisms $f_i : X \to \mathbb{P}^1_k$, one for each line. The general theory of height functions shows that if the height of $x \in X(k)$ is $\leq B$, then there is an index i such that $x \in f_i^{-1}(a, b)$ for some $(a, b) \in \mathbb{P}^1(k)$ of height $O(B^{2/3})$. The results from section 3 give estimates for the number of rational points on the fibres $f_i^{-1}(a, b)$ of height $\leq B$. By uniformity, the estimates only depend on B and the parameter (a, b). By choosing the most favourable estimate for each (a, b) and summing over all such estimates, we get the required bound $O(B^{4/3+\varepsilon})$ for $n_U(B)$.

Acknowledgements. I wish to thank my supervisor Per Salberger for his guidance and support during the course of this work.

2. Notations and preliminaries

In this section we fix the notation and state some preliminary results.

For any set A, we denote by $|A|$ or $\#A$ the cardinality of A.

If A and B are commensurable abelian subgroups of some group, then $[A : B]$ is the quotient $[A : A \cap B]/[B : A \cap B]$, where $[A : A \cap B]$ and $[B : A \cap B]$ are the index of $A \cap B$ in A and B, respectively.

If f and g are two non–negative functions such that $f \leq cg$ for some positive constant c on some common domain of f and g, then we write $f \ll g$ or $f = O(g)$. If the constant c is not absolute, then we may indicate in subscript the parameters on which it depends.

For any integral domain R and elements $x_1, \ldots, x_n$ in the quotient field of R, we let $\langle x_1, \ldots, x_n \rangle$ be the fractional ideal of R generated by $x_1, \ldots, x_n$.

Algebraic number fields. In general we denote a number field by k, and any of its places by v. If $k = \mathbb{Q}$, then by abuse of notation we write p for the non–archimedean (finite) place corresponding to the prime number p, and ∞ for its archimedean (infinite) place. If w is a place of $\mathbb{Q}$ obtained by restriction of a place v on k, we write $v \mid w$ and $d_v = [k_v : \mathbb{Q}_w]$ for the local degree of the extension $\mathbb{Q}_w \subset k_v$ of local fields. Since the number of infinite places of k will occur frequently we denote this number by s_k.

The normalized absolute value $|\ |_v$ on k is the one which induces the ordinary absolute value on $\mathbb{R}$ if $v \mid \infty$, and the p–adic absolute value $|p|_v = 1/p$ if $v \mid p$. We set $\|x\|_v = |x|_v^{d_v}$, so that we have the product formula $\prod_v \|x\|_v = 1$, for all $x \in k^*$.

We denote by $\mathfrak{o}_k = \mathfrak{o}$ and $\mathfrak{o}_v$ the ring of integers of k and k_v, respectively, and write $N_k(\mathfrak{a})$ for the index $[\mathfrak{o} : \mathfrak{a}]$, where $\mathfrak{a}$ is any fractional ideal of $\mathfrak{o}$. Note that if v is a finite place of k corresponding to the prime ideal $\mathfrak{p}$ of $\mathfrak{o}$ and π is a generator of the maximal ideal of $\mathfrak{o}_v$, then $\|\pi\|_v^{-1} = N_k(\mathfrak{p})$. We also have that $N_k(\langle x \rangle)$ is the absolute value of the norm $N_{k/\mathbb{Q}}(x)$ for $x \in k$. In this case we write $N_k(x)$ for short.

We will not use the notion of measure in the last two sections, but we need it in the formulation of Bombieri and Vaaler's theorem in this section.

If $v \mid \infty$ and $k_v = \mathbb{R}$, then $\mathrm{d}\mu_v$ is the ordinary Lebesgue measure on $\mathbb{R}$.

If $v \mid \infty$ and $k_v = \mathbb{C}$, then $\mathrm{d}\mu_v$ is the ordinary Lebesgue measure on the complex plane multiplied by 2.

If $v \nmid \infty$, then $\mathrm{d}\mu_v$ is the measure normalized so that $\mu_v(\mathfrak{o}_v) = \|\mathfrak{D}_v\|_v^{1/2}$, where $\mathfrak{D}_v$ is the local different of k at v.

The following two results are well–known, in one form or another, and may be found in almost any book on algebraic number theory (see [8, V, §1], for example).

Theorem 2 (Unit theorem). *Let U_k be the group of units of $\mathfrak{o}$ and W_k the subgroup of U_k consisting of the roots of unity in k. The image of the regulator map*

$$l : U_k \to \mathbb{R}^{s_k}, \quad x \mapsto (\log \|x\|_v)_{v|\infty}$$

is a $(s_k - 1)$–dimensional lattice in $\mathbb{R}^{s_k}$ and the kernel is W_k.

Let $\mathbf{r} \in (\mathbb{R}_{>0})^{s_k}$ be a vector with components r_v for $v \mid \infty$, and let $L(\mathbf{r})$ be the set of all $x \in \mathfrak{o}$ such that $\|x\|_v \le r_v$. The size $\|\mathbf{r}\|$ of the vector $\mathbf{r}$ is defined to be the product $\prod_{v|\infty} r_v$.

Proposition 1. *For any $\mathbf{r} \in (\mathbb{R}_{>0})^{s_k}$ we have*

$$\|\mathbf{r}\| \ll_k |L(\mathbf{r})| \ll_k \sup\{1, \|\mathbf{r}\|\}.$$

Height functions. Let k be a number field and $\mathbb{P}^n(k)$ the set of k–points in projective n–space $\mathbb{P}^n_k$. Since k is equipped with a product formula there is a well–defined height function $H_k : \mathbb{P}^n(k) \to \mathbb{R}_{\ge 1}$, given by

$$(x_0, \ldots, x_n) \mapsto \prod_v \sup_{0 \le i \le n} \|x_i\|_v = N_k(\langle x_0, \ldots, x_n \rangle)^{-1} \prod_{v|\infty} \sup_{0 \le i \le n} \|x_i\|_v .$$

Note that H_k is not a restriction of the absolute height on $\mathbb{P}^n(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. If K is an extension field of k, then $H_K(x) = H_k(x)^{[K:k]}$ for all $x \in \mathbb{P}^n(k)$. We mention this because Northcott's finiteness theorem below is formulated in terms of the absolute height on $\mathbb{P}^n(\overline{\mathbb{Q}})$. For a detailed discussion on heights and for proofs of the following two results see [12].

Theorem 3 (Northcott's finiteness theorem). *Let n, d, and B be positive integers. Then there are only finitely many points in $\mathbb{P}^n(\overline{\mathbb{Q}})$ of absolute height not exceeding B and of degree less or equal to d.*

Proposition 2. *Let $\phi_0, \dots, \phi_r$ be homogeneous polynomials of degree m and with coefficients in k. If the polynomials are not simultaneously zero on $\overline{k}$ (an algebraic closure of k), then*

$$\log H_k(\phi_0(x), \dots, \phi_r(x)) = m \log H_k(x) + O(1),$$

for all $x \in \mathbb{P}^n(k)$.

Note. A special, but important, case of this proposition is when $\phi : k^{n+1} \to k^{n+1}$ is an automorphism. Then $H_k(x) \ll H_k(\phi(x)) \ll H_k(x)$ for all $x \in \mathbb{P}^n(k)$.

The next result may also be found in [12, 13.2]. We include a proof since we will refer to it later.

Proposition 3. *Every point $x \in \mathbb{P}^n(k)$ is representable by homogeneous coordinates $(x_0, \dots, x_n) \in \mathfrak{o}^{n+1}$ such that $\sup_{0 \le i \le n} \|x_i\|_v \ll_{k,n} H_k(x)^{1/s_k}$ for all $v \mid \infty$.*

Proof. Suppose that $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ are ideals representing the ideal classes of $\mathfrak{o}$. Then any point $x \in \mathbb{P}^n(k)$ has coordinates $(y_0, \dots, y_n) \in \mathfrak{o}^{n+1}$ for which $\langle y_0, \dots, y_n \rangle = \mathfrak{a}_j$ for some j. In particular, if

$$(x_0, \dots, x_n) = (u^{-1} y_0, \dots, u^{-1} y_n)$$

for some unit u of $\mathfrak{o}$, then

$$H_k(x) = \frac{1}{N_k(\mathfrak{a}_j)} \prod_{v \mid \infty} \sup_{0 \le i \le n} \|x_i\|_v \,.$$

It is therefore sufficient to find a unit u such that

$$\sup_{0 \le i \le n} \|x_i\|_v \ll \prod_{v \mid \infty} \sup_{0 \le i \le n} \|x_i\|_v^{1/s_k}$$

for all $v \mid \infty$. Let

$$y_v = \sup_{0 \le i \le n} \|y_i\|_v \Big/ \prod_{v \mid \infty} \sup_{0 \le i \le n} \|y_i\|_v^{1/s_k} \,,$$

so that the inequalities above may be written as $y_v \ll \|u\|_v$. If $Y \subset (\mathbb{R}_{>0})^{s_k}$ is the locally compact subgroup of elements $y = (y_v)$ which satisfy $\prod_v y_v = 1$, then the image of U_k in Y under $u \mapsto (\|u\|_v)$ is a discrete cocompact multiplicative lattice, by theorem 2. Hence there exists u of the desired type. $\square$

We have not found the next result in the literature so we include a proof. The height $h_k(x)$ of an element $x \in k^*$ is defined to be $H_k(1,x)$.

Proposition 4. *If d is the degree of k over $\mathbb{Q}$, then the number of units $u \in U_k$ such that $h_k(u) \leq B$ is $\ll_d \sup\{1, (\log B)^{s_k}\}$.*

Note. The exponent s_k can be reduced to $s_k - 1$, but for our application the actual order is not very significant.

Proof. First note that $h_k(u) = h_k(u^{-1})$ for all $u \in U_k$, so if $h_k(u) \leq B$ for some $u \in U_k$, then $\sup_{v|\infty} |\log \|u\|_v| \leq \log B$. By theorem 2, it is therefore sufficient to show that there are $\ll_d \sup\{1, (\log B)^{s_k}\}$ lattice points of $l(U_k) \subset \mathbb{R}^{s_k}$ in the box centred at the origin with side length $2\log B$. From theorem 3 we have that there is a constant $c > 1$, only depending on d, such that $u \in W_k$ whenever $u \in U_k$ and $h_k(u) \leq c$. This implies that any box with side length $\frac{2}{s_k} \log c$ contains at most one of the points of $l(U_k)$. By comparing volumes we thus have that the number of points of $l(U_k)$ in the box $|\log \|u\|_v| \leq \log B$ is $\ll (\log B)^{s_k}/(\log c)^{s_k} \ll_d (\log B)^{s_k}$, providing that $B \gg c$. $\square$

Lattices over number fields. Let k be a number field of degree d over $\mathbb{Q}$, and let n be a positive integer. One usually says that an $\mathfrak{o}$–module in k^n is an $\mathfrak{o}$–lattice in k^n if it is finitely generated and contains a basis of k^n over k. It is not hard to see that if Λ is an $\mathfrak{o}$–lattice in k^n and v is a finite place of k, then $\Lambda_v = \mathfrak{o}_v \otimes_{\mathfrak{o}} \Lambda$ is a free $\mathfrak{o}_v$–module in $(k_v)^n$ such that Λ_v contains a basis for $(k_v)^n$ over k_v. We say that such an $\mathfrak{o}_v$–module is an $\mathfrak{o}_v$–lattice in $(k_v)^n$. The next result states that an $\mathfrak{o}$–lattice is known if it is known locally everywhere. For a proof see, for example, [10, 5.3].

Theorem 4. *For each finite place v of k, let L_v be an $\mathfrak{o}_v$–lattice in $(k_v)^n$ such that $L_v = (\mathfrak{o}_v)^n$ for almost all v. If $\Lambda = \bigcap_{v\nmid\infty} L_v \cap k^n$, then Λ is the unique $\mathfrak{o}$–lattice in k^n such that $\Lambda_v = L_v$ for all v.*

Proposition 5. *If $L \subset \Lambda$ are $\mathfrak{o}$–lattices in k^n, then there is an element $a \in k^*$ such that $\Lambda \subset aL$ and $[L : \Lambda] \ll_k N_k(a)$.*

Proof. By the invariant factor theorem (see [10, 4.14], for example), there are elements $u_1, \ldots, u_n \in \Lambda$, fractional $\mathfrak{o}$–ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, and $\mathfrak{o}$–ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_n$ such that

$$\Lambda = \bigoplus_{i=1}^{n} \mathfrak{a}_i\, u_i \qquad \text{and} \qquad L = \bigoplus_{i=1}^{n} \mathfrak{b}_i\, \mathfrak{a}_i\, u_i.$$

Then, if we choose $b \in \mathfrak{b}_1 \cdots \mathfrak{b}_n$ with $N_k(b) \ll_k \prod_{i=1}^n N_k(\mathfrak{b}_i) = [\Lambda : L]$, and put $a = b^{-1}$, we have $\Lambda \subset aL$ and $[L : \Lambda] \ll_k N_k(a)$. $\square$

Next we formulate Bombieri and Vaaler's adelic version of Minkowski's second theorem [1]. Later, when it is needed, we will use a slightly reformulated version of this result. We give this version as a corollary of the theorem. However, before we can formulate the result we have to make some definitions.

For each finite place v of k, let L_v be an $\mathfrak{o}_v$–lattice in $(k_v)^n$ such that $L_v = (\mathfrak{o}_v)^n$ for almost all v. For each infinite place v of k, let S_v be a nonempty, open, convex, symmetric, bounded subset of $(k_v)^n$. By symmetric we mean that $S_v = -S_v$. Then

$$\Gamma = \prod_{v|\infty} S_v \times \prod_{v\nmid\infty} L_v$$

is a subset of $(k_{\mathbb{A}})^n$, the n–fold product of adeles over k. In fact, Γ is an open neighbourhood of 0 and the closure of Γ is compact. Thus the volume

$$\mathrm{Vol}(\Gamma) = \prod_{v|\infty} \mu_v^n(S_v) \prod_{v\nmid\infty} \mu_v^n(L_v)$$

exists as a finite number.

Let Λ be the unique $\mathfrak{o}$–lattice such that $\Lambda_v = L_v$ for all $v \nmid \infty$. The i:th successive minima λ_i for $S = \prod_{v|\infty} S_v$, with respect to Λ is defined to be the infimum of all positive reals λ such that $\Lambda \cap \lambda S$ contains i linearly independent vectors. It is obvious that $\lambda_1 \leq \cdots \leq \lambda_n$. It is also evident from the definition that there exist n linearly independent vectors $\mathbf{u}_i \in \Lambda$ such that $\mathbf{u}_i \notin \lambda_i S_v$ for some v, but $\{\mathbf{u}_1, \ldots, \mathbf{u}_i\} \subset \lambda_i \overline{S}$, where $\overline{S} = \prod_{v|\infty} \overline{S}_v$ is the closure of S. We will use this observation later. For a proof of the following theorem see [1].

Theorem 5. *The successive minima $\lambda_1 \leq \cdots \leq \lambda_n$ satisfy the inequality*

$$(\lambda_1 \cdots \lambda_n)^d \,\mathrm{Vol}(\Gamma) \leq 2^{dn}.$$

Corollary. *The successive minima satisfy the relation*

$$(\lambda_1 \cdots \lambda_n)^d \prod_{v|\infty} \mathrm{Vol}(S_v) \ll_{k,n} [\mathfrak{o}^n : \Lambda].$$

Proof. All we have to do is to calculate the volume $\mathrm{Vol}(\Gamma)$. By definition the product $\prod_{v|\infty} \mu_v^n(S_v)$ is the product of the volumes $\mathrm{Vol}(S_v)$ multiplied by 2^{d-s_k} ($d - s_k$ being the number of complex places of k). By additivity and translation invariance of μ_v^n we obtain

$$\mu_v^n(\Lambda_v) = [\Lambda_v : \Lambda_v \cap (\mathfrak{o}_v)^n]\, \mu_v^n(\Lambda_v \cap (\mathfrak{o}_v)^n) = [\Lambda_v : (\mathfrak{o}_v)^n]\, \mu_v^n((\mathfrak{o}_v)^n).$$

But then we are done since

$$\prod_{v\nmid\infty} [(\mathfrak{o}_v)^n : \Lambda_v] = [\mathfrak{o}^n : \Lambda],$$

and

$$\prod_{v\nmid\infty} \mu_v(\mathfrak{o}_v) = \prod_{v\nmid\infty} \|\mathfrak{D}_v\|_v^{1/2} = |\Delta_k|^{-1/2},$$

where Δ_k is the discriminant of k. □

3. Ternary quadratic forms

In this section we estimate the number of rational points of bounded height on conics over number fields. The main estimates are uniform in the sense that the implied constants only depend on a few invariants of the coefficients of the quadratic form defining the conic.

The ground field k is assumed to be fixed from now on, so any implicitly given constants may depend on k, even if this is not stated explicitly. Before we begin our discussion, we also want to stress that most of the arguments in this and the next section are generalizations of Heath–Brown's arguments in the case $k = \mathbb{Q}$ (see [5]).

Let M be any invertible $n \times n$–matrix with entries in k. We define $\Delta(M)$ and $\Delta_0(M)$ to be the fractional ideal of $\mathfrak{o}$ generated by the determinant of M and the fractional ideal generated by the $(n-1) \times (n-1)$–minors of M, respectively.

Lemma 1. *$\Delta(MN) = \Delta(M)\,\Delta(N)$ and $\Delta_0(MN) \subset \Delta_0(M)\,\Delta_0(N)$.*

Proof. The equality $\Delta(MN) = \Delta(M)\,\Delta(N)$ is well–known, and the inclusion $\Delta_0(MN) \subset \Delta_0(M)\,\Delta_0(N)$ follows from the relation $\widetilde{MN} = \widetilde{N}\widetilde{M}$ between the cofactor matrices of M, N, and MN. $\square$

The main result of this section is the following theorem.

Theorem 6. *Let q be a ternary quadratic form with matrix $M \in \mathrm{M}_3(\mathfrak{o})$, and let $\mathbf{r}_1$, $\mathbf{r}_2$, $\mathbf{r}_3 \in (\mathbb{R}_{>0})^{s_k}$ be given. If q is non–singular, then there are*

$$\ll_\varepsilon \left(1 + \sqrt{\frac{\|\mathbf{r}_1\|\,\|\mathbf{r}_2\|\,\|\mathbf{r}_3\|\,N_k(\Delta_0(M))^2}{N_k(\Delta(M))}}\right) N_k(\Delta(M))^\varepsilon$$

points $(x_1, x_2, x_3) \in \mathbb{P}^2(k)$ on the conic $q = 0$ such that $x_i \in L(\mathbf{r}_i)$.

Note. By proposition 3 we know that for any point $x \in \mathbb{P}^2(k)$ with $H_k(x) \leq B$, we can find homogeneous coordinates $(x_1, x_2, x_3) \in \mathfrak{o}^3$ such that $\|x_i\|_v \ll B^{1/s_k}$ for all $v \mid \infty$. The theorem then says that there are $O_q(B^{3/2})$ points on the conic $q = 0$ of height at most B. Intuitively this estimate is not what one expects (q is of degree 2). One can of course do better if one does not require uniformity in q, as the following proposition shows.

Proposition 6. *If q is a non–singular quadratic form, then there are $O_q(B)$ points $x \in \mathbb{P}^2(k)$ on the conic $q(x) = 0$ such that $H_k(x) \leq B$.*

Proof. If q is isotropic, then q is "k–equivalent" to $\alpha(x_0^2 - x_1x_2)$ for some $\alpha \in k^*$. But $(y_0, y_1) \mapsto (y_0y_1, y_0^2, y_1^2)$ is a parametrization of the solutions of $x_0^2 - x_1x_2 = 0$, and $H_k(y_0y_1, y_0^2, y_1^2) = H_k(y_0, y_1)^2$ for all $(y_0, y_1) \in \mathbb{P}^1(k)$, so by Schanuel's theorem,

$$\begin{aligned} \#\left\{x \in \mathbb{P}^2(k) \,:\, q(x) = 0, H_k(x) \leq B\right\} &\ll_q \\ &\#\left\{y \in \mathbb{P}^1(k) \,:\, H_k(y) \leq B^{1/2}\right\} \ll B. \end{aligned}$$

$\square$

The proof of the theorem will be given in several steps. In lemma 4 we look at the equation $q = 0$ at each finite place of k and find that each solution $(x_1, x_2, x_3) \in \mathfrak{o}^3$ must belong to one of not too many $\mathfrak{o}$–lattices in k^3. We also find lower bounds for the indices of the lattices in $\mathfrak{o}^3$. By using the theory of successive minima we then use this information to reduce the proof to a problem of counting the number of points on a conic in a "bounded domain" of $\mathbb{P}^2(k)$. We obtain a solution to this problem in lemma 5. First, however, we formulate some minor results which are included for completeness and which we need in the proof of lemma 4.

For an ideal $\mathfrak{a}$ of $\mathfrak{o}$, let $\rho(\mathfrak{a})$ be the number of prime ideals containing $\mathfrak{a}$ and $\tau(\mathfrak{a})$ the number of ideals containing $\mathfrak{a}$. Recall that an arithmetical function $f : \mathbb{Z}_{>0} \to \mathbb{C}$ is said to be multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$. For a proof of the following result see, for example, [13, I. §5.1].

Theorem 7. *Let f be a multiplicative function. If $\lim_{p^\nu\to\infty} f(p^\nu) = 0$, where p^ν are prime powers, then $\lim_{n\to\infty} f(n) = 0$.*

Corollary. *If c is a positive number, then $c^{\rho(\mathfrak{a})}\tau(\mathfrak{a}) \ll_{c,\varepsilon} N_k(\mathfrak{a})^\varepsilon$ for all ideals $\mathfrak{a}$ of $\mathfrak{o}$.*

Proof. Let $\rho(n)$ and $\tau(n)$ be the number of primes dividing $n \in \mathbb{Z}_{>0}$ and the number of divisors of n, respectively. Then we have $\rho(\mathfrak{a}) \le d\,\rho(N_k(\mathfrak{a}))$ and $\tau(\mathfrak{a}) \le \tau(N_k(\mathfrak{a}))^d$ for all ideals $\mathfrak{a}$ of $\mathfrak{o}$, where d is the degree of k over $\mathbb{Q}$. Thus $c^{\rho(\mathfrak{a})}\tau(\mathfrak{a}) \le c^{d\rho(N_k(\mathfrak{a}))}\tau(N_k(\mathfrak{a}))^d \ll_{c,\varepsilon} N_k(\mathfrak{a})^\varepsilon$, since $f(x) = (c^{\rho(x)}\tau(x))^d/x^\varepsilon$ is a multiplicative function and $f(p^\nu) = (c\,(\nu+1))^d p^{-\nu\varepsilon} \to 0$ as $p^\nu \to \infty$. $\square$

If M, N, and T are square matrices of the same size, with entries in some ring R, and T is unimodular with $T^tMT = N$, then we say that M and N are R–equivalent. This means that M and N only differs by a finite number of simultaneous elementary row– and column–operations. The next lemma says that over a discrete valuation ring any symmetric matrix is almost equivalent to a diagonal matrix.

Lemma 2. *Let v be a discrete valuation on some field, and let R be the corresponding valuation ring. Then for any symmetric matrix $M \in \mathrm{M}_n(R)$ there exists an element $x \in R$ and matrices P, $D \in \mathrm{M}_n(R)$ such that D is diagonal, $P^tDP = xM$, and $v(\det P) = v(x) \le (n-1)v(2)$.*

Proof. Let n be a positive integer and M any symmetric $n \times n$–matrix with entries in R. It is sufficient to show that we can find an element $x \in R$ and a matrix $P \in \mathrm{M}_n(R)$ such that $v(\det P) = v(x) \le v(2)$ and $P^tDP = xM$, where D is some matrix with zeros in its first row and column, except perhaps on the diagonal. The lemma then follows by induction on the size of the matrices.

Since the existence of the objects x and P is trivially verifiable when $n = 1$ or $M = 0$, we may assume that $n \ge 2$ and that at least one of the entries of M is a unit in R. Then M is equivalent to a matrix with its first row equal to $(a, u, 0, \dots, 0)$ or $(u, 0, 0, \dots, 0)$, where u is a unit and a is some element of R such that $0 \le v(a) \le v(2)$. If $v(2) = 0$, then a matrix of the first shape is obviously equivalent to a matrix of the second shape. If, on the other hand, $v(2) > 0$, we can use the identity

$$\begin{pmatrix} \begin{smallmatrix} a & u \\ 0 & 1 \end{smallmatrix} & 0 \\ 0 & I \end{pmatrix}^t \left[\begin{pmatrix} 1 & 0 \\ 0 & aM' \end{pmatrix} - \begin{pmatrix} \begin{smallmatrix} 0 & 0 \\ 0 & u^2 \end{smallmatrix} & 0 \\ 0 & 0 \end{pmatrix} \right] \begin{pmatrix} \begin{smallmatrix} a & u \\ 0 & 1 \end{smallmatrix} & 0 \\ 0 & I \end{pmatrix} = a \begin{pmatrix} a & \mathbf{x} \\ \mathbf{x}^t & M' \end{pmatrix},$$

where M' is a symmetric $(n-1) \times (n-1)$–matrix and $\mathbf{x} = (u, 0, \dots, 0)$. This establishes the existence of the objects x and P. $\square$

Before the next lemma we just recall that if v is a finite place of k lying over a prime number p, then $\|p\|_v = \|\pi\|_v^r$, where π is a generator of the maximal ideal of $\mathfrak{o}_v$ and r is the ramification index of $\mathbb{Q}_p \subset k_v$.

Lemma 3. *For a finite place v of k and any integer $n \geq 1$, let R_n be the ring $\mathfrak{o}_v/\langle \pi^n \rangle$. If $\varepsilon \in R_n^*$, then the number of solutions of the equation $x^2 = \varepsilon$ is less or equal to $2\,\|2\|_v^{-1}$.*

Proof. Since $(x/y)^2 = 1$ if $x^2 = y^2 = \varepsilon$ for $\varepsilon \in R_n^*$, we only need to study the case $\varepsilon = 1$. Let r be the least integer such that $2 \notin \langle \pi^{r+1} \rangle$. Then either $x+1 \notin \langle \pi^{r+1} \rangle$ or $x-1 \notin \langle \pi^{r+1} \rangle$ for $x \in \mathfrak{o}_v$. Hence, if $x^2 - 1 = (x+1)(x-1) \in \langle \pi^n \rangle$, we must have $x + 1 \in \langle \pi^{n-r} \rangle$ or $x - 1 \in \langle \pi^{n-r} \rangle$. There are thus at most $2\,|\langle \pi^{n-r} \rangle / \langle \pi^n \rangle| = 2\,|(R_1)^r|$ solutions of $x^2 = \varepsilon$ in R_n. Moreover, $r = 0$ if $\|2\|_v = 1$, and r is the ramification index of $\mathbb{Q}_2 \subset k_v$ if $\|2\|_v < 1$. $\square$

We now have enough information to prove the first main lemma in the proof of theorem 6.

Lemma 4. *Let q be non–singular ternary quadratic form with matrix $M \in \mathrm{M}_3(\mathfrak{o})$. For each finite place v of k, let π_v be a generator of the maximal ideal of $\mathfrak{o}_v$, and let a_v and b_v be the non–negative integers defined by $\|\Delta(M)\|_v = \|\pi_v\|_v^{a_v}$ and $\|\Delta_0(M)\|_v = \|\pi_v\|_v^{b_v}$, respectively.*

(a) *If $a_v > 0$ and $q(\mathbf{x}) = 0$ for some $\mathbf{x} \in (\mathfrak{o}_v)^3$, then $\mathbf{x}$ belongs to at least one of at most $O(a_v)$ $\mathfrak{o}_v$–lattices Λ in $(k_v)^3$, each satisfying*

$$[(\mathfrak{o}_v)^3 : \Lambda] \geq \|2\|_v^8\, \|\Delta(M)\|_v^{-1}\, \|\Delta_0(M)\|_v^2 .$$

Moreover, the implied constant in $O(a_v)$, let us call it c, depends only on k and may be chosen to be the same for all v.

(b) *If $q(\mathbf{x}) = 0$ for some $\mathbf{x} \in \mathfrak{o}^3$, then $\mathbf{x}$ belongs to at least one of at most $O(N_k(\Delta(M))^{\varepsilon})$ $\mathfrak{o}$–lattices Λ in k^3, each satisfying*

$$[\mathfrak{o}^3 : \Lambda] \gg N_k(\Delta(M))\, N_k(\Delta_0(M))^{-2}.$$

Proof. It is (b) that really interests us, so assume for the moment that we have a proof of (a). If $q(\mathbf{x}) = 0$ for some $\mathbf{x} \in \mathfrak{o}^3$, then $\mathbf{x}$ belongs to an $\mathfrak{o}$–lattice Λ in k^3 with $\Lambda_v = (\mathfrak{o}_v)^3$ if $a_v = 0$, and Λ_v equal to one of the $\mathfrak{o}_v$–lattices from (a) if $a_v > 0$. This is a consequence of theorem 4. It follows immediately from the local nature of index that $[\mathfrak{o}^3 : \Lambda] \gg N_k(\Delta(M))\, N_k(\Delta_0(M))^{-2}$. Moreover, there are at most $\prod_{a_v > 0} c a_v$ such lattices Λ, and

$$\prod_{a_v > 0} c a_v \leq c^{\rho(\Delta(M))} \tau(\Delta(M)) \ll N_k(\Delta(M))^{\varepsilon}$$

by the corollary of theorem 7. It is thus sufficient to find a proof of (a).

Let v be a finite place of k such that $a_v > 0$. To keep the notations as simple as possible we skip the indices and write π, a, and b for π_v, a_v, and b_v, respectively. By lemma 2 there is an element $x \in \mathfrak{o}_v$ such that $x\,q(\mathbf{x})$ may be diagonalized over the ring $\mathfrak{o}_v$, using a matrix P with $\|\det P\|_v = \|x\|_v \geq \|2\|_v^2$. Let D be the matrix of this diagonalized form

$$Q(y_1, y_2, y_3) = \varepsilon_1 \pi^{\alpha_1} y_1^2 + \varepsilon_2 \pi^{\alpha_2} y_2^2 + \varepsilon_3 \pi^{\alpha_3} y_3^2,$$

where $\alpha_1 \geq \alpha_2 \geq \alpha_3 \geq 0$ are integers and $\varepsilon_1, \varepsilon_2, \varepsilon_3$ are units. From the identity $\Delta(xM) = \Delta(P)^2\, \Delta(D)$ and the inclusion $\Delta_0(xM) \subset \Delta_0(P)^2\, \Delta_0(D)$, we have $\|x\|_v \|\pi\|_v^a = \|\pi\|_v^{\alpha_1+\alpha_2+\alpha_3}$ and $\|x\|_v^2 \|\pi\|_v^b \le \|\pi\|_v^{\alpha_2+\alpha_3}$, respectively. If we combine these two relations and use the fact $\|x\|_v \ge \|2\|_v^2$, we get

$$\|\pi\|_v^{-\alpha_1+\alpha_2+\alpha_3} \ge \|2\|_v^8 \, \|\Delta(P)\|_v^{-1} \, \|\pi\|_v^{2b-a}.$$

This inequality makes the hypothesis of the lemma more understandable. All we have to prove is that any solution $\mathbf{y} \in (\mathfrak{o}_v)^3$ of $Q = 0$ belongs to at least one of at most $O(a)$ lattices, each with index $\ge \|\pi\|_v^{-\alpha_1+\alpha_2+\alpha_3}$ in $(\mathfrak{o}_v)^3$.

Now suppose that $Q(y_1, y_2, y_3) = 0$ for some $(y_1, y_2, y_3) \in (\mathfrak{o}_v)^3$. Then we find that

$$\varepsilon_2 \pi^{\alpha_2-\alpha_3} y_2^2 + \varepsilon_3 y_3^2 \in \langle \pi^{\alpha_1-\alpha_3} \rangle. \tag{3.1}$$

When α_2 and α_3 have opposite parities this implies that $y_2^2 \in \langle \pi^{\alpha_1-\alpha_2} \rangle$ and $y_3^2 \in \langle \pi^{\alpha_1-\alpha_3} \rangle$. It follows that (y_1, y_2, y_3) belongs to the lattice

$$\Lambda = \mathfrak{o}_v \times \langle \pi^{[\frac{\alpha_1-\alpha_2+1}{2}]} \rangle \times \langle \pi^{[\frac{\alpha_1-\alpha_3+1}{2}]} \rangle.$$

Since $[(\mathfrak{o}_v)^3 : \Lambda] \ge \|\pi\|_v^{-\alpha_1+\alpha_2+\alpha_3}$, this completes the proof in this case.

The case in which $\alpha_2 - \alpha_3 = 2h$, for some h, needs slightly more work. We can assume that $y_2^2 \notin \langle \pi^{\alpha_1-\alpha_2} \rangle$ and $y_3^2 \notin \langle \pi^{\alpha_1-\alpha_3} \rangle$. Otherwise (y_1, y_2, y_3) would belong to the lattice Λ and we would not get anything new. By studying (3.1) we see that $y_2 = u_2 \pi^n$ and $y_3 = u_3 \pi^{n+h}$ for some non–negative integer $n < [\frac{\alpha_1-\alpha_2+1}{2}]$ and some units u_2 and u_3, which satisfy $\varepsilon_2 u_2^2 + \varepsilon_3 u_3^2 \in \langle \pi^{\alpha_1-\alpha_2-2n} \rangle$. By lemma 3 there are at most $2\,\|2\|_v^{-1}$ solutions of the equation $r^2 + \varepsilon_2/\varepsilon_3 = 0$ in the ring $\mathfrak{o}_v / \langle \pi^{\alpha_1-\alpha_2-2n} \rangle$. If $r \in \mathfrak{o}_v$ represents the same solution as u_2/u_3, then $r\,\pi^h y_2 - y_3 \in \langle \pi^{\alpha_1-\alpha_2+h-n} \rangle$, so

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & \pi^n & 0 \\ 1 & r\pi^{h+n} & \pi^{\alpha_1-\alpha_2+h-n} \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$$

for some $(z_1, z_2, z_3) \in (\mathfrak{o}_v)^3$. Thus (y_1, y_2, y_3) belongs to at least one of at most $2\,\|2\|_v^{-1}\,[\frac{\alpha_1-\alpha_2+1}{2}]$ lattices, each with index

$$\|\pi\|_v^{\alpha_2-\alpha_1-h} \ge \|\pi\|_v^{-\alpha_1+\alpha_2+\alpha_3}$$

in $(\mathfrak{o}_v)^3$.

To complete the proof we have to show that $(2 + \alpha_1 - \alpha_2)\,\|2\|_v^{-1} + 1 \le ca$ for some constant c which only depends on k, but this is obviously true. $\square$

The next result is the second tool in the proof of the theorem. The significance of this result is that the bounds are completely independent of the form involved.

Lemma 5. *Let f be a ternary form of degree d with no linear factor, and let $\mathbf{r}_1, \mathbf{r}_2, \mathbf{r}_3 \in (\mathbb{R}_{>0})^{s_k}$ be given. Then there are*

$$\ll_d 1 + \sqrt{\|\mathbf{r}_1\|\,\|\mathbf{r}_2\|\,\|\mathbf{r}_3\|}$$

points $(x_1, x_2, x_3) \in \mathbb{P}^2(k)$ on the curve $f = 0$ such that $x_i \in L(\mathbf{r}_i)$.

Proof. Let r_{iv} be the v:th component of the vector $\mathbf{r}_i$, and set $R_i = \|\mathbf{r}_i\|$. We begin by showing that any point $(x_1, x_2, x_3) \in \mathbb{P}^2(k)$ with $x_i \in L(\mathbf{r}_i)$ lies on a line $a_1 x_1 + a_2 x_2 + a_3 x_3 = 0$, where the coefficients $a_i \in \mathfrak{o}$ are not all zero and $\|a_i\|_v \ll r_{iv}^{-1} \sqrt{r_{1v} r_{2v} r_{3v}}$. This is a simple application of the box principle. By proposition 1 there are $\gg Y^{3s_k}\sqrt{R_1R_2R_3}$ sets of coefficients with $\|a\|_i \le Yr_{iv}^{-1}\sqrt{r_{1v}r_{2v}r_{3v}}$. The corresponding values $a_1x_1+a_2x_2+a_3x_3$ satisfies

$$\|a_1x_1+a_2x_2+a_3x_3\|_v \ll Y\sqrt{r_{1v}r_{2v}r_{3v}},$$

so by the same proposition there are $\ll \sup\{1, Y^{s_k}\sqrt{R_1R_2R_3}\}$ such values. Hence, if Y is sufficiently large, then two such values must agree, and this for a Y independent of R_1, R_2, R_3 (for the case $R_1R_2R_3 < 1$ see below). Since f does not have any linear factors, each of the above lines has at most d points in common with $f=0$. Moreover, the number of lines is

$$\ll \prod_{i=1}^{3} \sup\{1, R_i^{-1}\sqrt{R_1R_2R_3}\} \ll \sqrt{R_1R_2R_3},$$

if $R_i^{-1}\sqrt{R_1R_2R_3} \ge 1$ for all i. If this last condition is not satisfied, then

$$R_iR_j = \inf\{R_1R_2, R_1R_3, R_2R_3\} \le \sqrt{R_1R_2R_3}.$$

Since each pair of elements $x_i \in L(\mathbf{r}_i)$, $x_j \in L(\mathbf{r}_j)$ produces at most d solutions of $f=0$, and the number of such pairs is

$$\ll \sup\{1, R_i\}\ \sup\{1, R_j\},$$

we can use the estimate $O(R_iR_j)$ in this case. Of course we have to assume that $R_i \ge 1$ and $R_j \ge 1$, but $L(\mathbf{r}_i) = \{0\}$ or $L(\mathbf{r}_j) = \{0\}$ in any other case, and then there are at most d solutions. $\square$

To prove theorem 6 we now use the theory of successive minima to combine these two last lemmas. Recall that q is a non–singular ternary quadratic form with matrix $M \in \mathrm{M}_3(\mathfrak{o})$, and $\mathbf{r}_1$, $\mathbf{r}_2$, $\mathbf{r}_3 \in (\mathbb{R}_{>0})^{s_k}$ are vectors with components r_{iv} for $v \mid \infty$. In order to have the same notation as in section 2, we define the nonempty, open, convex, symmetric, bounded subsets S_v of $(k_v)^3$ by

$$S_v = \left\{(x_1,x_2,x_3) \in (k_v)^3 \ :\ |x_i| < r_{iv}^{1/d_v}\right\},$$

and put $S = \prod_{v\mid\infty} S_v$. Obviously $\mathfrak{o}^3 \cap \overline{S} = L(\mathbf{r}_1) \times L(\mathbf{r}_2) \times L(\mathbf{r}_3)$, where $\overline{S} = \prod_{v\mid\infty} \overline{S}_v$ is the closure of S. If d is the degree of k over $\mathbb{Q}$ and $\lambda_1 \le \lambda_2 \le \lambda_3$ are the successive minima of S with respect to one of the lattices Λ from lemma 4, then

$$(\lambda_1\lambda_2\lambda_3)^d \prod_{v\mid\infty} \mathrm{Vol}(S_v) \ll [\mathfrak{o}^3 : \Lambda],$$

by the corollary of theorem 5. Moreover,

$$\prod_{v\mid\infty} \mathrm{Vol}(S_v) \gg \|\mathbf{r}_1\|\,\|\mathbf{r}_2\|\,\|\mathbf{r}_3\|$$

by the definition of the sets S_v. We mentioned in the preparations for theorem 5 that one can find a basis $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ of k^3 over k such that $\mathbf{u}_i \in \lambda_i\overline{S}$, but $\mathbf{u}_i \notin \lambda_iS_v$ for some v. If u_{ij} is the j:th component of $\mathbf{u}_i$, then these conditions imply that $\|u_{ij}\|_v \le \lambda_i^{d_v}r_{jv}$. Thus, if $(x_1,x_2,x_3) =$

$y_1\mathbf{u}_1 + y_2\mathbf{u}_2 + y_3\mathbf{u}_3 \in \overline{S}$ for some $(y_1, y_2, y_3) \in k^3$, and U is the matrix with columns $\mathbf{u}_i$, then

$$\|y_1\|_v = \frac{1}{\|\det U\|_v} \left\| \det \begin{pmatrix} x_1 & u_{21} & u_{31} \\ x_2 & u_{22} & u_{32} \\ x_3 & u_{23} & u_{33} \end{pmatrix} \right\|_v \ll \frac{r_{1v} r_{2v} r_{3v} (\lambda_2\lambda_3)^{d_v}}{\|\det U\|_v}$$

by Cramer's rule. There are of course analogous estimates for $\|y_2\|_v$ and $\|y_3\|_v$. Note that $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ does not constitute a basis for Λ over $\mathfrak{o}$. Presumably the lattice Λ is not even free. However, if L is the free $\mathfrak{o}$–lattice with $\mathbf{u}_1$, $\mathbf{u}_2$, $\mathbf{u}_3$ as generators, then by proposition 5 we have $L \subset \Lambda \subset aL$ for some $a \in k^*$ such that $N_k(a) \gg [L : \Lambda]$. Thus, any element $(x_1, x_2, x_3) \in \Lambda \cap \overline{S}$ may be written as $y_1(a\mathbf{u}_1) + y_2(a\mathbf{u}_2) + y_3(a\mathbf{u}_3)$ for some $(y_1, y_2, y_3) \in \mathfrak{o}^3$. This shows that if q' is the non–singular quadratic form with matrix U^tMU, then any solution $(x_1, x_2, x_3) \in \Lambda \cap \overline{S}$ of $q = 0$ gives a solution $(y_1, y_2, y_3) \in \mathfrak{o}^3$ of $q' = 0$ which satisfies

$$\|y_i\|_v \ll \frac{r_{1v} r_{2v} r_{3v}}{\|a\|_v \|\det U\|_v} \left(\frac{\lambda_1\lambda_2\lambda_3}{\lambda_i} \right)^{d_v} = t_{iv}.$$

Moreover, there are $\ll 1 + \sqrt{\prod_{i,v} t_{iv}}$ such solutions by lemma 5, and one gets

$$\prod_{i,v} t_{iv} = \left(\frac{\|\mathbf{r}_1\| \, \|\mathbf{r}_2\| \, \|\mathbf{r}_3\|}{N_k(a) N_k(\det U)} \right)^3 (\lambda_1\lambda_2\lambda_3)^{2d} \ll$$

$$\left(\frac{\|\mathbf{r}_1\| \, \|\mathbf{r}_2\| \, \|\mathbf{r}_3\|}{[L : \Lambda][\mathfrak{o}^3 : L]} \right)^3 \left(\frac{[\mathfrak{o}^3 : \Lambda]}{\|\mathbf{r}_1\| \, \|\mathbf{r}_2\| \, \|\mathbf{r}_3\|} \right)^2 = \frac{\|\mathbf{r}_1\| \, \|\mathbf{r}_2\| \, \|\mathbf{r}_3\|}{[\mathfrak{o}^3 : \Lambda]}$$

from the definitions and estimates above. Referring to lemma 4, this completes the proof of the theorem.

Next we prove a result that we can use when the determinant $N_k(\Delta(M))$ of the form q is small. In that case the estimate from theorem 6 is obviously not very good.

Proposition 7. *Let q be a non–singular ternary quadratic form such that the binary form $q(0, x_2, x_3)$ is also non–singular. Let $\mathbf{r} \in (\mathbb{R}_{>0})^{s_k}$ and $R \geq 1$ be given, and denote by $\|q\|$ the supremum of $\|\sigma\|_v$, where σ ranges over the coefficients of q and v over the infinite places of k. Then there are*

$$\ll \sup\{1, \|\mathbf{r}\| \, (\|\overline{\mathbf{r}}\| \, \|q\| \, R)^{\varepsilon}\}$$

points $(x_1, x_2, x_3) \in \mathbb{P}^2(k)$ on the conic $q = 0$, satisfying $(x_1, x_2, x_3) \in L(\mathbf{r}) \times \mathfrak{o} \times \mathfrak{o}$ and $\sup_{v|\infty} \|x_i\|_v \leq R$ for $i = 2, 3$. Here $\overline{\mathbf{r}} \in (\mathbb{R}_{>0})^{s_k}$ is the vector with the v:th component equal to r_v if $r_v \geq 1$ and 1 otherwise. As before, r_v denotes the v:th component of $\mathbf{r}$.

Proof. Since $q(0, x_2, x_3)$ is non–singular there is an invertible matrix $P \in \mathrm{M}_3(k)$ with first row $(1, 0, 0)$ such that $q(\mathbf{x}) = d(P\mathbf{x})$ for some diagonal form d. Moreover, we may choose P so that the entries p_{ij} satisfies $\sup\{\|p_{ij}\|_v, \|p_{ij}\|_v^{-1}\} \leq \|q\|^A$ for all $v \mid \infty$ and some fixed exponent A. The equation $q(x_1, x_2, x_3) = 0$ then becomes

$$\alpha L_1(x_1, x_2, x_3)^2 + \beta L_2(x_1, x_2, x_3)^2 = \gamma x_1^2 \tag{3.2}$$

with non–zero coefficients α, β, γ, and linear forms L_i such that $L_1(0, x_2, x_3)$ and $L_2(0, x_2, x_3)$ are linearly independent. By multiplying the equation with a suitable factor, we can assume that all coefficients are integers in k and satisfy $\sup_{v|\infty} \|\sigma\|_v \le \|q\|^A$, possibly with a new constant value of A. By the same argument, we may also assume that α is a square. The left hand side of (3.2) then factorizes over the field $K = k(\sqrt{\beta})$, and we have

$$L_3(x_1, x_2, x_3)\, L_4(x_1, x_2, x_3) = \gamma x_1^2 \tag{3.3}$$

for some linear forms L_i with coefficients in $\mathfrak{o}_K$.

Now suppose that $(x_1, x_2, x_3) \in L(\mathbf{r}) \times \mathfrak{o} \times \mathfrak{o}$ satisfies (3.3), and that $\sup_{v|\infty} \|x_i\| \le R$ for $i = 2, 3$. If $\|\mathbf{r}\| \le 1$, then there are at most two such solutions, considered as elements of $\mathbb{P}^2(k)$, since in that case $L(\mathbf{r})$ only consists of the zero element. If $\|\mathbf{r}\| \ge 1$, on the other hand, the cardinality of $L(\mathbf{r})$ is $\ll \|\mathbf{r}\|$, and in this case we show that there are $\ll (\|\overline{\mathbf{r}}\|\, \|q\|\, R)^\varepsilon$ possible pairs x_2, x_3 for each x_1. That is, we show that there are $\ll (\|\overline{\mathbf{r}}\|\, \|q\|\, R)^\varepsilon$ possible factorizations of the element γy_1^2 in the ring $\mathfrak{o}_K$ with certain conditions on the factors induced by the conditions on x_1, x_2, x_3 stated above.

Let $y_1 = x_1$, $y_2 = L_3(x_1, x_2, x_3)$, and $y_3 = L_4(x_1, x_2, x_3)$ so that we may write (3.3) as $y_2 y_3 = \gamma y_1^2$. If w is an infinite place of K, lying over the place v of k, then

$$\|y_i\|_w \ll (\|q\|^A \sup\{r_v, R\})^{d_w/d_v} \ll \|q\|^{2A} \sup\{r_v^2, R^2\} = t_w$$

for $i = 2, 3$. This follows from the conditions on x_1, x_2, x_3 and the conditions on the coefficients of the forms L_3 and L_4. Remember that $d_v = [k_v : \mathbb{Q}_v]$ is the local degree of k at v. We have seen earlier that there are $\ll N_k(\gamma y_1^2)^\varepsilon$ ideals of $\mathfrak{o}$ which contain the element γy_1^2 ($c = 1$ in the corollary of theorem 7). Since a prime of $\mathfrak{o}$ can split in at most two primes of $\mathfrak{o}_K$, there are thus $\ll N_k(\gamma y_1^2)^\varepsilon \ll (\|q\|\, \|\mathbf{r}\|)^\varepsilon$ ideals of $\mathfrak{o}_K$ containing γy_1^2. To complete the proof, then, it is sufficient to show that there are $\ll (\|\overline{\mathbf{r}}\|\, \|q\|\, R)^\varepsilon$ possible generators of any principal ideal $\langle y \rangle \subset \mathfrak{o}_K$ such that $\|y\|_w \ll t_w$. But if uy is another such generator for some unit u of $\mathfrak{o}_K$, then

$$h_K(u) \ll \prod_{w|\infty} t_w / \|y\|_w \ll (\|\overline{\mathbf{r}}\|\, \|q\|\, R)^{2As_K},$$

and by proposition 4 there are $\ll (\|\overline{\mathbf{r}}\|\, \|q\|\, R)^\varepsilon$ such units. □

Note. In contrary to theorem 6, this proposition gives the expected estimate $O(B^{1+\varepsilon})$ for the number of points of height $\le B$ on the conic $q = 0$.

4. Proof of the main theorem

We have now come to the proof of theorem 1. We will begin by redefining the objects of interest and formulate the hypothesis once again. As in the previous section we assume that the ground field k is fixed.

Let F be a non–singular quaternary cubic form such that the k–surface $X \subset \mathbb{P}_k^3$ given by $F = 0$ contains three coplanar lines defined over the ground field, and let $U \subset X$ be the complement of all the lines on X. We define $n(B)$ to be the number of rational points in U with height not exceeding B (note that $n(B)$ is finite by theorem 3). Our claim is that $n(B) = O(B^{4/3+\varepsilon})$.

To show this we will proceed in several steps. Clearly $n(B)$ depends on the choice of coordinates. But it follows from proposition 2 that the validity of the statement $n(B) \ll B^{4/3+\varepsilon}$ is independent of the choice of coordinates. Proposition 2 says that $H_k(\phi(x)) \ll_\phi H_k(x)$ if ϕ is an automorphism of k^4. The first thing we do, therefore, is to find appropriate coordinates in which to study F. By an initial linear change of variables we may assume that the plane containing the three lines is $x_0 = 0$. Then $F = L_1L_2L_3 - x_0Q$ for some non–zero quadratic form Q and some non–zero linear forms $L_i(x_1, x_2, x_3)$. After re–scaling both the variables and the form F appropriately we may moreover assume that Q and the L_i have coefficients in $\mathfrak{o}$.

The reduction which is about to follow is the most important part of our proof, and it is the reason why we assume that X contains three coplanar rational lines. The reduction is a generalization of an argument of Wooley and Heath–Brown. From the shape of F we see that the projections

$$f_1(x_0,x_1,x_2,x_3) = \begin{cases} (x_0, L_1) & \text{if } (x_0, L_1) \neq (0,0) \\ (L_2L_3, Q) & \text{otherwise,} \end{cases}$$

$$f_2(x_0,x_1,x_2,x_3) = \begin{cases} (x_0, L_2) & \text{if } (x_0, L_2) \neq (0,0) \\ (L_1L_3, Q) & \text{otherwise,} \end{cases}$$

$$f_3(x_0,x_1,x_2,x_3) = \begin{cases} (x_0, L_3) & \text{if } (x_0, L_3) \neq (0,0) \\ (L_1L_2, Q) & \text{otherwise} \end{cases}$$

define three conic bundle morphisms $f_i : X \to \mathbb{P}^1_k$.

Lemma 6. *For all $x \in X(k)$,*

$$H_1(x)H_2(x)H_3(x) \ll_F H(x)^2,$$

where $H_i(x) = H_k(f_i(x))$, and $H(x) = H_k(x)$.

Proof. Let $f : X(k) \to \mathbb{P}^1(k) \times \mathbb{P}^1(k) \times \mathbb{P}^1(k)$ be the morphism given by (f_1, f_2, f_3), and let $\psi : \mathbb{P}^1(k) \times \mathbb{P}^1(k) \times \mathbb{P}^1(k) \to \mathbb{P}^7(k)$ be the trilinear Segre embedding. Then from the equation $L_1L_2L_3 = x_0Q$ one sees that $\psi f(x_0, x_1, x_2, x_3)$ is given by

$$(y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7) = (x_0^2, x_0L_3, x_0L_2, L_2L_3, x_0L_1, L_1L_3, L_1L_2, Q).$$

Hence,

$$H_1(x)H_2(x)H_3(x) = \prod_v \sup_{0 \le i \le 7} \|y_i\|_v \ll \prod_v \sup_{0 \le i,j \le 3} \|x_ix_j\|_v = H(x)^2$$

for all $x = (x_0, x_1, x_2, x_3) \in \mathbb{P}^3(k)$. □

Note. The converse $H(x)^2 \ll H_1(x)H_2(x)H_3(x)$ is also true. The assertion that $2\log H = \log H_1 + \log H_2 + \log H_3 + O(1)$ on $X(k)$ is in fact a special case of a standard result in the theory of heights (cf. e.g. [12, 2.8]).

According to this lemma, we can choose a positive constant c_1 such that $H_1(x)H_2(x)H_3(x) \le c_1^3 H(x)^2$ on $X(k)$. If $n_i(B)$ is the number of points $x \in U(k)$ such that $H(x) \le B$ and $H_i(x) \le c_1B^{2/3}$, then

$$n(B) \le n_1(B) + n_2(B) + n_3(B).$$

It is thus sufficient to show that $n_i(B) \ll B^{4/3+\varepsilon}$ for $i = 1, 2, 3$. We will concentrate on the proof of the statement $n_1(B) \ll B^{4/3+\varepsilon}$. In this particular case, it is convenient to have $L_1 = x_1$ and $L_2 = x_2$. Of course, this change of variables will affect the counting function $n_1(B)$, but as pointed out above, the validity of the statement $n_1(B) \ll B^{4/3+\varepsilon}$ is independent of the choice of coordinates.

The next step in the proof is to look at the fibres of $f_1 : X \to \mathbb{P}^1_k$ in U. If we define $n_1(a, b, B)$ to be the number of rational points in $f_1^{-1}(a, b) \cap U$ with height not exceeding B, then we have

$$n_1(B) \le \sum_{\substack{(a,b)\in\mathbb{P}^1(k)\\ H(a,b)\le c_1 B^{2/3}}} n_1(a, b, B). \tag{4.1}$$

From the definition of F we see that $(ay_1, by_1, y_2, y_3) \in f_1^{-1}(a, b) \cap U$ only if $y_1 \neq 0$ and $q(y_1, y_2, y_3; a, b) = 0$, where

$$q(y_1, y_2, y_3; a, b) = 2\, b\, y_2 L_3(by_1, y_2, y_3) - 2\, a\, Q(ay_1, by_1, y_2, y_3).$$

In order to estimate the counting functions $n_1(a, b, B)$ in the sum (4.1), we shall apply the results from the previous section to the quadratic forms $q(y_1, y_2, y_3; a, b)$. However, the results in the previous section were formulated for quadratic forms, defined over the ring of integers of k, and points in projective space, with conditions on their integral coordinates. Before we can continue, we therefore have to look more closely at the definition of $n_1(a, b, B)$ and make some adjustments to be able to apply these results.

Let $\mathfrak{a}_1, \dots, \mathfrak{a}_h$ be ideals representing the ideal classes of $\mathfrak{o}$. By the proof of proposition 3, we can choose coordinates $(a, b) \in \mathfrak{o}^2$ for each point in $\mathbb{P}^1(k)$ such that $\langle a, b\rangle = \mathfrak{a}_j$ for some j and $\sup\{\|a\|_v, \|b\|_v\} \ll H(a, b)^{1/s_k}$ for all $v \mid \infty$. We let A be the set of all such coordinates and $A(B)$ be the subset consisting of the elements (a, b) with $H(a, b) \le c_1 B^{2/3}$. By the same proposition, each point on the fibres of f_1 has coordinates $(ay_1, by_1, y_2, y_3) \in \mathfrak{o}^4$, where $(a, b) \in A$ and

$$\sup\{\|ay_1\|_v, \|by_1\|_v, \|y_2\|_v, \|y_3\|_v\} \ll H(ay_1, by_1, y_2, y_3)^{1/s_k}. \tag{4.2}$$

A choice of (y_1, y_2, y_3) under these restrictions does not guarantee that $y_1 \in \mathfrak{o}$. However, by multiplying (y_1, y_2, y_3) with a suitable factor, say, a generator of the principal ideal $\prod_{i=1}^h \mathfrak{a}_i^2$, and by changing the implied constant of (4.2) accordingly, we may assume that $(y_1, y_2, y_3) \in \mathfrak{o}^3$. If we introduce the symbol c_2 for this modified implied constant, then we see that $n_1(a, b, B)$ is bounded from above by the number of points $(y_1, y_2, y_3) \in \mathbb{P}^2(k)$ satisfying $y_i \in \mathfrak{o}$, $(ay_1, by_1, y_2, y_3) \in U(k)$, and

$$\sup\{\|ay_1\|_v, \|by_1\|_v, \|y_2\|_v, \|y_3\|_v\} \le c_2 B^{1/s_k}.$$

In fact, we redefine $n_1(a, b, B)$ to be this cardinality.

Let $\mathbf{r} \in (\mathbb{R}_{>0})^{s_k}$ be a vector with components r_v. Then by the definition of the set $L(\mathbf{r}) \subset \mathfrak{o}$ we have that an integer x of k belongs to $L(\mathbf{r})$ if and only if $\|x\|_v \le r_v$ for all $v \mid \infty$. In agreement with the observations above, we now see that we can define $n_1(a, b, B)$ to be the number of points $(y_1, y_2, y_3) \in \mathbb{P}^2(k)$ on the conic $q(y_1, y_2, y_3; a, b) = 0$, not lying on any line on X, and such that $y_i \in L(\mathbf{r}_i)$, where $\mathbf{r}_1$ is the vector with components

$c_2B^{1/s_k}/\sup\{\|a\|_v, \|b\|_v\}$ and $\mathbf{r}_2 = \mathbf{r}_3$ the vectors with components c_2B^{1/s_k}. With this definition of $n_1(a,b,B)$, we are now in a position to use the results from the previous section to handle the sum (4.1). Note that with our new definitions we may write this sum as

$$\sum_{(a,b)\in A(B)} n_1(a,b,B).$$

Also note that we only have to sum over those $(a,b) \in A(B)$ for which $q(y_1,y_2,y_3;a,b)$ is non–singular. By definition, $n_1(a,b,B) = 0$ whenever the components of $f_1^{-1}(a,b)$ are lines on X.

On the hypothesis that $q(y_1,y_2,y_3;a,b)$ is non–singular, theorem 6 gives

$$n_1(a,b,B) \ll \left(1 + \frac{B^{3/2}\, N_k(\Delta_0(a,b))}{H(a,b)^{1/2}\, N_k(\Delta(a,b))^{1/2}}\right) N_k(\Delta(a,b))^{\varepsilon}, \tag{4.3}$$

where $\Delta(a,b)$ is the determinant of $q(y_1,y_2,y_3;a,b)$ and $\Delta_0(a,b)$ the ideal generated by all the 2×2–minors of the matrix of $q(y_1,y_2,y_3;a,b)$. If, in addition, $q(0,y_2,y_3;a,b)$ is non–singular, proposition 7 gives

$$n_1(a,b,B) \ll B^{1+\varepsilon}/H(a,b). \tag{4.4}$$

In order for these estimates to be useful we need the following two lemmas.

Lemma 7. *$N_k(\Delta_0(a,b)) \ll_F 1$ for all $(a,b) \in A$.*

Proof. Let $M(a,b)$ be the matrix of $q(y_1,y_2,y_3;a,b)$. The ij:th minor of $M(a,b)$ will be a certain integral form $M_{ij}(a,b)$. If these forms were to have a common factor $(\beta a - \alpha b)$ over some algebraic closure of k, then the rank of $q(y_1,y_2,y_3;\alpha,\beta)$ would be at most one. But $f_1^{-1}(\alpha,\beta)$ is not allowed to be a double line since X is non–singular. Thus the forms $M_{ij}(a,b)$ do not have a common factor. According to Hilbert's Nullstellensatz, there is a positive integer n and polynomials f_{ij}, g_{ij} such that $a^n = \sum f_{ij}M_{ij}$ and $b^n = \sum g_{ij}M_{ij}$. Then by clearing denominators we see that γa^n, $\gamma b^n \in \Delta_0(a,b)$ for some $\gamma \in \mathfrak{o}$. Hence, $N_k(\Delta_0(a,b)) \ll N_k(\langle a^n, b^n\rangle) = N_k(\mathfrak{a}_j)^n$ for some $j = 1,2,\ldots,h$. $\square$

The lemma tells us that we can forget about the factor $\Delta_0(a,b)$ in (4.3).

Lemma 8. *$q(0,y_2,y_3;a,b)$ is non–singular for almost all $(a,b) \in A$.*

Proof. By definition

$$q(0,y_2,y_3;a,b) = 2\,b\,y_2L_3(0,y_2,y_3) - 2\,a\,Q(0,0,y_2,y_3).$$

If $L_3(0,y_2,y_3) = \mu y_2 + \nu y_3$ and $Q(0,0,y_2,y_3) = \alpha y_2^2 + \beta y_2y_3 + \gamma y_3^2$ for some α, β, γ, μ, $\nu \in \mathfrak{o}$, then

$$q(0,y_2,y_3;a,b) = 2\,(b\mu - a\alpha)\,y_2^2 + 2\,(a\beta - b\nu)\,y_2y_3 - 2\,a\,\gamma\,y_3^2.$$

Hence, $q(0,y_2,y_3;a,b)$ is singular precisely when

$$(4\alpha\gamma - \beta^2)\,a^2 + 2\,(\beta\nu - 2\gamma\mu)\,a\,b - \nu^2b^2 = 0.$$

It is straightforward to check that X would be singular if this form were to vanish identically. Thus $q(0,y_2,y_3;a,b)$ is singular for at most two pairs $(a,b) \in A$. $\square$

From this last lemma, we see that if $q(0, y_2, y_3; a, b)$ is singular, then we may use the estimate $n_1(a, b, B) \ll B$ given by proposition 6. It thus remains to sum $n_1(a, b, B)$ over those $(a, b) \in A(B)$ for which both $q(y_1, y_2, y_3; a, b)$ and $q(0, y_2, y_3; a, b)$ are non–singular. In this sum, the constant term of (4.3) gives the contribution $O(B^{4/3+\varepsilon})$. Simply because the cardinality of $A(B)$ is $O(B^{4/3+\varepsilon})$. We therefore only have to account for the second term

$$B^{3/2+\varepsilon} H(a, b)^{-1/2} N_k(\Delta(a, b))^{-1/2} \tag{4.5}$$

in the contribution to $n_1(a, b, B)$.

We divide the ranges of $H(a, b)$ and $N_k(\Delta(a, b))$ into intervals $(R, 2R]$ and $(S, 2S]$, respectively. Since $\Delta(a, b)$ is a form of degree 5, the next lemma states that there are $O_F(S^{1/5} R^{1+\varepsilon})$ elements $(a, b) \in A$ which satisfy $H(a, b) \le 2R$ and $N_k(\Delta(a, b)) \le 2S$. The fact that $\Delta(a, b)$ is of degree 5 also implies that $N_k(\Delta(a, b)) \ll H(a, b)^5 \ll B^{10/3}$.

If $S \le B^{5/3}$, then

$$\sum_{\substack{H(a,b)\in(R,2R]\\ N_k(\Delta(a,b))\in(S,2S]}} n_1(a, b, B) \ll S^{1/5} R^{1+\varepsilon} B^{1+\varepsilon} R^{-1} \ll B^{4/3+\varepsilon}$$

by (4.4), and if $S \ge B^{5/3}$, then

$$\sum_{\substack{H(a,b)\in(R,2R]\\ N_k(\Delta(a,b))\in(S,2S]}} n_1(a, b, B) \;\ll\; S^{1/5} R^{1+\varepsilon} B^{3/2} R^{-1/2} S^{-1/2+\varepsilon} \;\ll\; B^{4/3+\varepsilon}$$

by (4.5). This completes the proof of the theorem, on summing over appropriate values of R and S.

Lemma 9. *Let $G(x, y)$ be a form of degree n with coefficients in $\mathfrak{o}$, and let R, $S \ge 1$ be given. Then there are $O_G(S^{1/n} R^{1+\varepsilon})$ elements $(x, y) \in \mathfrak{o}^2$ such that $0 < N_k(G(x, y)) \le S$ and $\sup\{\|x\|_v, \|y\|_v\} \le R^{1/s_k}$ for all $v \mid \infty$.*

Proof. First we note that we may assume that $G(x, y)$ is irreducible over k. If not, $G(x, y) = G_1(x, y)\, G_2(x, y)$ for some forms of positive degrees n_1 and n_2, respectively. If $N_k(G(x, y)) \le S$ for some $(x, y) \in \mathfrak{o}^2$, then either $N_k(G_1(x, y)) \le S^{n_1/n}$ or $N_k(G_2(x, y)) \le S^{n_2/n}$. On the assumption that the lemma is valid for all forms of degree less than n, we thus have that it is valid for all reducible forms of degree n.

Now assume that $G(x, y)$ is irreducible and let $\sigma_v : k \to \mathbb{C}$ be embeddings such that $|x|_v = |\sigma_v(x)|$ for all $x \in k$. Then there are non–zero complex numbers μ_{vi} and ν_{vi} such that

$$\sigma_v(G(x, y)) = \prod_{i=1}^{n} (\mu_{vi}\, \sigma_v(x) - \nu_{vi}\, \sigma_v(y)).$$

If $(x, y) \in \mathfrak{o}^2$ satisfies $N_k(G(x, y)) \le S$, then

$$\prod_{v\mid\infty} |\mu_{vi}\, \sigma_v(x) - \nu_{vi}\, \sigma_v(y)|^{d_v} \le S^{1/n} \tag{4.6}$$

for some i. It is thus sufficient to show that there are $O(S^{1/n} R^{1+\varepsilon})$ elements $(x, y) \in \mathfrak{o}^2$ satisfying the assumptions of the lemma and (4.6) for a fixed i. Note that there are $O(R)$ elements $y \in \mathfrak{o}$ such that $\sup \|y\|_v \le R^{1/s_k}$.

We therefore assume that y is fixed and show that there are $O(S^{1/n}R^{\varepsilon})$ elements $x \in \mathfrak{o}$ such that (x,y) have the required properties. In order to accomplish this, we choose one place w of k and divide the ranges of $|\mu_{vi}\,\sigma_v(x) - \nu_{vi}\,\sigma_v(y)|^{d_v}$ for the places $v \neq w$ into intervals $(T_v, 2T_v]$. Note that

$$R^{1/s_k - n} \ll |\mu_{vi}\,\sigma_v(x) - \nu_{vi}\,\sigma_v(y)|^{d_v} \ll R^{1/s_k}$$

for all $(x,y) \in \mathfrak{o}^2$ satisfying the assumptions of the lemma. We get the lower bounds from the above bounds and the fact $1 \leq N_k(G(x,y))$.

Now, if $|\mu_{vi}\,\sigma_v(x) - \nu_{vi}\,\sigma_v(y)|^{d_v} \in (T_v, 2T_v]$ and (4.6) holds, then

$$|\mu_{wi}\,\sigma_w(x) - \nu_{wi}\,\sigma_w(y)|^{d_w} \ll S^{1/n} / \prod_{v \neq w} T_v.$$

Since $\|x - x'\|_v \ll Y / |\mu_{vi}|^{d_v}$ whenever $|\mu_{vi}\,\sigma_v(x) - \nu_{vi}\,\sigma_v(y)|^{d_v} \leq Y$ and $|\mu_{vi}\,\sigma_v(x') - \nu_{vi}\,\sigma_v(y)|^{d_v} \leq Y$, proposition 2 gives the estimate $O_G(S^{1/n})$ for the number of elements $x \in \mathfrak{o}$ which satisfies the above conditions. By summing over all the intervals $(T_v, 2T_v]$, we get the required estimate $O_G(S^{1/n}R^{\varepsilon})$, and this completes the proof. $\square$

References

[1] E. Bombieri and J. Vaaler. On Siegel's lemma. *Invent. Math.*, 73:11–32, 1983.

[2] J. W. S. Cassels. *An Introduction to the Geometry of Numbers.* Springer–Verlag, 1959.

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

[4] R. Hartshorne. *Algebraic Geometry.* Springer–Verlag, 1977.

[5] D. R. Heath-Brown. The density of rational points on cubic surfaces. *Acta Arith.*, 79(1):17–30, 1997.

[6] D. R. Heath-Brown. Counting rational points on cubic surfaces. In E. Peyre, editor, *Nombre et Répartition de points de hauteur bornée*, number 251 in Astérisque, pages 13–29. Société mathématique de france, 1998.

[7] C. Hooley. On the numbers that are representable as the sum of two cubes. *Angew. Math.*, 314:146–173, 1980.

[8] S. Lang. *Algebraic Number Theory.* Springer–Verlag, second edition, 1994.

[9] Yu. I. Manin and Yu. Tschinkel. Points of bounded height on del Pezzo surfaces. *Compositio Math.*, 85:315–332, 1993.

[10] I. Reiner. *Maximal Orders.* Academic Press Inc., 1975.

[11] S. H. Schanuel. Heights in number fields. *Bull. Soc. Math. Fr.*, 107:433–449, 1979.

[12] J.-P. Serre. *Lectures on the Mordell–Weil Theorem.* Wieweg, 1989.

[13] G. Tenenbaum. *Introduction to analytic and probabalistic number theory.* Cambridge university press, 1995.

[14] T. D. Wooley. Sums of two cubes. *Internat. Math. Res. Notices*, (4):181–185, 1995.

Dept. of Mathematics, Chalmers University of Technology, Göteborg University, SE–412 96 Göteborg, Sweden

E-mail address: `nibro@math.chalmers.se`